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
XXIX МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ
15 декабря 2021 г., Москва

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

НАУЧНОЕ ЭЛЕКТРОННОЕ ИЗДАНИЕ

Москва
ИПУ РАН
2021

УДК 658.012:658.382.2
ББК 65.9:66.2:68.9
П78

Проблемы управления безопасностью сложных систем : материалы XXIX Международной конференции, 15 декабря 2021 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. (6,1 Мб). – Москва : ИПУ РАН. – 2021. – 1 электрон. опт. диск (CD-R). – Систем. требования: Pentium 4; 1,3 ГГц и выше; Acrobat Reader 4.0 или выше. – Загл. с титул. экрана. – ISBN 978-5-91450-257-4. – Номер госрегистрации в НТЦ «Информрегистр» 0322103523. – 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 978-5-91450-257-4

СОДЕРЖАНИЕ

I. Общетеоретические и методологические вопросы обеспечения безопасности

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

Как не оказаться в XVI веке

Аннотация: В настоящее время общество сталкивается с переменами и рисками такого масштаба, которые могут кардинально изменить социально-технологическую среду и в мире, и в России. Следуя логике выдающегося русского философа Н.А. Бердяева, можно сказать, что имеется возможность отката назад, на несколько столетий в прошлое. Этому способствует проходящая на наших глазах гуманитарно-технологическая революция.

Происходящие изменения носят системный характер и не ограничиваются отдельными сферами жизнедеятельности. Происходит деглобализация и разбиение мирового пространства на несколько цивилизаций, развивающихся по своим сценариям. Пандемия COVID-19 обнажила глубокие противоречия в мировом развитии.

В этих заметках, опирающихся на результаты системного анализа и математического моделирования, рассмотрен ряд угроз, стоящих перед нашей цивилизацией – миром России, и пути выхода из нынешнего кризиса.

Ключевые слова: мир России, управление рисками, исторический прогноз, точка бифуркации, самоорганизация, гуманитарно-технологическая революция, сценарии выхода из кризиса, XVI век, Новое Средневековье

Игры со временем

> Наступает такой момент, когда противоречия становятся настолько острыми, что начинают приводить к все более значительным отклонениям. На языке новой науки это означает наступление хаоса (или резкого снижения тех параметров, которые можно объяснить, исходя из детерминистских уравнений), что, в свою очередь, ведет к бифуркациям, наличие которых очевидно, но контуры которых непредсказуемы по самой их природе. На этой основе и возникает новый системный порядок.
>
> И. Валлерстайн

Одним из принципиальных достижений исторической науки XX века стала концепция *исторического времени*, выдвинутая французским исследователем Фернаном Броделем [1].

Следуя логике количественного анализа, он выделил три интервала:

– *короткое время* смены политических событий, характеризующее чрезвычайные ситуации, экономическую конъюнктуру, повседневную жизнь;

– *средняя продолжительность* или *циклическое время*, описывающее подъемы и спады культурных, экономических, демографических, миграционных процессов;

– *длительная продолжительность*, *долгое время* (фр. *longue duree*), характеризующее крупные структуры совместного проживания, медленные процессы, поддерживающие целостность цивилизаций, этносов, сложившийся мировой порядок.

До настоящего времени риски, угрозы, кризисы рассматривали в коротком времени с целью не допустить разрушительных перемен на циклическом времени, переломить неблагоприятные тенденции.

Однако сейчас ситуация меняется. Увеличение масштабов угроз, их стремительное распространение требует усилий, чтобы не допустить масштабных перемен в долгом времени.

О возможности таких перемен писал в 1924 году выдающийся русский философ Н.А. Бердяев, пессимистически оценивая происходящие изменения. Он полагал, что эти перемены приведут в Новое Средневековье. Он пишет: «Духовные начала новой истории изжиты, духовные силы ее истощены… Все категории пережитого уже солнечного дня непригодны для того, чтобы разобраться в событиях и явлениях нашего вечернего исторического часа». Наука отступает, предоставляя место религии: «Знание свободно. Но я не могу уже осуществить целей познания без обращения к религиозному опыту, без религиозного посвящения в тайны бытия. В этом я уже средневековый человек, а не человек новой истории» [2].

Бердяев рисует и новый социальный строй, в котором нет равенства и ключевую роль играют иерархические структуры: «Индустриально-капиталистическая эпоха оказалась хрупкой, она сама себя отрицает, она порождает катастрофы. Мировая война с ее неслыханным ужасом порождена этой системой… Город должен приблизиться к деревне. Придется организоваться в хозяйственные союзы и кооперации… Чудовищных частных богатств новой истории не будет, но не будет и голодных и погибающих от нужды. Придется перейти к более упрощенной и элементарной культуре. Конец капитализма есть конец новой истории и начало средневековья. Грандиозное предприятие новой истории нужно ликвидировать, оно не удалось».

Стоит обратить внимание еще на один важный откат к прошлому: «Сама наука начинает возвращаться к своим магическим истокам, и скоро окончательно выявится магический характер техники… Мы опять вступаем в атмосферу чудесного, столь чуждого новой истории, опять возможными станут белая и черная магии. Опять возможны страстные споры о тайнах божественной жизни. Мы переходим от душевного периода к духовному периоду» [2].

По счастью, Бердяев ошибался. Социализм открыл новые перспективы. Взлет СССР во многом определил XX век. Оказалось, что можно хорошо жить и эффективно хозяйствовать без буржуазии, империй и религиозной мистики. Влияние науки и технологий трудно переоценить – за век число жителей в мире выросло почти вчетверо, а средняя ожидаемая продолжительность жизни в России и многих развивающихся странах увеличилась вдвое. По сути, это воплощение мечты Фауста о второй молодости. Человечество открыло путь в космос, в мир атомных и ядерных масштабов. Но среднее время, на котором развивался социализм, закончилось, и человечество делает новый выбор.

Вновь возникает ощущение тупика и мысли о новом Средневековье. Известный российский философ Ф.И. Гиренок пишет: «Грубо говоря, вся история помещена в пространство пата. У нее есть то, что можно назвать днем, и то, что можно назвать ночью.

День – это Возрождение. Ночь – это Средние века. Днем зародилась национальная экономика. Днем возникло национальное государство. Днем появилась философия. В ночи появляется хозяин. И вера. Ночь дробит, разделяет и размножает… День закончился. В XX веке были уже сумерки. Наступило время ночи. И нужно учиться жить в эпоху иррационального… В момент, когда схлопнется радужный пузырь экономики, мы узнаем, что пришла ночь и пора разрушать идолы культа денег. Тогда мы узнаем, что пришло время империй нового средневековья» [3].

Для такого взгляда есть серьезные основания, не опирающиеся только на обобщение текущих событий. При описании сложного объекта специалисты проецируют его на ось или плоскость, чтобы выяснить и описать наиболее важные причинно-следственные связи. При описании мировой истории Маркс и Энгельс взяли в качестве оси собственность на средства производства. Это привело к историческому материализму с его делением на эпохи – от первобытнообщинной до коммунистической.

Но возможна и другая ось, отражающая роль науки как источника развития общества. При этом деление оказывается другим. Традиционная фаза развития цивилизации (до XX века), в которой в центре внимания оказывается мир природы. Индустриальная фаза (XX век) – в центре внимания «вторая

природа» – техносфера. Постиндустриальная фаза (в которую мир входит сейчас). В ней самые большие риски, возможности и проблемы связаны с человеком. Такую теорию около полувека назад предложил американский социолог Дэниел Белл. В течение нескольких десятилетий она была одной из возможных концепций.

Однако ситуация кардинально изменилась в связи с массовым использованием компьютеров в быту. Скорость, масштаб и влияние происходящих перемен на общество позволяют говорить о происходящей на наших глазах *гуманитарно-технологической революции* [4].

И здесь мы имеем выбор, точку бифуркации, которая может определить будущее.

В самом деле, в кармане у каждого появилась огромная библиотека. Он может узнавать и осмысливать новости о происходящем на планете, немедленно связываться с огромным количеством людей, прослушать любую из миллионов мелодий, фотографировать и снимать происходящее перед ним. Это огромное расширение возможностей, ключ к новым социальным и производственным технологиям, прекрасный инструмент для получения образования.

С другой стороны, это способ жить не своей жизнью, а способ уходить в чужой, виртуальный мир. Интернет позволяет найти свой «клуб по интересам» и общаться в нем, игнорируя всех остальных. В Библии рассказывается о Вавилонской башне, которую люди, объединенные одной идеей, строили, чтобы достичь небес. Но Бог, чтобы блокировать этот впечатляющий проект, «перепутал языки». Интернет может сыграть такую же разрушительную роль. Это наглядно показывает опыт по «электронному образованию», который ставился в России в связи с пандемией COVID-19. Огромное потерянное время при незначительных результатах, зачастую связанное с отторжением учебы и знания.

Выбор очень серьезен. Он определяет будущее. Одни и те же инструменты могут использоваться и для блага, и для разрушения.

Вспомним XVII век – начало Нового времени, столетие науки и технологий. Он начинался с творчества Галилея и Декарта, а заканчивался работами Ньютона и Лейбница. Произошел очень важный переход от исследования и осмысления Бога к изучению

его творения – природы. Именно в XVII веке было сформулировано «Знание – сила».

И Бердяев, и Гиренок, по сути, провозглашают переход из века знания и технологий, столетия больших проектов в XVI век с религией, магией, разнообразием и замкнутостью каст, сословий, цехов, к неравенству и иерархиям. Корень стратегических рисков сегодня связан с движением в XVI век – из настоящего в прошлое. Как остаться в настоящем или шагнуть в будущее? Как сохранить лозунг «Будущее принадлежит всем», а не «Каждому свое»? Несколько последующих фрагментов этого текста посвящены этому выбору в разных сферах жизнедеятельности.

Выход из культурного провала

> Без возврата к основам культуры невозможно творить дело будущего.
>
> С.М. Эйзенштейн

Наша цивилизация – мир России – переживает глубокий культурный кризис. Показатель этого – доля людей в мире, считающих русский язык родным. В 1961 году наш язык был третьим по числу людей, считающих его родным, после китайского и испанского. Сейчас картина иная. Приведем данные сайта Ethnologue 2019 [5]. Первый десяток стран таков: китайский 1311 млн.; испанский – 460 млн.; английский – 379 млн.; хинди – 341 млн.; арабский – 319 млн.; бенгальский – 228 млн.; русский – 134 млн.; португальский – 128 млн.; японский – 128 млн.; лахнда (западный панджаби) – 119 млн.

Почему место России на языковой карте мира так быстро уменьшилось за последние полвека? Ответ дает французский исследователь Клод Ажеж, рассматривавший этот вопрос. По его теории, решающими являются три обстоятельства.

Идеология, представление о перспективах, видение будущего у носителей этого языка. В 1961 году значительная часть мира связывала развитие с коммунистической идеей, с представлением о равенстве, братстве, свободе, с улучшением качества жизни на основе современных технологий. Со всем этим связывался Советский Союз. В Послании Федеральному Собранию 01.03.2021 г. Президент РФ основной угрозой для нашей страны назвал

отсталость и наметил план по ее ликвидации. Однако последующие три года показали, что с воплощением этого плана возникли серьезные проблемы.

Средства, вкладываемые в развитие и распространение культуры.

Знакомство с работой этих фондов, представляющих нашу культуру за рубежом, показывает, что они знакомят людей не с настоящим и будущем нашей страны, а с далеким прошлым – с матрешками, поварешками, сарафанами. Но если страна (в отличие от многих других) не хочет заглядывать вперед, больна футурофобией, то ее будущее, скорее всего, не состоится.

Президент дал поручение создать единый учебник истории. Это поручение не выполнено. В стране преподают историю по 86 разным учебникам и пишутся новые. Элиты не знают, как трактовать развитие СССР в XX веке. Кроме советского наследия опираться не на что, а вспоминать его элитам не хочется.

Освоенные и развиваемые технологии. В народе при описании последнего тридцатилетия популярна фраза «Бухгалтеры победили инженеров». И действительно, остается удивляться таланту и творчеству наших бюрократов и бухгалтеров.

По оценкам экспертов, в мире сейчас эксплуатируется 6,08 млрд. компьютеров, из них 4,3 млрд. – смартфоны, настольные персональные компьютеры – 522 млн., 796 млн. – ноутбуки, 473 млн. – планшеты. По сути, компьютер стал предметом личного пользования.

И среди всего этого компьютерного богатства практически нет инструментов, сделанных в России. Мы не имеем собственной цифровой платформы, персональных компьютеров, мобильных телефонов, планшетов и многого другого, несмотря на решения, постановления, немалые деньги, вложенные во все это, программу «Цифровая экономика».

Создание своей электроники и программного обеспечения для оборонного комплекса и государственных структур в качестве ключевой задачи несколько лет назад обозначил вице-премьер правительства РФ Ю.И. Борисов. Но, судя по всему, у него при рещении этой задачи начались серьезные проблемы.

Отсюда понятно управление обсуждаемым риском. Формирование большого проекта для России, разработка

идеологии, предъявление ее миру. Принятие собственной истории. Обретение технологического суверенитета и форсированное развитие сферы высоких технологий.

Демографический императив

> Легко следовать правильно за тем, кто правильно идет впереди.
>
> Я.А. Коменский

В 2020 году численность населения России уменьшилась более чем на 500 тысяч человек. Это рекордное падение численности населения с 2005 года. Ряд экспертов прогнозируют еще большее сокращение населения в 2021 году. Многие существенные проблемы выявила пандемия COVID-19. Обратимся к цифрам на 10.10.2021.

В США было заражено 44,3 млн. человек, привито 57,8% населения (45-е место в мире), умерло 713 тыс. человек.

В Индии заражено 34 млн., привито 20,40% (108-е место), умерло 451 тыс.

В Бразилии заражено 21,5 млн., привито 48,04% (64-е место), умерло 601 тыс.

Великобритания, 8,2 млн. заражено, привито 71,44% (19-е место), 138 тыс. умерло.

Россия – заражено 7,6 млн., привито 30,6% (86-е место), умерло 212 тыс. [6].

В мире заражено 238 млн. и умерло 4,85 млн. человек [6]. По сути, вирус ведет мировую войну против человечества. И эта война стала тестом для систем здравоохранения, медицинской науки, цивилизаций.

Оказалось, что в США нет развитой массовой системы охраны здоровья. Представление о заботе о жизни каждого человека в «граде на холме» оказалось блефом.

Тяжело переносит пандемию Россия. Потери населения сравнимы с числом жертв в крупном военном конфликте – около 1000 человек ежедневно. По военной аллегории – полк за неделю, больше дивизии за месяц.

Большим успехом отечественной науки стала разработка вакцины «Спутник-V». Несмотря на развал биотехнологической

отрасли в 1990-х годах, удалось наладить массовый выпуск этого средства и создать условия для массовой вакцинации.

Однако цифры показывают, что люди не вакцинируются, имея для этого все возможности. Это своеобразная «плата» за невежество, развал образования, недоверие к науке и технологиям.

Другая причина – недоверие к власти – раз она советует прививаться, то многие думают, что делать это не следует. По данным сотрудников Института психологии, уровень доверия граждан к правительствам составляет в Китае – 77%, в Италии – 48%, в США – 45%, в России – 27% [7].

Есть и еще одна причина возникших трудностей. В 2000-2015 году количество больниц в России сократилось в два раза – с 10,7 тыс. до 5,4 тыс. Эксперты отмечали, что при таком темпе закрытия больниц (353 в год) количество медучреждений к 2022 году достигнет 3 тысяч, то сеть уровня Российской империи в 1913 году [8]. Естественно, коронавирус спутал карты «оптимизаторов» от медицины.

Закрытие больниц и поликлиник означает уменьшение числа врачей. И это уже серьезная долговременная проблема. Студентов-медиков надо учить 5 лет, и еще 5 лет уходит на то, что бы он действительно стал профессиональным специалистом.

Советская система здравоохранения являлась одной из лучших в мире, пандемия COVID-19 показала, что сейчас мы имеем место с ее развалинами. Отсюда следует важнейшее направление прорыва, связанное с форсированным развитием медицины и доведением ее до мирового уровня. Это полностью согласуется с Посланием Федеральному собранию 01.03.2018. Важно перейти от слов к делу.

Следует обратить внимание на то, что в войне с COVID-19 есть страны, которые действуют намного успешнее России. Обратим внимание на две: Китай – 1250555 заразившихся (76,15% привитых, 13-место), Австралия – 129567 заразившихся (53,79% привитых, 55 место в мире).

Заметим ключевое значение перемен в этой области для России. Руководитель Давосского экономического форума К. Шваб и его соавтор Т. Маллерет считают, что мир погрузился в режим постоянных пандемий. И это требует ликвидации национальных границ, религий, правительств, нового мирового правительства и нового социального строя – «инклюзивного капитализма» [9].

Для такого взгляда, по сути, блокирующего развитие человечества, есть серьезные «технологические основания». Создание атомной бомбы требует огромных затрат энергии, высоких технологий, создания целой отрасли промышленности, и поэтому мировому сообществу в той или иной степени удавалось держать создание и распространение этого оружия под контролем. Для того, чтобы «заменить» COVID-19 другой инфекцией, которая может привести к сравнимой по масштабу пандемии, требуется работа 10-15 квалифицированных специалистов в нескольких комнатах и затраты в несколько миллионов долларов. Это совсем другая жизнь, кардинально отличающаяся от той, что была раньше.

Здесь нужны совсем другие механизмы управления рисками и очень высокие профессиональные и нравственные требования к специалистам, которые владеют подобными технологиями.

Отсюда следует ключевое направление прорыва Росси в будущее. Оно связано с форсированным развитием медицины, биотехнологий и защитой биологического пространства. Без всего этого наша страна не сумеет сохранить суверенитет.

Отношение к населению, к собственным гражданам в России должно кардинально измениться к лучшему. Центральным событием переживаемой эпохи является глобальный демографический переход. Этот процесс связан с изменением репродуктивной стратегии – от «высокая смертность – высокая рождаемость» к «низкая смертность – низкая рождаемость». Однако разные страны, этносы, цивилизации проходят этот переход в разном темпе. По прогнозам население мира стабилизируется на уровне 11,5 млрд. человек [10]. Но при этом демографическая карта мира кардинально изменится. По прогнозу соответствующего департамента ООН, в Азии будет жить 40% людей, в Африке – 40%, в Европе – 10%, в Америке – 10%. По численности населения Россия будет на 22 месте, уступая Судану и Мозамбику и превосходя Мадагаскар и Вьетнам. Многие специалисты называют XXI век столетием Африки.

Для нашей страны это означает, что у нас не будет больше возможности «брать числом, а не умением». Каждый квалифицированный, профессиональный человек, связывающий судьбу с Россией, важен.

Это означает энергичное привлечение соотечественников. Опыт привлечения гастарбайтеров к работе в Европе показывает, что это дает кратковременный, локальный выигрыш и большой локальный проигрыш, порождая множество серьезных социальных и цивилизационных проблем.

Отсюда следует, что должна быть изменена политика обеспечения людей жильем. Ипотеки, при которых люди в течение многих десятилетий платят огромные суммы, в наших условиях неприемлемы.

У детей должно быть превосходное по мировым меркам образование, множество бесплатных секций и дешевые вещи.

Недавно министр обороны РФ выступил с инициативой построить четыре новых города в Сибири. Эта инициатива требует кардинального изменения политики развития Сибири и Дальнего Востока.

«Мягкая сила» государства состоит не в лозунгах, в прессе, в наличии популярных ансамблей, а в том, чтобы в данной стране жить было лучше, чем в других, в некоторых, важных для людей, отношениях. У России должна появиться мягкая сила.

Наше главное достояние – не территория, не полезные ископаемые, а, прежде всего, люди. Вести дела следует, исходя именно из этого.

Экономическая пропасть

Экономика должна быть экономной.

Л.И. Брежнев

Наверное, многих в детстве волновал вопрос, можно ли бесконечно долго падать в бесконечную пропасть. Развитие экономической сферы России в последние тридцать лет позволяет – да. Можно, но до той поры, пока есть огромные ресурсы.

Для того, чтобы заглядывать в будущее, очень полезно оглянуться в прошлое. Во времена горбачевщины, с 1985 года наши ведущие экономисты доказывали, что все или часть средств производства надо передать в частные руки. Капиталисты сумеют

вести хозяйство лучше, чем государство. Некий деятель считал, что мы перейдем в «рыночный рай» за 500 дней.

Одним из инициаторов реформ российской экономики был академик А.Г. Агангебян. Поэтому, чтобы избежать предвзятости в оценке произошедшего в этой сфере, приведем цитату из его и М. Ефремова статьи, опубликованной в газете «Ведомости» в 2020 году: «В 2019 году ВВП России был всего на 10% выше уровня 1990 г.… Объем промышленности в 2019 году немного не дотянул до размеров, которые он имел в Советской России. Доля фонда потребления населения в ВВП существенно возросла, поэтому реальные доходы в расчете на душу населения в 2019 г. превысили уровень 1990 г. на 25%. Это превышение произошло главным образом за счет формирования немногочисленной прослойки богатых людей. 10% самых богатых семей имеют душевный доход около 100 000 руб. в месяц, в то время как 10% самых бедных – только 6000 руб., в 15 раз меньше.

В 1990 г. это социальное неравенство было всего четырехкратным, в 80-х – трехкратным. Так что реальные доходы 2/3 населения России находятся либо на уровне, либо ниже показателей советской России.

В мире нет сколько-нибудь крупной страны с такими низкими темпами социально-экономического развития в последние тридцать лет. За эти годы ВВП стран ЕС вырос в 2 раза, США – в 2,5 раза, Китая – в 3,5 раза. При этом уже сегодня из-за девальвации рубля втрое по сравнению с 2008 г. ВВП России, по оценке Всемирного банка (ВБ), опустился среди крупных стран на 10-е место, а по оценке МВФ и ООН – даже на 12-е. А по уровню экономического развития (ВВП на душу населения при оценке по паритету покупательной способности) Россия занимает 50-е место (оценка ВБ МФ)» [11].

Другими словами, капитализм, который по обещаниям реформистов должен быть «лучше социализма» в России и практически во всех постсоветских странах, не получился.

Богатые ограбили бедных, но не смогли организовать экономическое развитие страны, о чем говорит ее тридцатилетний застой. У власти оказался олигархат, ставящий совсем другие цели.

Суть проблемы олигархата у власти в России сформулировал американский политик Збигнев Бжезинский: «Россия может иметь

сколько угодно ядерных чемоданчиков и ядерных кнопок, но поскольку 500 миллиардов долларов российской элиты лежат в наших банках, вы еще разберитесь: это ваша элита или уже наша? Я не вижу ни одной ситуации, при которой Россия воспользуется своим ядерным потенциалом» [12]. Следует обратить внимание на другое знаковое высказывание этого деятеля: «Новый мировой порядок будет строиться против России, на руинах России и за счет России» [12]. Санкции Запада и его политика во многих других областях полностью подтверждает это заявление. При этом дети и внуки представителей олигархата и руководителей страны учатся в Великобритании и в США. Политика «национализации элиты», заявленная президентом РФ, судя по всему, не удалась.

В настоящее время происходит *гуманитарно-технологическая революция*. В отличие от прежних фаз развития цивилизации именно человек становится основным источником достижений и угроз. Отношение к людям становится важнейшим конкурентным преимуществом страны.

В условиях власти отечественного олигархата это не получается: «Россия занимает 50-е место среди 150 стран по уровню реальных доходов, по индексу социального развития – только 80-е место, по численности бедных и социальному неравенству – 100 место, по уровню жизни пенсионеров 79-98 место» [13].

Россию стремятся на экономической, технологической и многих других картах мира превратить в «маленькую страну». Это показывает, например, доля мирового продукта разных стран в 2017 году – США – 24,32%, Китай – 17,84%, Россия – 1,8%, что меньше, чем у Южной Кореи – 1,86% и Австралии – 1,81%.

Застой в экономике среди прочего связан с ее старением. Если в Германии инновации внедряются в 58,9% компаний, во Франции – 46,5%, в Великобритании – 46,7%, в России – 9,6%.

Доля России в мировой сфере высоких технологий составляет 0,3%. Наша экономика не экономна – она является сырьевым донором других стран, обеспечивая им ресурсы для создания высоких технологий и повышения качества жизни людей. Ориентация на сырьевое развитие, на построение «нефтегазовой империи», «энергетического гаранта» в ущерб остальным отраслям промышленности, как показали прошедшие 30 лет, были ошибкой.

Тем более этих ресурсов не так и много в нашей стране, расположенной в экстремальных географических условиях. В самом деле, доказанные запасы нефти в мире на 2021 год оценивались в 1780 миллионов баррелей. Их распределение по странам таково: Венесуэла – 16%, Саудовская Аравия – 16,7%, Иран – 11,9%, Канада 9,5%, Иран – 8,0%, Объединенные Арабские Эмираты – 5,9%, Кувейт – 5,7%, Россия – 4,5%, США – 2,0%, Китай – 1,4%. Заметим также, что с 2018 года «Би-Пи (до мая 2001 года British Petroleum) принадлежит 20-процентная доля в компании «Роснефть» [13].

Как же СССР в XX веке, начав с очень невысокого уровня, стал сверхдержавой? Ответ прост, и он был дан еще в 2000 году в книге А.П. Паршева «Почему Россия не Америка». Это – *протекционизм, системная достаточность, планирование* и, конечно, другая социальная система.

Протекционизм связан с экстремальными географическими условиями, а, значит, с более высокой себестоимостью продукции. Все, что может производиться в других странах в условиях товарно-финансовой глобализации в этих странах и будет производиться. Отсюда следует, что наш выбор в мировом разделении труда – высокие технологии. Мы должны делать то, что не умеют другие.

Системная достаточность связана с тем, ключевые сферы развития и продукты должны делаться у нас, а не покупаться. В 2014 году Россия закупила товаров за рубежом на $300 млрд. Это своеобразный «налог на развал», – практически вся эта продукция могла бы производиться у нас, развивая нашу страну, а не другие государства.

Планирование, показавшее высокую эффективность в СССР, стратегический прогноз, основы которого были заложены у нас, были успешно восприняты и воплощены другими странами: «В настоящее время 39 стран, по нашим подсчетам, используют систему планирования, а «пятилетки» использовались для быстрого подъема Японией, Южной Кореей, послевоенной Францией и другими государствами» [14].

Основные направления управления рисками в этой сфере поняты. Вопрос лишь в том, когда произойдет транзит от нынешнего «гайдаровского курса» в экономике к другому курсу.

Распад образования

Хочешь победить врага –
воспитай его детей.
Пословица

В 1990-х годах несколько авторов этого текста участвовали в системном анализе и математическом моделировании системы образования России. В частности, был сделан вывод, что при сохранении этого курса произойдет распад образования России в течение 15-20 лет. Это время пришло, и сделанный прогноз, к сожалению, оправдался.

Однако сейчас, в последние несколько лет, мы имеем качественные сдвиги. Они связаны с развалом школьного образования. Это стало видно в преподавательской деятельности. «Болонизация» российского образования, начавшаяся с 2003 года, участие вузов страны в программе «5-100-20» под контролем западных экспертов уничтожила преимущества советской школы и сориентировала систему на подготовку кадров для западных компаний. Однако при этом «держалась» средняя школа страны. На знания, полученные в ней, можно было опираться. Сейчас это время прошло – мы пытаемся дать высшее образование тем, кто не имеет среднего.

В средней школе происходило столкновение российской и западной культур. И, в конце концов, при активной поддержке сверху западная победила. Реформатор от образования А.Г. Асмолов обозначил этот переход «от культуры полезности к культуре достоинства», от предмето-центричного образования к личностно-ориентированному.

Выдающийся психолог А.Н. Леонтьев развил деятельный подход в образовании и представление о высших эмоциях (совесть, ответственность, коллективизм). Эти идеи успешно развивала Н.Ф. Талызина. Речь идет о коллективном воспитании, о тесной связи с обществом, где эти эмоции формируются и для которого они очень важны. Предметоцентричность означает, что мы оцениваем подготовку школьников по тому, знают ли они предмет, а учителей по тому, могут ли они ему научить. Советское образование, построенное на этих принципах, было одним из лучших в мире.

В новой России образование превратили в услугу, учителей, по существу, в слуг, ликвидировали воспитание. «Личностно-ориентированный подход» означает, что надо «развить личность», а не знания, умения, навыки, связанные с предметом. При этом большой упор делался на «цифровое образование», ведь «в интернете можно все найти». Лишение учителя инструментов наказания привело к катастрофическому падению дисциплины во многих классах. Это калька с западной системы провоцирует разрыв поколений, катастрофический для нашего общества. Школа начала растить одиночек. Дети ощущают одиночество, часто не умеют дружить. Расстрелы во многих школах, да еще и при наличии охраны, – признак психологического неблагополучия в школах.

По данным социологов, около половины школьников на постсоветском пространстве пользуются услугами репетиторов. Школы превратились в инструмент разделения общества – те, кто способен нанять репетиторов (часто весьма дорогих), купить платные компьютерные курсы, имеют одно, а остальные – совсем другое. Появились негосударственные школы, обучение в которых стоит более 500 тыс. рублей в год. В Москве имеет место острый дефицит квалифицированных учителей.

История имеет огромное значение и для формирования мировоззрения, и для судеб страны. Несколько лет назад Президент РФ поручил подготовить единый учебник истории для школ России. Это поручение не выполнено – историю нашей страны в XX веке сейчас преподают по 86 учебникам. Большинство выпускников считает, что мы живем в стране с непонятным будущем и неясным прошлым; не знает, что же делали старшие поколения. Лекции, которые довелось читать одному из авторов этих строк будущим экономистам и юристам одного из ведущих вузов, показывают, что большинство ясно представляют двух людей XX века – Ю.А. Гагарина и В.В. Путина. Остальных они либо не знают, либо не представляют их дела. Эту печальную картину победы Запада над Россией в области образования показывают международные сравнения.

С 2000 года проводится Международная программа по оценке образовательных достижений – Programme for International Student Assessment (PISA). Главная цель исследования – ответить на

вопрос: «обладают ли 15-летние школьники знаниями и умениями, необходимыми им для решения широкого диапазона задач в различных сферах человеческой деятельности, общения и социальных отношений».

Если в 2000 году наши ребята были в третьем десятке среди школьников мира, то сейчас они в четвертом. Тест проводится для средних школьников по математике, по естественным наукам, по чтению на родном языке. Приведем для примера данные по естественным наукам: Китай (4 провинции, где проводится тест) – 590; Сингапур – 551, Макао (Китай) – 544; Эстония – 550; Японии – 529; Финляндия – 528; Южная Корея – 519; Канада – 518; Латвия – 481; Литва – 482; Россия – 478; Беларусь – 471; Украина – 469; Молдова – 428; Казахстан – 397; Грузия – 383.

Другими словами, прозападные реформы катком проехались по школьному образованию почти во всех постсоветских странах.

Еще один наглядный пример. В 1970 году был создан замечательный журнал «Квант» для школьников, интересующихся физикой и математикой. Он издается до сих пор. И в советское время его тираж составлял 350 тыс. экземпляров, а сейчас 900 штук. Ребята, читавшие его, приходили в науку, в инновационную среду, в оборонно-промышленный комплекс. Кто в эти области придет сейчас?

В советской школе были свои недостатки, но тот, кто сравнивает ее с нынешней «в чужом глазу соринку видит, а в своем бревна не замечает». У нас была и должна быть в будущем одна из лучших систем образования мира, неразрывно связанная с нашей культурой, стратегией, целями. Поэтому как предотвратить распад и начать двигаться вверх и здесь достаточно понятно.

Глупость или измена? Научный контекст

Американские коллеги объяснили мне, что «низкий уровень школьного образования в их стране – сознательное достижения ради экономических целей. Дело в том, что, начитавшись книг,

образованный человек становится худшим покупателем: он меньше покупает и стиральных машин, и автомобилей, начинает предпочитать им Моцарта или Ван Гога, Шекспира или теоремы. От этого страдает экономика общества потребления и, прежде всего, доходы хозяев жизни – вот они и стремятся не допустить культурности и образованности (которые, вдобавок, мешают им манипулировать населением, как лишенным интеллекта стадом).

В.И. Арнольд

Бухгалтеры победили ученых.

Фольклор

Оценка происходящего в российской науке и управление рисками в этой сфере зависит от ответа на один вопрос: нужна ли нынешней правящей элите наука в современной России.

Если не нужна, то все делается идеально. В самом деле, если ориентироваться на роль сырьевого донора более развитых стран, то наличие умных, образованных людей этому только мешает. Важнейшая функция науки – прогноз. Вы когда-нибудь слышали по радио или телевидению, что будет с нашей страной через 20-30 лет? Мнение ученых, опирающихся на данные, модели, сравнения тут явно не ко двору.

Цикл воспроизводства инноваций, с которым в России проблема, включает *фундаментальную науку* (которую координировала Академия наук, созданная в 1724 году), *прикладную науку* (в которой делается 75% изобретений), *опытно-конструкторские разработки* (их должны были, по замыслу реформаторов, вести крупные высокотехнологичные компании).

В силу ориентации на сырьевой сектор и проводившуюся политику таких компаний в стране практически нет, прикладная наука в большей своей части была ликвидирована в 1990-е. И в качестве «вишенки на торте» в 2013 году Российскую академию наук лишили научных институтов и сделали клубом заслуженных ученых. Академия наук (1724-2013), созданная Петром I по совету Г.В. Лейбница, приказала долго жить. В соответствии с принятым в 2013 году законом РАН перестала быть научной организацией, которой можно проводить исследования.

Очевидно, тут есть наша национальная традиция. Царь-пушка, которая никогда не стреляла, Царь-колокол, который никогда не звонил, и РАН без научной работы.

Институты трех академий (РАН, РАМН, РАСХН) отдали под начало Министерству образования и науки РФ (Минобр). Что делать, если наука не нужна? Чем занять ученых? Чиновники блестяще решили эту задачу. Пусть ученые пишут статьи, неважно какие и о чем. Но чтобы усложнить им задачу «настоящими» статьями были признаны те, которые упомянуты в базах данных Scopus и Web of Science.

Оценку и определение направления развития отечественной науки поручили западным экспертам. Отечественная наука оказалась «на подхвате» у западной. Западу же наша наука не нужна. «Если в стране есть много людей, знающих физику или математику, то у такой страны появляются ядерные и космические амбиции, а это не входит в наши планы», – объяснял одному из авторов этих строк вице-президент Всемирного банка.

Наши изобретательные чиновники придумали такие штучки как «самоцитирование» и «автоплагиат». Статьи надо писать новые – без «автоплагиата», наличие которого проверяет искусственный интеллект! Ведущих научных сотрудников увольняют из бывших академических институтов, потому что им «скопуса не хватило».

Огромные первоклассные «научные мануфактуры», оставшиеся с советских времен, превратили в цех ремесленников, пишущих статьи в западные или признанные Западом журналы. Но ведь все равно работают и пишут! Несмотря ни на что. И тут пошла в ход другая уловка. Судя по сайтам, зарплата директоров и их замов в ряде институтов составляет около 1 млн. рублей, что в 30 раз больше зарплаты старшего научного сотрудника и в 60 раз больше,

чем инженера без степени. «Разделяй и властвуй»! Сытый голодного не понимает, но и голодный сытого тоже.

Сумеет ли Иван-дурак – отечественная наука – перепрыгнуть и через эти препятствия? Посмотрим!

Но если наука нужна России, если мы хотим сохранить научный, образовательный, технологический, экономический, политический суверенитет, если хотим совершить «прорыв в сферу высоких технологий», о котором говорит Президент РФ, то разговор совсем другой.

Направление выхода из кризиса, в котором оказалась отечественная наука, очерчены в статье [15], широко обсуждавшейся в 2021 году.

Мы и мир находимся в точке бифуркации. У нас есть еще один шанс выбрать ветвь, которая ведет вверх, а не вниз.

Литература:

1. *Бродель Ф.* Материальная цивилизация, экономика и капитализм XV-XVIII вв. Т.1. Структуры повседневности: возможное и невозможное / Пер. с фр. Л.Е. Куббеля. – М.: Издательство «Весь мир», 2007. – 592 с.

2. *Бердяев Н.А.* Смысл истории. Новое средневековье. – М.: Kanon+, 2017. – С. 219-251.

3. *Гиренок Ф.И.* Удовольствие мыслить иначе. – М.: Проспект, 2021. – С. 220-221.

4. *Иванов В.В., Малинецкий Г.Г.* Россия: XXI век. Стратегия прорыва. Технологии. Образование. Наука. – М.:URSS, 2020. – 304 с.

5. Список языков по количеству носителей. – URL: https://yandex.ru/turbo/ru/wikipedua.org/s/wiki/список_языков_по_количеству_носителей (дата обращения 15.10.2021).

6. Коронавирус статистика. – URL: https://yandex.ru/covid19/stat?utm_source=main_graph&geld=225(дата обращения 15.10.2021).

7. *Малинецкий Г.Г.* Риски, эпидемии и образ будущего // Человек. – 2020. – Т.31. №4. – С. 57-82.

8. Эксперты предсказали сокращение числа больниц до уровня 1913 года. – URL: https://www.rbc.ru/society/07/04/2017/58e4feb59a794722462a85aa (дата обращения 15.10.2021).

9. *Schwab K., Malleret T.* COVID-19: The Great Reset. – Cologny/Geneva: World Economic Forum, 2020. – 213 p.

10. *Капица С.П., Курдюмов С.П., Малинецкий Г.Г.* Синергетика и прогнозы будущего: Образование. Демография. Проблемы прогноза. Кн. 2. – М.: URSS, 2020. – 384 с.

11. *Аганбегян А. Ершов М.* Нет длинных денег – нет роста. – URL:
https://yndex.ru/turbo/vedomostu.ru/s/economics/articles/202/09/08
(дата обращения 15.10.2021).

12. «Денационализация российской элиты. – URL: htps://yandex.ru/turbo/topwar.ru/s/152222-denacionalizacija-jelity.html (дата обращения 15.10.2021).

13. Запасы нефти в мире по странам. Список 2021. Доказанные запасы. Карта. – URL: нефть-газ-ископаемые.рф (дата обращения 15.10.2021).

14. *Сиренко С.Н.* Образование в Союзном государстве в цифровую эпоху: международный опыт и направление модернизации / Проектирование будущего. Проблемы цифровой реальности: труды 3-й Международной конференции (6-7 февраля 2020 г. Москва). – М.: ИПМ им. М.В.Келдыша, 2020. – С. 200-210.

15. *Малинецкий Г.Г.* Наука и стратегия развития России // Знание. Понимание. Умение. – 2021. – №3. – С. 26-44.

Цыганов В.В.

Механизмы общественной безопасности на основе искусственного интеллекта

Аннотация: Предложены механизмы нормирования и стимулирования повышения эффективности властей в интересах общества на основе искусственного интеллекта.

Ключевые слова: общество, власть, искусственный интеллект, машинное обучение, человеческий фактор, COVID-19

В работе [1] рассматривалось влияние пандемии COVID-19 на изменения технологии, культуры и общества. Этими и подобными изменениями, как всегда, стремится воспользоваться мировая закулиса. В книге «COVID-19: великая перезагрузка» [2] идеолог

глобализма, глава Давосского клуба Клаус Шваб раскрывает ее планы построения нового миропорядка: «не надейтесь, возврата к жизни до COVID-19 не будет». Новый мировой порядок предполагает проект т.н. «инклюзивного поведения», в котором упраздняется суверенитет государств, а управлять миром будут структуры т.н. «мирового правительства». Все страны и народы должны смириться с новым образом жизни, предполагающим полный контроль общества с помощью цифровых технологий искусственного интеллекта (ИИ). Способы контроля над людьми с помощью ИИ были отработаны и отрепетированы в 2020-2021 годах. Сегодня с помощью ИИ возможен контроль над людьми, не доступный ни одному тоталитарному режиму прошлого. Даже в США консерваторы заговорили о цифровом концлагере.

И сегодня Россия – главное препятствие на пути человечества к светлому будущему инклюзивного капитализма. Но серьезная опасность для России заключается в том, что и внутри страны есть силы, которые не прочь поучаствовать в строительстве нового инклюзивного капитализма с его тотальным цифровым контролем над гражданами и обществом в целом.

В связи с этой проблемой, представляется весьма актуальной разработка систем, структур и механизмов общественной безопасности и противодействия этим планам. Фундаментальной их основой может стать теория гуманитарных систем, с ее высокими гуманитарными технологиями и адаптивными механизмами [3]. Некоторые методы ее использования для обеспечения общественной безопасности описаны в монографии [4].

На практике, особенно важна международная солидарность, объединение всех здоровых сил как национальных обществ, так и мирового сообщества. Например, эта проблема сегодня является центральной для издаваемого в Великобритании журнала «Искусственный интеллект и общество» («AI & Society»). Авторы из связанного с ним мирового научного сообщества публикуют много статей, посвященных этой проблеме (см., например, обзор [5]).

В частности, пути решения вышеуказанной проблемы на основе теории гуманитарных систем рассматриваются в статье [6], на примере использования ИИ для общественного контроля деятельности властей, политиков и чиновников в деле закупок

жизненно важного товара (такого как вакцина от COVID-19). Исследуется проблема обеспечения политической стабильности социальной системы при нехватке такого товара. В такой системе члены общества – граждане оценивают власть, в зависимости от закупок этого товара. А именно, действия власти по увеличению закупок вызывают одобрение граждан и, следовательно, способствуют политической стабильности. Но на эти закупки влияют случайные факторы, действия конкурентов, мировая закулиса и др. Поэтому граждане не имеют достаточной информации обо всех возможностях закупок, и им сложно принимать адекватные решения. Такая неосведомленность граждан может использоваться недобросовестными политиками для достижения личных целей (например, для таких закупок, которые способствуют сохранению или приобретению влияния в мировой закулисе). Пример – блокирование Еврокомиссией закупок российской вакцины «Спутник-V» в Европейском Союзе (ЕС), в условиях дефицита вакцины против COVID-19 в ЕС в 2020г. и в первой половине 2021 года. Другой пример – блокирование властями Украины использования российской вакцины «Спутник-V», в условиях отсутствия вакцины против COVID-19. Следовательно, необходимо организовать общественный контроль, чтобы мотивировать политиков использовать все имеющиеся возможности в снабжении таким жизненно важным товаром, как вакцина против COVID-19.

Задача работы [6] – исследование и разработка такого цифрового механизма общественного контроля властей со стороны граждан, который бы лучше всего оценивал и стимулировал действия властей по закупкам жизненно важного товара. Такой контроль в условиях неопределенности, в эпоху ИИ, может быть основан на машинном обучении. При этом необходимо учитывать человеческий фактор, и моделировать деятельность политиков, связанную с наличием их собственных целей, не обязательно совпадающих с целями общества. Такие политики могут использовать закупки для достижения своих целей, используя процедуры машинного обучения граждан.

Эта задача работы [6] решается путем анализа и синтеза оптимального цифрового механизма общественного контроля деятельности властей в двухуровневой модели социальной системы

– цифровом обществе. На верхнем ее уровне находится член цифрового общества – независимый Гражданин, который дает оценку Политику, находящемуся на нижнем уровне. В свою очередь, Политик определяет закупки жизненно важного товара. Политическая стабильность гарантируется, если Гражданин регулярно одобряет действия Политика по управлению закупками. Но, для достижения личных целей (например, обусловленных влиянием мировой закулисы), Политик может не использовать имеющиеся у него возможности закупок (как власти ЕС и Украины в приведенных выше примерах).

Чтобы избежать этого, разработан механизм контроля Политика со стороны Гражданина на основе ИИ. Он включает в себя процедуру машинного обучения Гражданина, а также процедуру оценки активности Политика. Найдены достаточные условия для синтеза такого механизма управления Политиком со стороны Гражданина, при котором Политик заинтересован в использовании всех (в том числе – случайных) возможностей увеличения закупок товара. Функционирование такого механизма контроля иллюстрируется на примере вакцинирования в Англии (рисунок 1). Члену общества (гражданину) ежедневно доступны официальные данные о числе англичан, вакцинированных в день t, где t – день и месяц 2021 года (черная линия на рисунке 1(a)). Гражданин рассчитывает суточную норму оценки властей Англии, ответственных за вакцинацию, с помощью процедуры машинного обучения [6] (синяя линия на рисунке 1a). Ежедневный рейтинг властей Англии, ответственных за вакцинацию (розовая линия на рисунке 1(b)) определяется путем сравнения данных суточной вакцинации и нормы.

В работе [7] подобный подход, основанный на теории гуманитарных систем, применяется для обеспечения безопасности социально-экономической системы при дефиците жизненно необходимого товара (такого как вакцина от COVID-19). При этом власти, политики и чиновники имеют возможность влиять не только на закупки, но и на производство этого товара. Одобрение гражданами действий властей по увеличению его производства и предложения способствует политической стабильности. В условиях неопределенности, управление безопасностью такой социально-экономической системы может быть основано на таких процедурах

ИИ, как цифровая адаптация и машинное обучение. При этом, как и в работе [6], необходимо учитывать активность элементов социально-экономической системы, связанную с наличием их собственных целей, не совпадающих с целью системы в целом. Примеры – запреты властей ЕС и Украины на приобретение лицензий и производство российской вакцины «Спутник-V» на подведомственных территориях, в период острого дефицита вакцин.

Рисунок 1 – a) суточное количество вакцинированных q_t (черная линия) и норма оценки властей, ответственных за вакцинацию p_t (синяя линия), в миллионах человек; b) ежедневный рейтинг r_t властей, ответственных за вакцинацию (розовая линия)

Для решения этой проблемы рассмотрена трехуровневая модель социально-экономической системы. На ее верхнем уровне находится член общества – Гражданин, который дает оценку Политику, находящемуся на среднем уровне системы. В свою очередь, политик может влиять на увеличение предложения жизненно важного товара, включая как его закупку, так и производство на местном предприятии, относящемся к нижнему уровню системы. Политическая стабильность гарантируется, если гражданин регулярно одобряет действия политика по увеличению этого предложения.

Но менеджмент предприятия лучше Политика знает собственный производственный потенциал. Таким образом, этот менеджмент может манипулировать объемом собственного производства, чтобы получить больше поддержки со стороны Политика и Гражданина. Со своей стороны, Политик также может не использовать доступные ему возможности воздействия на менеджмент для достижения личных целей (например, в угоду либеральным принципам свободного рынка, продвигаемым той же мировой закулисой в целях неограниченного обогащения).

Чтобы избежать этого, разработан иерархический механизм социально-экономического контроля, включающий экономическую и политическую подсистемы [7]. Экономическая включает в себя процедуру адаптивного прогнозирования производства, а также процедуру поддержки предприятия. Политическая включает в себя процедуру машинного обучения Гражданина, а также процедуру оценки активности Политика. Найдены достаточные условия для синтеза такого социально-экономического механизма управления, при котором используются все случайные возможности увеличения предложения жизненно важного товара, включая как его закупку, так и производство на местном предприятии. Пример такого социально-экономического механизма рассмотрен на примере вакцинирования в Великобритании [7].

Возможный путь реализации описанных выше механизмов социальной безопасности – разработка соответствующих приложений для смартфонов. При массовой их установке на смартфоны граждан политикам, властям и чиновникам придется постоянно следить за этими рейтингами и стремиться их повышать. А поскольку в оптимальных механизмах контроля рейтинги повышаются с ростом эффективности, то политики, власти и чиновники будут стремиться улучшать свою работу, максимально используя все возникающие возможности (в том числе случайные).

Таким образом, воздействуя на национальные власти, политиков и чиновников с помощью описанных выше механизмов, общество может стимулировать активное сопротивление национальной политической элиты планам мировой закулисы по формированию инклюзивного капитализма.

Литература:

1. *Цыганов В.В.* Пандемия, технологии, культура и международная стабильность / Материалы XXVIII международной конференции «Проблемы управления безопасностью сложных систем» (16 декабря 2020 г. Москва). – М.: ИПУ РАН, 2020. – С. 48-53.

2. *Schwab K., Malleret T.* COVID-19: the great reset. – Geneva: Forum Publishing, 2020. – 213 p.

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

4. *Цыганов В.В., Шульц В.Л.* Социология общественной безопасности. – М.: Наука, 2014. – 415 с.

5. *Gill K. S.* The trappings of AI Agency // AI & SOCIETY. – 2020. – Vol. 35. – P. 289-296.

6. *Tsyganov V.V.* Artificial intelligence, public control, and supply of a vital commodity like COVID-19 vaccine // AI & SOCIETY. – 2021. doi 10.1007/s00146-021-01293-y.

7. *Tsyganov V.V.* Adapting, learning, and control the production of a vital commodity such as COVID-19 vaccine / Communications in Computer and Information Science. – Springer, 2021. – Vol. 1448. doi 10.1007/978-3-030-87034-8_2.

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

Анализ фактора неопределенности в процессе подготовки управленческих решений

Аннотация: Рассматривается комплекс проблем оценки влияния неопределенности на качество принятия управленческих решений. Приведена укрупненная классификация видов неопределенности. В качестве одного из путей решения проблемы снижения влияния неопределенности на эффективность решений предлагается использование технологий сценарного анализа.

Ключевые слова: управление, неопределенность, управленческое решение, сценарный анализ, моделирование

Введение

Анализ видов имеющейся неопределенности является важным этапом, во многом определяющими эффективность и результативность разрабатываемых управленческих решений, особенно на длительном временном горизонте. При этом одной из центральных проблем повышения эффективности процессов принятия решений является высокий уровень сложности разработки методов и механизмов выявления потенциальных источников неопределенности, а также оценки их воздействия на процессы развития объекта управления.

В настоящее время вследствие многогранности факторов неопределенности в организационном управлении, методология ее оценки развивается в основном в направлении разработки методов решения достаточно «узких», т.е. ограниченных рамками выбранных сегментов исследуемых предметных областей прикладных задач. При этом для решения рассматриваемых проблем используется широкий арсенал различных подходов, а также применяются разнообразные классы различающихся по методам формализованного описания свойств и характеристик неопределенности математических моделей: классические вероятностно-статистические, стохастические, нечетко-множественные, игровые, экспертные, детерминированные и т.д.

В то же время попытки разработки универсальных методов оценки влияния неопределенности на эффективность управленческих решений сталкиваются со значительными объективными трудностями, преодоление которых во многом возможно с использованием методологии сценарного анализа [1].

1. Анализ неопределенности как ключевого элемента подготовки решений

Несмотря на общепризнанность существования источников неопределенности при решении широкого круга задач организационного управления, пока практически отсутствует единая точка зрения в отношении их характеристик, методов оценки и механизмов снижения их влияния на конечный результат реализации управленческих решений. В настоящее время отсутствует также и единое определение неопределенности, поскольку данный термин

обычно привязывается к понятийному аппарату исследуемой предметной области и отражает специфику решаемых задач [2].

В соответствии с целью настоящих исследований будем рассматривать неопределенность как наличие фактора случайности, частичное или полное отсутствие, неполноту или неточность исходной информации о структуре и возможных состояниях объекта управления и (или) внешней среды, а также об условиях реализации решения, вследствие чего не представляется возможным достоверно и однозначно оценить ожидаемые результаты и возможные последствия. Фактически данное определение интерпретирует неопределенность как недостаток знаний и отражение свойства труднопредсказуемости характера внутренней изменчивости объекта управления или воздействия на его развитие (функционирование) внешней среды (что связано с человеческим фактором, а также динамикой институциональных, политических, социальных, экономических, технологических, природных и т.д. процессов и явлений).

Как следствие, процесс принятия решений усложняется многовариантностью как исходных условий, так и самих решений, причем вырабатываемые альтернативы могут во многих случаях оказываться эффективными только для определенного сочетания исходных условий, наступление которых предугадать крайне сложно (если вообще практически возможно).

В стратегическом планировании и управлении выделяют четыре базовых уровня неопределенности, которые можно интерпретировать следующим образом [3, 4]:

- низкий, практически не влияющий на типовые процедуры при выработке управленческого решения;
- средний, требующий определенного пересмотра ряда традиционных подходов и процедур разработки и оценки эффективности управленческих решений;
- высокий, требующий разработки и применения принципиально новых подходов и процедур при выработке решений;
- сверхвысокий, находящийся за границами понимания специалистов и ЛПР (лиц, принимающих решения) и требующий дополнительных аналитических исследований предметной области.

Среди всех видов неопределенности обычно выделяют виды, отражающие прямые связи в процессе управления, и виды, отражающие обратные воздействия и эффекты. Каждый из данных видов неопределенности порождает комплекс присущих ему проблем и предполагает совокупность специфических методов его анализа.

2. Классификация основных видов неопределенности

Несмотря на то, что в настоящее время разработано множество типологий неопределенности для различных целей, единая классификация практически отсутствует, что связано, как уже упоминалось выше, с тем, что сам рассматриваемый термин интерпретируется по-разному в зависимости от характера и специфики решаемых задач поддержки принятия решений (политика, экономика, финансы, право, социальная сфера, экология, информатизация, производство, наука, образование и т.д.) [2].

Один из возможных подходов к формированию укрупненной типологии неопределенности, непосредственно влияющей на качество подготовки и результативность реализации управленческих решений иллюстрируется на рисунке 1.

Неопределенность знаний об объектах управления, внешней среде и протекающих процессах в исследуемой системе представляет собой ключевой вид неопределенности, который фактически проистекает из двух основных источников [5]:

1. Субъективный (эпистемологический) источник представляет собой результат недостатка знаний, необходимых для принятия решений (уровень данной неопределенности может быть снижен дополнительными исследованиями или самостоятельного получением ЛПР новых знаний, привлечением экспертов и т.д.);

2. Объективный (алеаторный, онтологический) выступает следствием стохастической природы объекта управления или исследуемых процессов (влияние данного источника неопределенности крайне сложно поддается снижению и требует применения технологий сценарного анализа для оценки эффективности принимаемых решений или возможных ущербов).

Отдельный класс составляет лингвистическая (субъектная) неопределенность, которая обусловлена рядом объективных свойств естественного языка (расплывчатость, двусмысленность,

контекстная смысловая зависимость и т.д.). Лингвистическая неопределенность порождается, с одной стороны, множественностью значений слов (понятий и отношений) языка (полисемией или лексической многозначностью), с другой, – неоднозначностью (многозначностью) смысла фраз.

Рисунок 1 – Классификация основных видов неопределенности

Рассматриваемый вид неопределенности наиболее рельефно проявляется при использовании естественного языка с целью

отображения исходной информации, необходимой для принятия решений

Практически каждый из вышеперечисленных источников вносит свой «вклад» и отражает различные аспекты интегральной неопределенности, с которой сталкивается ЛПР при подготовке управленческих решений. На практике достаточно часто крайне сложно определить, какой вид неопределенности можно существенно снизить с использованием различных методов и механизмов анализа и исследования предметной области, а какой является несводимым (т.е. неотъемлемым свойством рассматриваемых явлений и процессов на объекте управления и во внешней среде). В любом случае, оценка неопределенности является важнейшим этапом процесса подготовки, в первую очередь, стратегических и нацеленных на долгосрочную перспективу решений, поскольку оказывает существенное влияние на их эффективность и результативность.

Заключение

Одним из путей комплексного решения проблемы снижения влияния неопределенности на эффективность решений является использование технологий сценарного анализа, позволяющих исследовать самые разнообразные по своей природе и взаимозависимые процессы и явления, определяющие развитие объекта управления, что принципиально позволяет в процессе синтеза сценариев учитывать результаты прогнозирования значений отдельных параметров модели с использованием «внешних» по отношению к сценарной системе средств моделирования.

Одновременно с этим данное расширение функциональных возможностей сценарного анализа требует дальнейшего развития теоретических и прикладных мультидисциплинарных исследований в области разработки методологии сценарного анализа, а также технологий автоматизации процессов интегральной оценки неопределенности при принятии решений.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта 18-29-16151 «Разработка методов управления процессами трансформации права в условиях цифровой технологии»

Литература:

1. 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.

2. *Magruk A.* Uncertainties, knowledge, and futures in foresight studies – A case of the Industry 4.0 // Foresight and STI Governance. – 2020. – Vol. 14. № 4. – P. 20-33.

3. *Хортни Х., Керкленд Дж., Вигери П.* Стратегия в условиях неопределенности // Экономические стратегии. – 2002. – №6. – С. 78-85.

4. *Капустин В.Ф.* Неопределенность: виды, интерпретации, учет при моделировании и принятии решений // Вестник Санкт-Петербургского университета. Сер. 5. – 1993. – Вып.2 (12). – С. 108-113.

5. *Ascough II J.C., Maier H.R., Ravalico J.K and Strudley M.W.* Future research challenges for incorporation of uncertainty in environmental and ecological decision-making // Ecological Modelling. – 2008. – №219 (3-4). – P. 383-399.

6. *Шульц В.Л., Любимова Т.М.* Язык как конструкт реальности и сверхреальности. – М.: Наука, 2019. – 288 с.

7. *Мартынова И.А.* Трактовка понятия «неопределенность» в лингвистике: обзор и оценка существующих теорий / Сб. статей победителей VII Межд. научн.-практ. конкурса. – Пенза: Изд-во «Наука и просвещение», 2017. – С. 129-135.

Bachtadze N., Zaikin O., Żylawski A.

Team collaboration model of a project learning process

Abstract: The ability to create the project team and manage their knowledge is commonly recognized as one the most important quality of the knowledge and innovative organization. The management of knowledge and skills, as well as the management of project competencies has turned out to be essential factors influencing performance of project process. In the paper, the authors present the method and tools for incentive modelling for project knowledge management. The kind of open distance learning systems is represented, that can be used as a model of project process aimed at active behaviour of

students in the project development of not only knowledge, but also acquiring of competencies.

Keywords: project learning process, incentive model, project team, competence management, game theoretical model, repository development

1. Introduction

The ability to create the project team and manage their knowledge is commonly recognized as one the most important quality of the knowledge and innovative organization. The management of knowledge and skills, as well as the management of project competencies has turned out to be essential factors influencing performance of project process. In this paper, the method and tools for incentive modelling for project knowledge management is presented. Also the kind of educational systems is examined, that can be used as a model of project learning process aimed at active behaviour of students in the project development of not only knowledge, but also acquiring of competencies.

In open distance learning (ODL) conditions, as an incentive model we consider scenario of a game (interaction, interplay) between the teacher and the students/project team, conducted in a specific education situation and oriented on performing the actions which allow to raise the level of student's involvement in subject-specified task realization and to extend the repository with complex tasks performed in the project (Zaikin et al., 2016).

The project process in every education situation includes the didactic, research and education aspects and takes place at the following levels: cognitive, information and computer-based (Gomez-Perez et al., 2004). At each of these levels the teacher and the students (participants of project team) have their own roles corresponding different competencies in the project and involvement intensity. At the cognitive level assumptions are made and tasks are solved. At the information level the information is exchanged between the participants of the project learning process. The computer-based level is characterized by repository organization and ability to use it. The role of the teacher is to develop an ontological model reflecting the project of the education situation, showing the source of information, formulating tasks and presenting methods and examples of their solutions. All ontological models are stored in the repository (Różewski et al., 2011).

In the discussed approach the project tasks are created on the basis of the ontology and differ in their complexity level (Kushtina, 2006). The proposed scenario assumes that the role of the student is to choose a set of project tasks relevant to his/her competence and solve it. The final grade depends on the correctness of the solution and the complexity level of the tasks. The project tasks solved by the student team and highly graded by the teacher is placed in the repository and will serve as an example solution for other students. All materials stored in the repository are copyrighted. This way the students of the project team participate in the didactic activity and we assume that it will raise his/her self-esteem, what has a positive influence on learning, meaning that it will be a part of the project team reward function. At the same time filling the repository with a wide spectrum of high quality solved project tasks gives satisfaction to the teacher, for his/her laborious, requiring intelligent efforts of preparing the repository and this will make up the *teacher's reward function* (Small and Venkatesh, 2000).

Teacher's and students' interaction with the repository can have a research character. We assume that thematically the content of the repository is in concordance with the teacher's scientific-research interests, what causes appearance and extension the repository with the tasks differing from the complexity level. For helping to solve project tasks stored in the repository, the teacher will pay more attention and spend more time with the students. We can assume that for a certain part of students participation in common research is a challenge and the obtained results are an extra added value (Miller and Brickman, 2004).

The educational aspect is reflected in the *repository development* as a common success of all participants of the project process. Making the material copyrighted shows and visualizes the contribution and involvement of each participant of the project. Feeling the synergy effect motivates to develop collaboration skills and tolerance. Collaboration in distance conditions requires a more logical formulation of questions and answers. All this reflects the interests of both the teacher and the students (Tuckman, 2007).

2. Organization of team collaboration in developing the project

The problem of organizing the team collaboration in project learning process is very similar to the problem of selecting staff for project

development, when the project goal, time and financial limitations have already been established.

The project's success guarantee consists of:

1) Sufficient summary competences of specialists involved in the project.

2) The way they are organized (specific scenario, game model).

3) Assessment of information certainty that participants will be able to use both outside and inside the project through mutual communication.

The development of a formal model that will take into account the listed constituent factors is complicated and needs an explanation of the source that predetermines the scale of specialists' competence or a description of how to describe them. In innovative situations, which include the problem of developing a project in ODLS conditions (the need to respond to market requirements), it is not possible to rely on a fixed scale of competences with an orientation on graduate profiles.

For this it is important to find the right method to determine the required competences. The selection of competent partners, regardless of the criterion for assessing the results of solving this problem, should be considered within the framework of motivational management. Motivational management (as opposed to institutional and information management) consists in creating a stimulation system aimed at achieving maximum competences at a minimum cost.

Tasks of this type are considered in game theory (Owen, 1975). An analysis of the interests and goals of participants in the process of developing a project shows that the solution to this problem can be implemented in the form of a cooperative game, where the players' goal is the aggregate profit of a stable coalition (Malawski et al., 2004). Methods of team creation for the consortium implementing scientific research project involve the use of multiple criteria decision making. One of them is the criterion of having competences. In the analysis of the criterion the teams-candidates for the project are compared from point of the view of having competences required to solve the task. The teams, which have all the competences necessary to execute the project are preferred. If the team does not have all the required competence must incur a cost related with getting the missing knowledge and skills. It can be stated that the usefulness of the team according to criterion of having competence is inversely proportional to the cost of obtaining the missing

competencies required for effective implementation of the task (Różewski and Zaikin, 2015).The model of the process, which use an analysis of the cost expansion of the ability of person or team is shown in figure 1.

The whole process of determining the cost of the missing competence consists of three stages:

1) identification of a set of competencies required for the task.

First, based on the description of objective and scope of task, all the competencies needed to effectively implement it must be identified. In the simplest case, if the task of the project is one of the typical frequently realized tasks is possible to find standardized competencies using one of the existing standards or norms. When the task is atypical and any standards of competence does not exist, the skills necessary to implement this task may be identified through expert analysis. The expert making analysis may base to their own experience and various sources of knowledge in the field of the task. These can be all kinds of books, articles, compendia of knowledge, whose analysis can help identify the typical competencies related to task domain. For example, the competencies related to solving mathematical problems or solved using mathematical methods can be identified on the basis of the Classification of mathematical terms (called Mathematics Subject Classification) which categorizes as taxonomic mathematical discipline (American Mathematical Society, 2000);

2) identification of a set of competencies having by the team.

On the basis of a set of competencies required to complete the task identified at the first stage it is then possible to identify these competencies in teams-candidate. This can be achieved by analysing their experiences in the form of previously completed projects, experimental research, publications, reports and so on. The most reliable source of knowledge about the competence of the team is to analyse the formal qualifications of its members, or obtained diplomas, degrees, certificates of completion of training, etc;

3) determining the cost of obtaining the missing competencies required for the task.

Quantitative analysis of the cost extension of the competencies by comparing the sets of the competence of the team with the set of skills required to accomplish the task. This analysis is performed using mathematical models of competence outlined in section 2. The costs of

extension of the competencies for each team-candidate are used for comparing them according to the criterion of having competencies in the proposed method of choice of teams for the consortium.

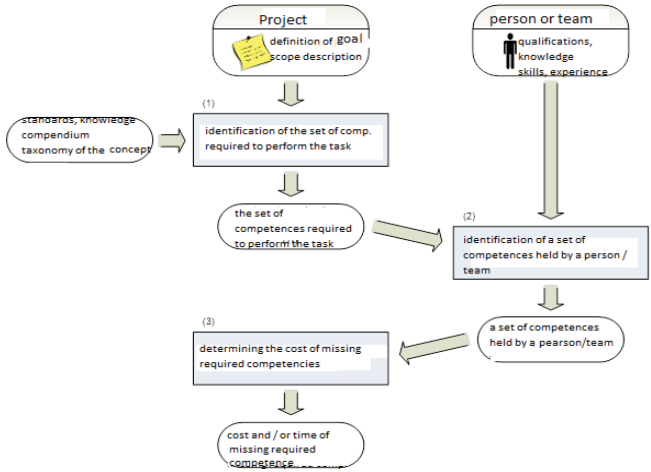


Figure 1 – Model of process to analyse the competence to perform a project

3. Team collaboration model and competence expansion algorithm to perform the project task

Basic components of the project situation

a) $\{P, N^P, S^P\}$ - participants of the project situation,

where N^P – co-ordinator of project P, $S^P = \{s_k\}$ -project team, where $k=1,2,...k$ - index of team participant.

b) $\{p, C^P, G^P\}$ - ontological/hierarchical graph of the project domain (figure 2),

where p – is a root vertex of the graph $C^P = \{c_1^p, c_2^p, ...c_{i*}^p\}, i = 1,...i*$ – competence portions of the project / subordinate nodes of the ontology graph, $G^P = \{G(c_1^p), G\{c_2^p\}, ...G(c_{i*}^p)\}$ – a set of tasks, having to solve in the

project, $G(c_i^p) = \{g_1^i, g_2^i, ...g_{j*}^i\}, j = 1,....j_i*$ - subordinate tasks of the project competence c_i^p,

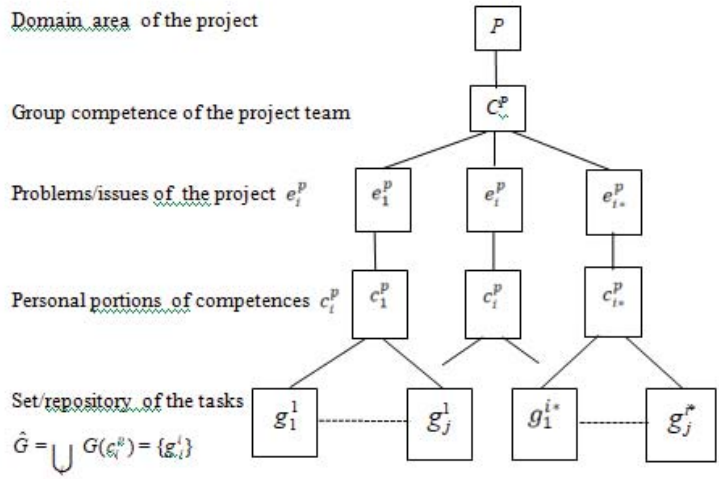


Figure 2 – Hierarchical graph of the project domain

c) $\hat{G} = \bigcup_i G(c_i^p) = \{g_j^i\}$ -set/repository of the tasks,

where g_j^i – task *'j'* consisting for competence portion c_i^p,

$j=1,....j_i^*$ – index of task

$i=1,...,i^*$ – index of acquired competence,

d) $q(g_j^i), j = 1,....j*, i = 1,...i*$ – degree of complexity of a task, which can be expressed in numerical scale (depends on number of concepts included in the task, solution method, etc.)

$0 \le q(g_j^i) \le 1$

e) $R_g^q = r(e_i^p, g_j^i), j = 1,....j*, i = 1,...i*$ – relationships between the vertices of the graph *P*

If the task g_j^i is a *base task* of the problem e_i^p, then between them exists the *relationship* $r(e_i^p\ g_j^i)$ of value

$0 \le r(e_i^p, g_j^i) \le 1$

f) Power of personal competence required for solution of the problem

is determined on *the principle of maximum*

$\alpha(c(e_i^p)) = \underset{j=1,..j*}{Max}\ (c(g_j^i)\, r(e_i^p, g_j^i))$

g) Minimal potential of personal competence, required for solution of the problem

$\beta(c(e_i^p), i = 1,.... i*$

h) Relation of a project and problems

$R_i^P = \{r(p, e_i^p)\},\ \ i = 1,.... i*$

If the problem e_i^p is a *base problem* of the project *P*, then between them exists the *relationship* $r(p, e_i^p)$ of value $0 < r(p, e_i^p) \le 1$.

i) Power of group/team competence required for solution of the project

$\alpha(c^p) = \underset{j=1, j*}{Min}\ (c(e_i^P)\, r(p, e_i^p))$

is determined on *the principle of minimum*

Decision variables:

a) Project team $S^P = \{s_k\}$, where *k=1,2,...k**- index of project participant.

Numerical characteristics of the project participant:

$\alpha(c(s_k))$ - power of competence of participant $s_k \in S^P$

$\beta(c(s_k))$ -potential of competence of participant $s_k \in S^P$

b) Matrix of assignment of the project problems/issues to participants of project team

$$H = h(\| e_i^p, s_k \|, i = 1,... i^*, s = 1,.... s^*$$

,

where

$$h(e_i^p, s_k) = \left\{ \begin{array}{l} \varepsilon 1, if\ the\ problem\ e_i^P\ is\ assigned\ to\ participant\ s_k \\ 0, otherwise \end{array} \right\}_{\tau}$$

Constraints on decision variables

Relation one-to-one of the project problems and team participants

$$\lambda_{s_k \in S} h(e_i^p, s_k) = 1 \qquad \lambda_{q_i \in Q^P} h(e_i^p, s_k) = 1$$

i.e. only one problem assigned to one participant and vice versa.

Criteria

3 kinds of individual competence:

1) The power of person competence more required competence of the problem

$$\alpha(c(s_k)) \lambda\ \alpha(c(e_i^P), s_k \in S_1, e_i \in E_1$$

It is no important potential of the person $\beta(s_k)$ and minimal potential of personal competence $\beta(c(e_i)$, required for solution of the problem. Here no cost and time are required for solving the problem e_i

2) The power of person competence less required competence of the problem

$$\alpha(c(s_k)) < \alpha(c(e_i^P)$$

and potential of the person $\beta(s_k)$ more minimal potential of personal competence $\beta(c(e_i)$, required for solution of the problem

$$\beta(s_k) > \beta(c(e_i)$$

Here some cost and time are required for solving the problem e_i

$$f[\alpha(c(e_i^P)) - \alpha(c(s_k)], s_k \in S_2, e_i \in Q_2$$

3) The power of person competence less required competence of the problem/issue

$$\alpha(c(s_k)) < \alpha(c(e_i^P)$$

and potential of the person $\beta(s_k)$ less minimal potential of personal competence $\beta(e(q_i)$, required for solution of the problem $\beta(s_k) < \beta(c(e_i)$

Here additional efforts are required to increase the potential of the person and after it some cost and time are required for solving the problem e_i

$$f[\alpha(c(e_i^P)) - \alpha(c(s_k)]s_k \in S_3, e_i \in E_3$$

Therefore the criterion is the following

$$f = f_1 + f_2 + f_3 = \sum_{s_k \in S_1} \sum_{e_i \in E_1} h(e_i^p, s_k) \times 0 +$$

$$\sum_{s_k \in S_2} \sum_{e_i \in E_2} h(e_i^p, s_k) f[\alpha(c(e_i^P)) - \alpha(c(s_k)]] +$$

$$+ \sum_{s_k \in S_3} \sum_{e_i \in E_3} h(e_i^p, s_k) f[\alpha(c(e_i^P)) - \alpha(c(s_k)] + g[\beta(c(e_i) - \beta(s_k)]$$

Conclusion

1. To summarize the above considerations, competence is a general concept, which defines the ability to perform different patterns of behaviour based on accumulated knowledge and experience. While the qualifications relate to all kinds of formal evidence confirming possessing by person the specific knowledge and skills. Simply put, the qualification is formal evidence of specific competences.

2. Computer-aided management of human resources in the project requires the use of formal model of competence, which enables to quantify the usefulness of the research team to participate in the project. The above definitions and integrated model of the competence reflect only the nature of the competence and don't provide tools for quantitative analysis of competence. In cases when exact quantitative analysis of competence is required, it is necessary to rely on a model that will provide mathematical foundations and tools to carry it out. This model can precisely describe the competences, their comparison, determining the cost of the competence increase, determination of the adequacy of the

competence of the individual to the aim of the tasks and to solve many other problems of a quantitative nature.

3. The results can be used by a decision-maker or, on the basis of the organization consisting of several organizational units. Basing on knowledge assessments of participants of the project or organizational units the method allows to estimate the cost of team's training necessary to meet the requirements of the project. The competence expansion costs are then used as criterions to assign project tasks to participants of the project defined. All steps of the proposed approach were illustrated in the case study, where it is proposed a practical method of team's knowledge estimation in the knowledge and innovative organizations.

References:

1. *Zaikin O., Tadeusiewicz R., Różewski P., Busk Kofoed L., Malinowska M., Żyławski A.* Teachers' and students' motivation model as a strategy for open distance learning processes // Bulletin Of The Polish Academy Of Sciences Technical Sciences. – 2016. – Vol. 64(4). – P. 943-955.

2. *Gomez-Perez A., Fernandez-Lopez M. and Corcho O.* Ontological Engineering. – Springer Press, 2004. – 420 p.

3. *Różewski P., Kusztina E., Tadeusiewicz R., Zaikin O.* Intelligent Open Learning Systems. Concepts, Models and Algorithms. – Berlin-Heidelberg: Springer-Verlag, 2011. – 257 p.

4. *Kushtina E.*Concept of open and distance information system (in polish). – Szczecin: Publisher house of Szczecin University of Technology, 2006.

5. *Small R. and Venkatesh M.* A cognitive-motivational model of decision satisfaction //Instructional Science: An International Journal of the Learning Sciences. – 2000 – Vol. 28(1). – P. 1-22.

6. *Miller R. and Brickman S.* A Model of Future-Oriented Motivation and Self-Regulation // Educational Psychology Review. – 2004. – Vol. 16(1). – P. 9-33.

7. *Tuckman B*. The effect of motivational scaffolding on procrastinators' distance learning outcomes // Computers & Education. – 2007 – Vol. 49(2). – P. 414-422.

8. *Owen G.* Game theory. – Warsaw: Polish Scientific Publishing House, 1975.

9. *Malawski M., Wieczorek A., Sosnowska H.* Competition and cooperation. Game theory in economics and social sciences. – Warsaw: Scientific Publishing House, 2004. (in Polish)

10. *Różewski P., Zaikin O.* Integrated mathematical model of Competence-based learning/teaching process // Bulletin of the Polish Academy of Sciences. Technical Sciences. – 2015 – Vol. 63. № 1. – P. 245-258. doi:10.151/bpasts-2015-0029

11. *Broens R., de Vries M.J.* Classifying technological knowledge for presentation to mechanical engineering designers // Design Studies. – 2003. – Volume 24. Issue 5. – P. 457-471.

Быстров В.В., Маслобоев А.В., Датьев И.О.

Инструменты цифровизации управления кадровой безопасностью регионального производственного кластера

Аннотация: Для повышения эффективности управленческой деятельности в сфере обеспечения кадровой безопасности социально-экономических систем разработан модельный и программный инструментарий информационного управления кадровой безопасностью региональной экономики. Созданы прикладные средства информационно-аналитической поддержки управления кадровой безопасностью регионального производственного кластера: прикладная онтология и предметно-ориентированный тезаурус кадровой безопасности, комплекс имитационных моделей прогнозирования кадровых потребностей, архитектура мультиагентной системы сетецентрического управления кадровой безопасностью для организации сервис-ориентированной цифровой платформы.

Ключевые слова: кадровая безопасность, управление, поддержка принятия решений, моделирование, региональный производственный кластер

Исследование направлено на решение актуальной научной проблемы повышения эффективности управления кадровой политикой региона с целью обеспечения баланса между спросом и предложением трудовых ресурсов для осуществления устойчивой

хозяйственной деятельности региональным производственным кластером в условиях возникающих негативных вызовов социально-экономического характера.

Объектом исследования является информационная инфраструктура распределенной системы управления кадровой безопасностью горно-химического кластера Мурманской области.

Целью исследования является разработка методологии и инструментальных средств информационно-аналитической поддержки управления кадровой безопасностью регионального горно-химического кластера на основе методов предсказательного моделирования (на примере Мурманской области).

Для решения задачи по созданию методических и программных средств информационно-аналитической поддержки управления кадровой безопасностью регионального производственного кластера применялся комплекс известных методов синтеза сложных динамических систем, а также подходов к сценарному анализу и прогнозированию динамики развития этих систем. По отдельности использованные в работе методы и подходы уже применялись для изучения широкого круга фундаментальных и прикладных проблем управления безопасностью сложных систем, однако их совместное использование в рамках настоящего исследования для решения поставленной задачи позволяет получить синергетический эффект. По мнению авторов, этот эффект проявляется в повышении адекватности и точности прогнозов, а также сокращении сроков их получения за счет создания и внедрения программных средств информационной поддержки управления кадровой безопасностью производственного кластера.

Большинство зарубежных и отечественных работ в области управления человеческими (трудовыми) ресурсами акцентируют свое внимание на таких вопросах как:

– рассмотрение ключевых проблем в управлении человеческими ресурсами и потенциальных способов улучшения региональной экономики за счет совершенствования механизмов управления кадровым обеспечением;

– построение прогнозов спроса и предложений на региональном рынке труда с помощью количественных и качественных методов экспертной оценки и методик статистического анализа ретроспективных данных (например, концепция Regional Strategic Human Resources Management);

– создание организационных систем управления кадровым обеспечением регионального развития (например, система управления региональными человеческими ресурсами, основанная на знаниях);

– разработка проблемно-ориентированных систем поддержки принятия решений в сфере управления персоналом на основе современных технологий проектирования и реализации сложных программных продуктов (например, системы поддержки принятия решений по управлению человеческими ресурсами на основе OLAP-технологий и хранилищ данных).

В ходе исследования разработаны следующие инструменты информационной поддержки управления кадровой безопасностью:

1. Прикладная онтология кадровой безопасности регионального производственного кластера, обеспечивающая интероперабельность данных и знаний при разработке распределенных систем поддержки принятия решений в сфере регионального управления. Онтология построена на основе формализованной концептуальной модели кадровой безопасности региональной экономики [1] и реализована на языке OWL в среде онтологического моделирования Protege. Онтология предназначена для комплексного представления структуры и задач управления кадровой безопасностью и связанных с этими задачами информационных процессов. Онтология кадровой безопасности содержит концепты и отношения, определяющие основные компоненты региональной социально-экономической макросистемы и отдельного производственного кластера, индикаторы системы оценивания состояния кадровой безопасности и их взаимосвязи, а также классификацию потенциальных угроз кадровой безопасности. При этом в качестве основных компонентов региональной социально-экономической макросистемы выделены сектора экономики региона, региональный рынок труда, региональная система подготовки и переподготовки кадров, региональная система управления кадровой политикой. Онтологическое описание производственного кластера содержит основные сущности и связи кадрового состава кластера, кадровой внешней и внутренней логистики кластера, системы подготовки кадров кластера.

2. Тезаурус кадровой безопасности горно-химического кластера для повышения адекватности и организации интеллектуальной

обработки собираемой информации о кадровых потребностях производственного кластера и возможностях региональных структур по их удовлетворению. Для этого предложено включить в перечень анализируемых источников информации социальные сети. Первоначальным шагом для организации процедур автоматизированной обработки неформализованной информации из социальных сетей является создание предметно-ориентированного тезауруса [2], содержащего основные понятия и термины, ассоциированные с кадровой безопасностью производственного кластера. Предметно-ориентированный тезаурус составлен в результате анализа профессиональных сообществ социальной сети «Вконтакте». Анализ сообществ (описаний сообществ, сообщений в сообществе и комментариев к ним) проводился в «ручном» режиме. Первоначальный необработанный тезаурус содержал более 1000 терминов, ассоциированных с кадровой безопасностью горно-химического кластера Мурманской области. После проведения обработки с привлечением коллектива экспертов мощность тезауруса была уменьшена до 500 терминов, а сам тезаурус был разбит на категории: предприятия кластера, профессии кластера, профессиональные термины, устоявшиеся выражения, организации системы подготовки кадров, профсоюзные организации кластера и др. Сформированный тезаурус используется в качестве справочника для организации процедур поиска и анализа информации из социальной сети «Вконтакте». При этом применяется три типа анализа текстовой информации, получаемой из социальной сети: синтаксический, семантический (на базе количественных методов оценки метрики семантического пространства), интеллектуальный (на базе нейросетевого подхода).

3. Комплекс программ автоматизированного направленного поиска и анализа неформализованной открытой информации в социальных сетях (на примере социальной сети «ВКонтакте»), ассоциированной с кадровой безопасностью производственного кластера региона [2]. Алгоритм работы комплекса программ по извлечению неформализованной информации из социальной сети сводится к выполнению следующих основных этапов:

1) задание конфигурации комплекса программ: определение перечня анализируемых профессиональных сообществ, задание

тезауруса-справочника, определение временных характеристик поиска (за какой хронологический период анализируются данные);

2) взаимодействие комплекса программ с социальной сетью;
3) формирование базы данных поиска;
4) анализ данных из сформированной базы данных поиска;
5) визуализация результатов поиска и обработки информации.

Хранение данных реализовано в виде СУБД Mongo DB и/или в отдельных файлах формата CSV (Comma-Separated Values). Взаимодействие комплекса с социальной сетью «Вконтакте» реализуется посредством отправки запросов через функции API социальной сети. Результаты выполнения запроса поступают из социальной сети в программный комплекс в формате JSON. Анализ данных сводится к преобразованию извлеченной информации в необходимые числовые значения для дальнейших вычислений. Например, формируются временные ряды индикаторов пользовательской активности – лайки, репосты, комментарии, просмотры. Комплекс программ разработан на языке Python в среде JupiterLab. Статистическая обработка данных выполнена с помощью модуля Statsmodels. Работа программного комплекса организована на платформе Debian Linux.

4. Сервис-ориентированная архитектура системы поддержки принятия решений по управлению кадровой безопасностью регионального производственного кластера [3], разработанная на базе интеграции принципов многоагентных и сервис-ориентированных систем с ориентацией на парадигму сетецентрического управления. Архитектура системы включает три уровня: организационный, виртуальный и концептуальный. Ключевым уровнем архитектуры является виртуальный, который реализуется в виде многоагентной сетецентрической программной среды, ориентированной на решение различных типов задач кадрового обеспечения производственного кластера. Виртуальный уровень представляет собой сетецентрическую структуру, состоящую из множества программных агентов, структур хранения данных и компонентов распределенной имитационной среды. Концептуальный уровень представляет собой формальное описание предметной области. Организационный уровень представляет собой совокупность организационных структур, принимающих прямое или косвенное участие в процессах, связанных с планированием,

реализацией и контролем действий, направленных на достижение целей обеспечения кадровой безопасности кластера.

Для организации взаимодействия между про-активными объектами сетецентрической системы используются принципы и стандарты разработки многоагентных и одноранговых распределенных систем, такие как: инкапсуляция, ведение каталога сервисов и агентов, использование провайдеров и координаторов, применение специальных интерфейсов и протоколов взаимодействия и другие.

Реализация системы управления кадровой безопасностью региона на основе сетецентрического подхода обусловлена особенностями этой системы [4], для которой характерны большие объемы передаваемых и обрабатываемых данных, разнородность элементов системы, перемещение центра принятия решения по сети и т.д. Сетецентрическая система поддержки принятия решений, имеющая предлагаемую архитектуру, позволяет эффективно организовать процесс управления кадровым обеспечением производственного кластера в условиях децентрализованного принятия решений, как обмен запросами и ответами между соответствующими агентами и веб-сервисами.

Представленные разработки позволят повысить оперативность и качество принимаемых управленческих решений в сфере обеспечения кадровой безопасности производственного кластера с учетом влияния разнообразных факторов.

Результаты исследования и сформированные на их основе рекомендации смогут найти применение при реализации Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности до 2035 года на территории Мурманской области.

Результаты получены в рамках выполнения государственного задания ИИММ КНЦ РАН. Практическая реализация разработок поддержана РФФИ (проект 19-07-01193-а)

Литература:

1. *Быстров В.В., Маслобоев А.В., Путилов В.А.* Информационно-аналитическая поддержка управления кадровой безопасностью арктических регионов (Методология и инструментарий) // Арктика: экология и экономика. – 2020. – №2(38). – С. 122-133.

2. *Datyev, I.O., Fedorov, A.M., Shchur, A.L., Bystrov, V.V.* Social Networking Services as a Tool for State and Regional Governance (On the Example of the Arctic Region) // Advances in Intelligent Systems and Computing. – 2019. – Vol. 1047. – P. 360-370

3. *Bystrov V.V., Khaliullina D.N., Malygina S.N.* Architecture of the Decision Support System for Personnel Security of the Regional Mining and Chemical Cluster // Advances in Intelligent Systems and Computing. – 2020. – Vol. 1294. – P. 442-463.

4. *Быстров В.В., Маслобоев А.В., Путилов В.А.* Информационно-аналитическая поддержка управления кадровой безопасностью арктических регионов (Приложения разработок на примере Мурманской области) // Арктика: экология и экономика. – 2020. – №3(39). – С. 126-140.

Нижегородцев Р.М.

Формализация институтов, неблагоприятный отбор и управление коррупционным поведением агентов

Аннотация: Предлагается институциональный подход к изучению коррупции как стоимостного преодоления нестоимостных институциональных барьеров. Обосновывается связь между формализацией институтов и проявлением рентоориентированного поведения, основанного на потребности в преодолении барьеров нестоимостного характера. Предлагаются рекомендации по управлению коррупционным поведением агентов, основанному на частичной легализации рентоориентированного поведения, частичной деформализации институтов принятия решений и сосредоточении на задачах управления рентоориентированным поведением, а не его искоренения.

Ключевые слова: формальные институты, рентоориентированное поведение, коррупция, ухудшающий отбор, принцип Диогена, нестоимостные барьеры входа

В настоящее время много законодательных актов посвящено вопросам коррупции. На законодательном уровне достаточно часто

и интересно это обсуждается, но, к сожалению, под этим нет серьезной экономической составляющей, нет серьезного экономического анализа – прежде всего, нет анализа тех причин, которые порождают соответствующее явление. Единственное, что могут сказать по этому поводу профессиональные юристы, – что коррупция связана с нелегальным присвоением доходов, а эти доходы обычно связаны с извлечением ренты. Для экономистов степень легальности доходов не столь важна, имеет значение происхождение доходов с институциональной точки зрения.

Вопросы легальности и нелегальности в большей степени относятся к компетенции юристов. С точки зрения экономики какие-то действия можно объявить легальными, какие-то нелегальными, отдельные алгоритмы действий выходит за пределы правового поля, но экономическая логика диктует необходимость наличия соответствующих локальных рынков. Агенты, принимающие решения, не всегда исходят из этой реальности, они нередко считают, что можно принять закон, и то, что в нем написано, будет работать так, как это написано. К счастью, это не всегда так. Жизнь организована сложнее, и недостаточно просто написать правила для того, чтобы они работали. И то, что запрещается правилами, чаще всего не исчезнет из жизни, а приобретет какие-то превращенные формы. Примером тому может быть прекращение авиасообщения между Россией и Украиной: предполагалось, что отказ от авиаперевозок позволит прекратить все контакты между странами, но вместо этого повысилась нагрузка на железнодорожное и автомобильное сообщение. Затем были приняты меры по значительному сокращению и этих перевозок, в результате организация соответствующих видов деятельности стала уделом частных структур, лишь частично контролируемых государством, повысился спрос на нелегальные перевозки, как пассажирские, так и грузовые. Формальные запреты не работают, потому что нельзя остановить экономику, которой требуется перемещение благ в виде товарных, финансовых и трудовых потоков [1]. Таким образом, неразумно ставить задачу пресечения или искоренения нелегальных или нежелательных (с точки зрения правительства) явлений и действий, более реальной задачей является управление ими.

С точки зрения экономики, коррупция – это преодоление стоимостным путем институциональных барьеров, имеющих нестоимостную природу.

Как уже упоминалось выше, степень легальности этого процесса вторична. Важно, что те или иные агенты проявляют рентоориентированное поведение. Это один из признаков коррупционной модели поведения, вопрос только в том, что рентные отношения возникают совершенно независимо от степени из легальности. Например, с точки зрения экономики неважно, оплачивается ли чиновнику исполнение его функций, или оплачивается услуга, которую он оказывает сверх его непосредственных обязанностей (а иногда и вопреки таковым). И в том и другом случае природа получаемого им дохода совершенно одинакова, этот доход имеет рентное происхождение. А степень его легальности совершенно различна, и законодательство к нему относится абсолютно по-разному.

Сторонники цифровизации считают, что цифровые технологии помогают избавиться от коррупции. Происходит это за счет сокращения числа посредников, которые ограничивают доступ к определенным благам и тем самым воздвигают барьеры входа. Исчезает функция и, следовательно, исчезают эти барьеры, но они исчезают посредством частичной легализации этих коррупционных отношений. Например, существует электронная очередь в дошкольное образовательное учреждение. Чтобы ребенок поступил в него раньше, чем это предусмотрено очередью, родители могут воспользоваться услугой платных групп, которые существуют в том же учреждении. До появления этого цифрового механизма требовалось договариваться с конкретным чиновником на месте, прибегая к коррупционным схемам. Сейчас же это переведено в официальные услуги с легальными тарифами на том же портале «Госуслуги». Но нестоимостные барьеры входа при этом преодолеваются стоимостным путем. Природа этого поведения не изменилась, это рентная природа, но цифровые механизмы позволили легализовать модели этого поведения. Официальная продажа «красивых», т.е. потенциально пользующихся повышенным спросом, госномеров автотранспорта относится к этому же разряду. Существуют легализованные виды рентных

отношений, которые имеют то же самое происхождение, что и абсолютно коррупционные, незаконные денежные доходы.

В работе почти любого учреждения, в том числе и государственного, такого рода возможности есть, существуют лазейки, которые позволяют легализовать прежде не считавшиеся легальными доходы. Они очень распространены, и на самом деле это логично, потому что существующие барьеры входа во многом избыточны и не оправданы реальной необходимостью.

Для общества нет никакого вреда от существования этих институтов, нацеленных на преодоление барьеров. Поэтому, вопреки распространенному мнению, оказание либо нелегальной услуги (то, чего нельзя), либо вполне легальной услуги, но нелегальным путем, представляет собой неучтенный дополнительный объем услуг и является прибавкой к ВВП, а не вычетом из него.

Существуют расчеты – сколько теряет бюджет от наличия коррупционных доходов. Идея этих расчетов в том, что если бы эти услуги оказывались легально, то бюджет получил бы некоторое количество доходов. Но существуют блага, которые нельзя предоставить легально, и нет легальных институтов, которые позволяли бы это сделать. В таких случаях остаются каналы только нелегальные. Поэтому прежде чем сказать, что это недополученные бюджетом доходы, нужно, как минимум, это проверить и, по нашему мнению, следует подвергнуть сомнению категоричность такого утверждения. На самом деле любая формализация институтов в том или ином виде вызывает рентоориентированное поведение и постольку порождает коррупционные схемы. Об этом говорит так называемый принцип Диогена: формальные институты порождают формальные барьеры входа, которые преодолеваются формально, и это преодоление вызывает неблагоприятный отбор [2, 3].

В результате формализации институтов, регламентирующих взаимодействие принципала и агента, ценность для агента имеет только то, что можно включить в отчет о проделанной работе. Поэтому усилия агента закономерно направляются не на содержание его работы, а на достижение определенных значений формальных показателей успешности этой работы.

Формализация институтов порождает стремление агентов удовлетворить предъявляемым к ним формальным требованиям, и это удовлетворение подчас принимает криминальные формы. Например, действия врачей, предпринимаемые в погоне за достижением формальных показателей качества работы, наносят вред пациентам, и это в лучшем случае оставление без помощи из боязни взять на себя ответственность [4], а в худшем случае их действия вызывают заболевания и смерть пациентов [5, 6]. В сфере образования и науки широко распространилась купля-продажа авторства научных текстов, пригодных к публикации в высокорейтинговых научных журналах, поскольку достижение формальных показателей такого рода вменено в обязанность работникам соответствующих сфер. Подобные примеры присутствуют во всех сферах жизни общества, и не только в России, а в любых странах, где применяются подобного рода методы стимулирования деятельности.

Поэтому коррупция – это не самое негативное последствие, возникающее при использовании формальных институтов. Формализация институтов опасна, прежде всего, тем, что она конструирует новую, вмененную реальность, подменяя содержательные критерии успешности формальными, не имеющими прямого отношения к содержанию [7]. Формализация институтов вызывает ухудшающий отбор, ведет к искусственным манипуляциям с показателями, которые вменяются тем или иным агентам и на основании которых судят об успешности их работы.

Решение данной проблемы требует действий троякого рода.

Во-первых, необходима частичная легализация теневых доходов, т.е. формальные институты, содержащие запрет на удовлетворение определенных потребностей, должны быть заменены другими формальными институтами, формирующими алгоритмы легального удовлетворения соответствующих потребностей.

Во-вторых, требуется частичная деформализация институтов и переход к содержательным (а не формальным) критериям успешности определенных видов деятельности. Формальные институты порождают вмененную реальность и искажают поведение агентов, пытающихся им следовать: чаще всего это делается в ущерб миссии, которую эти агенты призваны выполнять.

Наконец, в-третьих, необходимо ставить задачу не в плоскости искоренения рентоориентированного поведения, а в плоскости управления им. Коррупцию следует искоренять там, где она действительно мешает и вредит, где ее наличие мешает достижению определенных целей агентов, принимающих решения, но при этом АПР должен хорошо понимать, достижению каких целей мешает наличие тех или иных теневых потоков продуктов и ресурсов (денег, людей, и т.д.).

Литература:

1. *Goridko N.P., Nizhegorodtsev R.M.* Public Losses – Private Gains: Some Institutional Filters for Russian Economy // IFAC – PapersOnLine. 2018. – Vol. 51. Iss. 11. – P. 868-875. – URL: https://www.sciencedirect.com/journal/ifac-papersonline/vol/51/issue/11 (дата обращения 15.10.2021).

2. *Горидько Н.П., Нижегородцев Р.М.* Принцип Диогена, провалы институтов и противоречие между миссией и функцией // Друкеровский вестник. – 2019. – № 6. – С. 5-20.

3. *Goridko N.P., Nizhegorodtsev R.M.* The Diogenes Principle and Import of Formal Social Institutions in Research and Education Management / 5th International Conference on Education Science and Development (ICESD 2020): DEStech Transactions on Social Science, Education and Human Science, 2020. – P. 175-180. – URL: http://dpi-proceedings.com/index.php/dtssehs/article/view/34068/32655 (дата обращения 15.10.2021).

4. «Врачи просто не знают и боятся» – URL: https://news.rambler.ru/community/40090433-vrachi-prosto-ne-znayut-i-boyatsya/?utm_source=head&utm_campaign=self_promo&utm_medium=news&utm_content=news (дата обращения 15.10.2021).

5. США: главная причина, вызывающая рак – лечение рака. – URL: http://newsland.com/news/detail/id/1312261/ (дата обращения 15.10.2021).

6. В Хакасии акушер убил младенца, чтобы не портить больничную статистику. – URL: http://www.vesti.ru/m/doc.html?id=1146350 (дата обращения 15.10.2021).

7. *Нижегородцев Р.М.* Формализация институтов как механизм ухудшающего отбора / Глобализация экономики и

российские производственные предприятия: Материалы 16-ой Международной научно-практической конференции (14-18 мая 2018 года г. Новочеркасск). – Новочеркасск: ЮРГПУ (НПИ), 2018. – С. 27-39.

Меденников В.И.

Системный подход к применению искусственного интеллекта для разрешения проблем экологической безопасности при цифровой трансформации сельского хозяйства

Аннотация: В работе рассматривается эффективное решение проблемы экологизации сельского хозяйства на основе применения технологий искусственного интеллекта, реализуемых на подплатформе точного земледелия, входящей в свою очередь в единую цифровую платформу АПК, полученную математическим моделированием. Показано, что в этом случае будет обеспечено допустимое негативное воздействие природных и антропогенных факторов экологической опасности на окружающую среду, на продукцию АПК и самого человека.

Ключевые слова: точное земледелие, экологическая безопасность, искусственный интеллект, математическая модель, эрозия почв

Введение

В настоящее время технологическое развитие сельского хозяйства привело к тому, что отрасль встала в один ряд главных загрязнителей природы наряду с транспортом, энергетикой и промышленностью. В свою очередь, растениеводство из всех отраслей сельского хозяйства порождает наибольшие экологические проблемы, которые проявляются в виде: химического загрязнения и эрозии почвы, губительного влияния на фауну и флору водоемов, а также на различные виды сухопутных живых организмов. При этом основной причиной антропогенной эрозии почвы служат несоблюдения технологий выращивания растений, в частности, повсеместным нарушением в России севооборотных ограничений в погоне за прибылью, нормы и

правила внесения ядохимикатов, которые попадают в почву, воду, воздух и, наконец, в продукты питания.

Если экологические проблемы в виде истощения и засоления плодородной земли, эрозии почв, возрастания гнетущего состояния флоры и фауны все больше привлекают внимание регулирующих органов, то качество пищи уже вызывает беспокойство у жителей развитых стран. С резко возросшими возможностями цифровой экономики сочетание этих факторов начинает оказывать значительное влияние на характеристики производимой продукции почти всех отраслей. Данные тенденции, диктуемые государством и обществом, с одной стороны, увеличивают социальную ответственность товаропроизводителей, с другой стороны, вынуждают их выпускать продукцию надлежащего качества за счет цифровизации управления и логистики на всех этапах ее жизненного цикла.

Такой социальный заказ не мог не породить появление новых перспективных направлений цифровой трансформации сельскохозяйственного производства, которые и рассмотрим в данной работе.

1. Технологии точного земледелия

Появление такого перспективного направления в сельском хозяйстве на основе современных ИКТ, электронно-оптических средств, глобальных систем позиционирования получило название технологий точного земледелия (ТЧЗ). Суть их заключается в интеграции новых цифровизированных агротехнологий и высокоточного позиционирования на основе технологий дистанционного зондирование Земли (ДЗЗ), а также дифференцированных высокоэффективных и экологобезопасных агротехнических мероприятий на угодьях на основе детальной информации о химико-физических характеристиках каждого участка. В результате подобной интеграции, обеспечивающей оптимальные условия роста и развития растений в установленных рамках экологической безопасности, цифровые ТЧЗ обеспечивают получение максимально возможного объема продукции, отвечающего ряду необходимых ценовых, качественных и экологических требований. Во всем мире идут интенсивные исследования в совершенствовании этих технологий [1,2].

Современное электронно-оптическое оборудование, устанавливаемое на различных подвижных и стационарных аппаратах, за счет высокой разрешающей способности обеспечивает решение значительно большего количества задач в аграрной области – от картографирования границ отдельных небольших участков полей до мониторинга использования угодий по назначению и состоянию растений на значительных площадях. Появление специальных инструментов дешифровки спектральных параметров растений дает возможность рассчитывать различные вегетационные индексы, характеризующие фазы развития и биомассу их во временном разрезе. Такой полученный динамический ряд данных ДЗЗ обеспечивает анализ проведения большинства агротехнических мероприятий с выявлением зараженных болезнями и вредителями угодий и оценкой причиненного им ущерба, а также последствий прочих стихийных природных явлений. В этих условиях учет и мониторинг максимально возможного количества сельскохозяйственных процессов становится основной целью в разработке стратегией цифровизации крупнейших агропромышленных и машиностроительных фирм в мире. Так, прогнозируется, что к 2050 году количество замеров на «умных» фермах вырастет до 4,1 млн. в день. Сориентироваться в этом потоке информации самостоятельно практически невозможно [3]. И здесь на помощь должны прийти технологии искусственного интеллекта (ИИ), поскольку одна из задач применения ИИ – обобщение, анализ и обработка данных различных средств мониторинга, и выдача рекомендаций на их основе.

2. Применение искусственного интеллекта в ТЧЗ

Однако необходимость интеграции огромного количества информации в технологиях ТЧЗ требуют достаточного количества структурированных и надежных данных, для формирования которых необходимо некоторое единое цифровое пространство. Так, среди проблем ИИ отсутствие структурированных, достоверных данных поставили на первое место специалисты в этой области [4].

Поскольку в настоящее время почти все известные технологии ТЧЗ не обходятся без применения приложений ИИ, приведем наиболее значимые, предлагаемые рынком разработки ИИ [3].

2.1 Машинное обучение при мониторинге полей

Израильский стартап Taranis предоставляет точную информацию о состоянии растений на основе показаний полевых датчиков, метеостанций, аэрофотосъемки, что позволяет своевременно выявлять негативные факторы в виде идентификации болезней и вредителей, дефицита питательных веществ с выработкой рекомендаций по оперативному вмешательству.

2.2 Технологии ИИ для борьбы с сорняками

Так, компаниями Bayer и Bosh разрабатывается технология умного опрыскивания Smart Spraying, которая будет «узнавать» сорняк и определять вид и необходимое количество пестицида. «Убийца сорняков» от компании EcoRobotix способен самостоятельно перемещаться по полю, дифференцированно распознавая и обрабатывая обнаруженные сорняки. Утверждается, что технология позволит в 20 раз сократить объем использования гербицидов.

2.3 Технологии ИИ идентификации болезней растений

ИИ в настоящее время помогает также фермерам после идентификации заболевания растений выбрать методы их лечения с расчетом экономических показателей. Процесс происходит на основе фотографий пораженной части растения. Аналогичное мобильное приложение Plantix компании Peat предоставляет фермерам возможность идентификации свыше 60 болезней растений. Приложение содержит огромную БД снимков с идентификацией по сортам растений, видам бактерий, заболеваний и др.

3. Интеграция ТЧЗ в единую цифровую платформу АПК

В России концептуальные вопросы системного подхода к цифровизации ТЧЗ на основе единой цифровой платформы управления экономикой АПК исследованы в работе [5]. Модель позволила выделить ряд цифровых подплатформ, одна из них

представляет облачный сервис единой БД технологического учета отрасли растениеводства с выделением 240 функциональных управленческих задач с единым описанием алгоритмов, общих для всех сельскохозяйственных предприятий АПК.

Анализ онтологической модели показывает, что из 946 ее показателей более половины имеет отношение к экологии. Приведем некоторые примеры. В группе «Земля» (291 показатель) в подгруппу «Севооборот» входит 30 показателей. В подгруппе «Участок» группы «Поле» имеются показатели: «Запрещающие условия использования земельного участка», «Геоморфологические характеристики», «Мелиоративная характеристика», «Грунтовые воды», «Засоление», «Почва», «Агрофизическая характеристика», «Гидрофизическая характеристика», «Состояние почвы». Аналогично, в подгруппу «Культура» (108 показателей) входят следующие показатели: «Экологическая группа сорта», «Поражаемость болезнями по видам болезней», «Поражаемость вредителями» и т.д.

Соответственно, перечислим наиболее экологически выраженные решаемые задачи: «Землеустройство», «Севообороты и их размещение», «Система удобрения и воспроизводство почвенного плодородия», «Система защиты растений», «Учет агрофизического состояния почв», «Учет агрохимического состояния поля, участка», «Учет этно-фитосанитарного состояния участков полей», «Учет засоренности полей», «Учет численности вредителей», «Учет пораженности растений болезнями», «Разработка методов борьбы по защите растений».

Если объединить данную подплатформу с еще одной, сформированной на основе указанной выше модели, представляющей облачный сервис сбора и хранения пооперационной первичной учетной информации всех хозяйств в следующем виде: вид и объект операции, место осуществления, субъект проведения, дата и интервал времени проведения, задействованные средства производства, объем и вид потребленного ресурса, то получим перспективную цифровую платформу ТЧЗ, максимально учитывающую почти все экологические проблемы, а также обеспечивающую реализацию, как внутрихозяйственную, так и межотраслевую прослеживаемость продукции. Под прослеживаемостью понимается инструмент,

позволяющий достоверно информировать партнера, контролирующие органы, конечного пользователя об изготовителе, сроках, качестве, цене и других характеристиках товара.

Заключение

Таким образом, на основе представленного подхода будет значительно снижена экологическая опасность в сельском хозяйстве посредством комплексной экологической оценки земель; экологического мониторинга их, всего производственного процесса с учетом поступающих ресурсов и продукции на выходе; посредством формирования соответствующих управленческих решений, направленных на предупреждение проявления и минимизацию последствий проявления антропогенных и природных факторов экологической опасности.

Литература:

1. *Kannan B., Rajasekar M., Jayalakshmi K., Thiyagarajan G., Selvakumar S., Rajendran V.* Protected cultivation and precision farming technologies. – India: Sree Kumaran ComputersTNAU Campus, 2019. – 297 p.

2. *Меденников В.И., Богатырева Л.В.* Системный подход к проектированию цифровой платформы точного земледелия / Сборник статей по материалам международной научно-практической конференции «Развитие и внедрение современных наукоемких технологий для модернизации агропромышленного комплекса». – Курган: Издательство Курганской ГСХА, 2020. – С. 241-246.

3. Как начать внедрять точное земледелие на предприятии. – URL: https://smartfarming.ua/ru-blog/kak-nachat-vnedryat-tochnoe-zemledelie-na-predpriyatii (дата обращения 16.08.2021).

4. *Галустьян А.* Пять проблем, которые пока не может решить искусственный интеллект. – URL: https://rb.ru/opinion/problemy-ii/ (дата обращения 16.08.2021).

5. *Ereshko F.I., Kulba V.V., Medennikov V.I.* Digital platforms clastering model / Twelfth International Conference "Management of large-scale system development" (MLSD) (1-3 Oct. 2019 Moscow). – URL: https://ieeexplore.ieee.org/document/8911012 (дата обращения 16.08.2021).

Горелова Г.В., Мельник Э.В., Орда-Жигулина М.В., Орда-Жигулина Д.В.

Безопасность состояния водной экосистемы Азово-Черноморского региона, когнитивное исследование

Аннотация: Приведен ряд результатов когнитивного имитационного моделирования водной экосистемы, основанных на данных исследований природных явлений в Азово-Черноморском регионе. Представлен модуль когнитивного анализа в системе мониторинга и прогнозирования состояния водной экосистемы.

Ключевые слова: безопасность, водная экосистема, мониторинг, когнитивное моделирование, прогнозирование

В настоящее время, когда в мире происходят заметные климатические изменения, гидросфера земли подвержена множеству воздействий как природного, так и антропогенного характера, что серьезно влияет на безопасность населения. Это ставит перед государствами и их правительствами задачи либо противодействия этим изменениям, либо адаптации к новым условиям. ЮНЦ РАН проводит многолетние исследования изменений в Азовско-Черноморском регионе [1]. Целью настоящего исследования была разработка научных основ применения технологий цифровой экономики при построении новых методов и средств систем мониторинга и прогнозирования опасных процессов и обеспечения безопасности населения и береговой инфраструктуры [2,3]. В данной работе представлена информация о некоторых результатах этого исследования, связанная с когнитивным анализом и имитационным моделированием процессов в водной экосистеме Азовско-Черноморской территории и разработкой системы мониторинга опасных явлений и процессов. В эту систему входит подсистема поддержки принятия решений на основе когнитивного моделирования. Разработка такой системы вызвана необходимостью проводить многочисленные и непрерывные наблюдения за процессами изменений, обрабатывать огромное количество разнородных и разновременных данных, готовить и принимать решения по противостоянию опасным явлениям и снижению ущерба от негативных последствий. Важным при этом

является прогнозирование, научное предвидение возможного развития событий в природных системах, влияющих на жизнедеятельность населения. Часть необходимой информации для научного предвидения развития событий в водной экосистеме возможно получить с помощью имитационного когнитивного моделирования [4,5,6,7].

На рисунке 1 изображена разработанная с помощью авторской программной системы CMCS (Cognitive Modeling Complex Systems) [8,9,10] когнитивная карта G, названная «Состояние водной экосистемы территории». Получение изображения является завершением первого этапа когнитивного моделирования – разработки когнитивной модели.

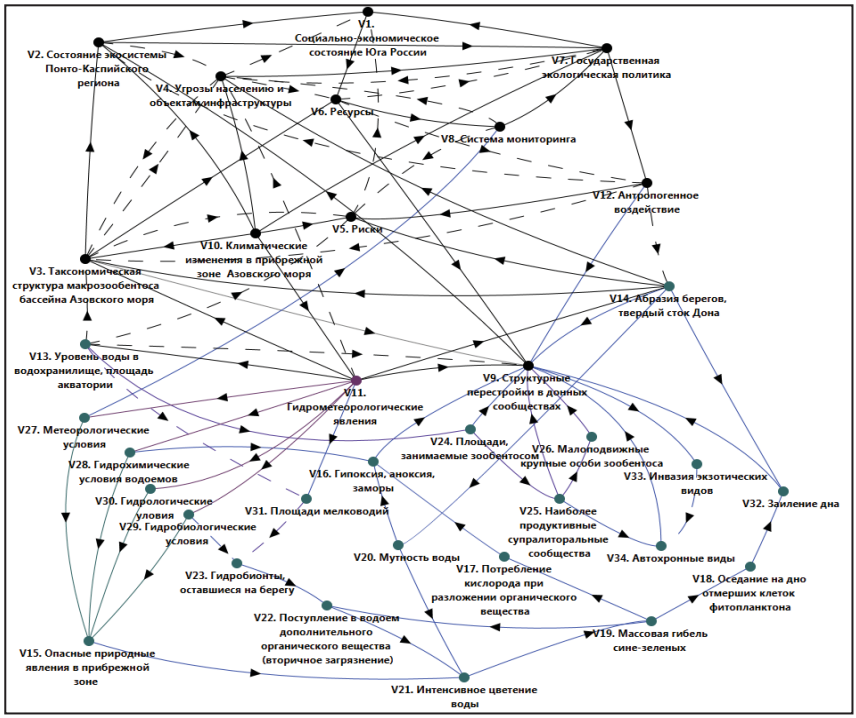


Рисунок 1 – Когнитивная карта *G* «Состояние водной экосистемы территории»

Для осуществления первого этапа когнитивного моделирования «Разработка когнитивной модели» были использованы теоретические, экспертные, статистические данные по Азово-Черноморскому региону.

Второй этап когнитивного моделирования посвящен анализу структурных свойств (вершин, путей, циклов, сложности, связности) и устойчивости модели (к возмущениям и структурной). Рисунок 2 представляет один из результатов второго этапа моделирования – определение циклов модели G; изображен один из 254 положительных циклов когнитивной карты, всего циклов 363, отрицательных циклов – 109. Нечетное число отрицательных циклов свидетельствует о структурной устойчивости такой системы [4,7].

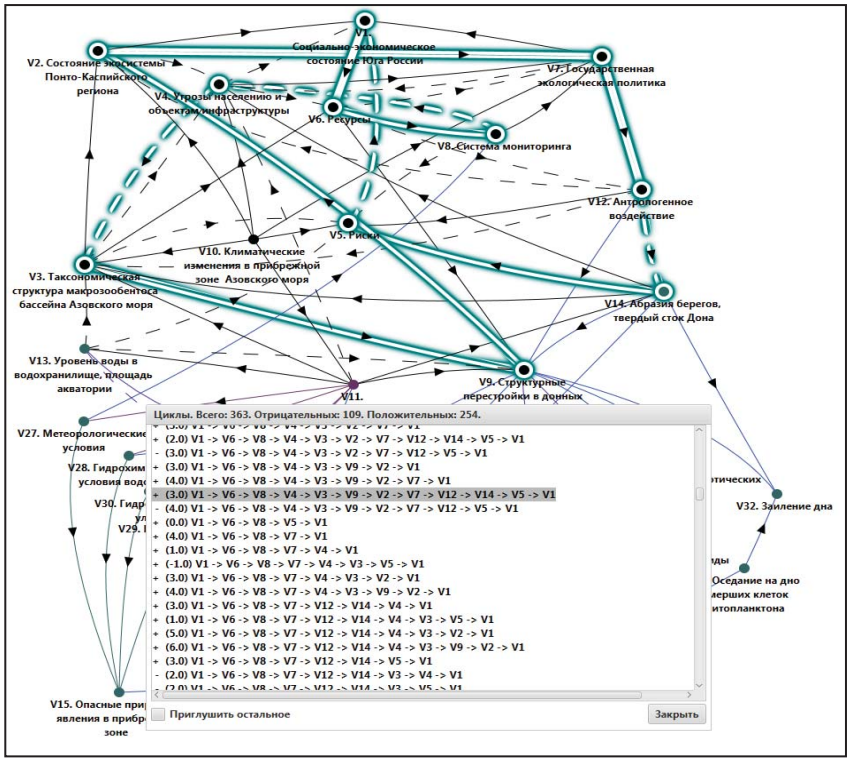


Рисунок 2 – Определение циклов когнитивной карты G

На рисунке 3 представлены результаты импульсного моделирования по одному из рассмотренных сценариев (3 этап когнитивного моделирования), в котором предполагалась возможность проявления опасных природных явлений в прибрежной зоне.

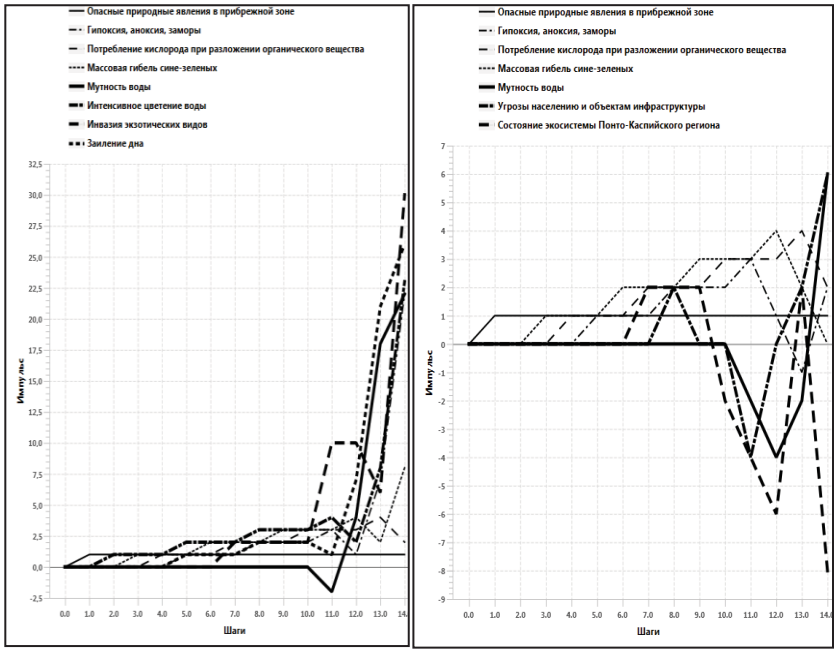


Рисунок 3 – Сценарий развития ситуаций в системе в предположении проявления опасных природных явлений в прибрежной зоне

На рисунке 4 изображена схема структуры распределенного хранилища данных, которая была реализована в процессе работы.

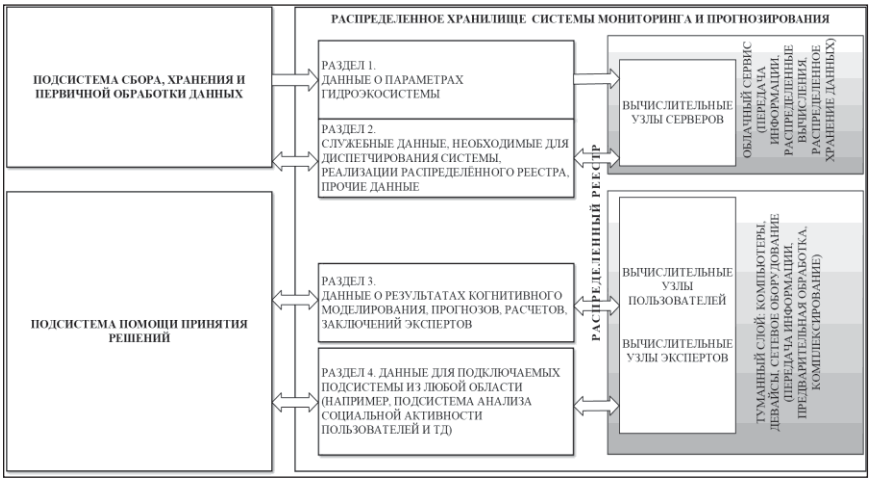


Рисунок 4 – Структура распределенного хранилища данных системы мониторинга опасных явлений и процессов

Работа проведена при финансовой поддержке РФФИ №18-05-80092

Литература:

1. *Матишов Г.Г., Матишов Д.Г., Бердников С.В., Яицкая Н.А.* Природные катастрофы в Азово-Черноморском бассейне в начале XXI века. – Ростов н/Д: Изд-во ЮНЦ РАН, 2017. – 160 с.

2. *Мельник Э.В., Орда-Жигулина М.В., Орда-Жигулина Д.В., Иванов Д.Я., Родина А.А.* Применение технологий цифровой экономики при разработке средств мониторинга и прогнозирования опасных процессов и обеспечения безопасности населения и береговой инфраструктуры / Закономерности формирования и воздействия морских, атмосферных опасных явлений и катастроф на прибрежную зону РФ в условиях глобальных климатических и индустриальных вызовов («Опасные явления»): материалы Международной научной конференции. – Ростов-на-Дону: Южный научный центр РАН, 2019. – С. 289-291.

3. *Горелова Г.В., Мельник Э.В., Орда-Жигулина М.В., Орда-Жигулина Д.В.* Модуль когнитивного анализа в системе мониторинга и прогнозирования состояния водной экосистемы /

Труды XXV научн. и уч.-практ. конф. «Системный анализ в пректировании и управлении». – Санкт-Петербург: ПОЛИТЕХ-ПРЕСС, 2021. – С. 300-313.

4. *Gorelova G.V., Pankratova N.D.* Scientific Foresight and Cognitive Modeling of Socio-Economic Systems /18 th IFAC Conference on Technology, Culture and International Stability (TECIS-2018). – IFAC Papers OnLine. – 2018. – Volume 51. Issue 30. – P. 145-149.

5. *Калиниченко А.И.* Преобразование данных мониторинга сложной системы в формат когнитивной имитационной модели / Сборник научных трудов XXIV Международной научной и учебно-практической конференции «Системный анализ в проектировании и управлении». В 3 ч. / Под общ. ред. В.Н. Волковой, Г.В. Гореловой, А.В. Логиновой. – Санкт-Петербург: ПОЛИТЕХ-ПРЕСС, 2020. – С. 46-52.

6. Свидетельство о государственной регистрации программы для ЭВМ №2018661506. Программа для когнитивного моделирования и анализа социально-экономических систем регионального уровня. Авторы: Горелова Г.В., Калиниченко А.И., Кузьминов А.Н. – 07.09.2018.

7. Свидетельство о государственной регистрации программы для ЭВМ №2018661506. Программный модуль преобразования данных мониторинга природных явлений в прибрежных зонах в формат когнитивной имитационной модели экосистемы. Авторы: Горелова Г.В., Калиниченко А.И., Мельник Э.В. – 17.06.2020.

Lepeshkin O.M., Ostroumov O.A., Sinyuk A.D.

The communication system functional stability with critical objects

Annotation: One of the requirements for complex technical systems is stability, a probabilistic characteristic of the system that determines the system ability to fulfill its purpose. The article deals with the problem of ensuring the communication system functional system with critical objects, determined through the ability of the system to perform its functions. To ensure functional stability, it is proposed to consider the process of managing the system resources on the basis of monitoring and control data.

Keywords: critical object, communication system, control system, the communication system functions and tasks, functional stability

Modern technical control systems include a communication system that ensures the delivery of commands that characterize the control action. The communication system, like the control system, is a complex functional-dynamic and organizational-technical multi-object hierarchical system distributed in space. Complex technical systems are subject to stringent requirements.

One of the most important requirements for any such systems is stability. In accordance with GOST [1], stability is considered through reliability, survivability. Stability can be viewed as a requirement for a system with a certain indicator, or as a property of the system that determines the constancy of the structure, behavior of the system and the processes occurring in it. Russian mathematician A.M. Lyapunov gave a definition of a complex system stability, which means the ability of the system to function in states close to equilibrium, under conditions of constant external and internal disturbing influences [2].

In [2], the key concept of determining the stability of the system functioning is structural and functional stability. Under the influence of various factors, the system constantly undergoes changes in state, and the measure that allows you to determine the influence of these changes on it is the set of functions it performs.

In the works of V.V. Lipaeva, M.G. Kuznetsova, E.S. Gorbachik [2] and other scientists, stability was considered as a probabilistic value that characterizes the change in the standard state of the system under the action of clearly defined influences. The stability of the system functioning must be considered from the side of functioning process in conditions of uncertainty of various factors influence with the possibility of predicting the system state at the moment of the influence beginning, during the process of influence and at the moment of such influence termination.

What does the system functioning mean? The system functioning is understood as a complex process of performing its functions by the system [3]. The stability of the network functioning is defined as its ability to perform its functions in the event of some of the elements failure [1]. The functional stability of a communication system does not always imply finding an equilibrium state of the system and maintaining

it, while the presence of critically important objects (CIO) determines the lack of equilibrium. The functional stability of the communication system with the CIO is the ability of the system in conditions of important objects criticality to perform its functions and tasks that allow achieving the goal of the system's functioning under the influence of various destabilizing factors.

The criticality of a communication system object is its property, which characterizes the impact of a violation (termination) of its functioning on the functioning of the system, the fulfillment by it or its elements of goals, functions, tasks.

A distinction should be made between static and dynamic criticality. Static criticality is a property of the system element, itself, which does not change over time. Dynamic criticality characterizes a property, which is determined by the conditions of its functioning in time.

Functional stability, as a scientific direction, has been developed with the emergence of complex technical systems, primarily in the aviation, space, rocket and navigation areas. The reservation of system individual elements, the use of additional control systems did not give a significant result and did not in any way affect the likelihood of failure of the system elements, but only complicated the system and gave an additional load on it. In addition, the additional load in the form of new elements and new tasks requires large material costs.

The main idea of ensuring the functional stability of a complex functional-dynamic and organizational-technical system is resource management, in the event of (prerequisites for) conflict situations in the system, to ensure the performance of its functions and purpose.

In works [4], the fundamental condition for ensuring functional stability in problems of managing complex autonomous objects is the possibility of redistributing available resources within the system. Abnormal system conditions,

In work [4], the fundamental condition for ensuring functional stability in problems of managing complex autonomous objects is the possibility of redistributing available resources within the system. Abnormal states of the system caused by failures were considered as admissible, functionally stable management of them is aimed at eliminating the consequences of failures and ensuring the performance of system functions.

The technological basis for ensuring the functional stability of complex systems is the creation of information and control complexes [4] and decision support systems that allow concentrating information about the state of the system, the processes occurring in it and the provision of their resources. It should be borne in mind that to ensure the functional stability of the system, it is necessary to combine all monitoring and control systems of various systems and elements of a complex system as part of a single information and control complex, to ensure their interface and interaction.

To ensure the functional stability of the communication system with the CIO, it is necessary to determine the target purpose of the system, the conditions for ensuring its functional stability.

The target purpose of the communication system with the CIO will be as follows:

$$f(y,d,u,v) \in Q, \qquad f^*(y^*,d,u,v^*) \in Q \tag{1}$$

where f – is some operator defined on the set $(y,d,u,v) \in Z$, $y(x,t) \in$ Y – is the set of communication system tasks, the execution of which over time is provided by the corresponding set of resources $x \in X$, $d \in D$ – is the set of internal and external influences that disrupt the functioning of the system, $u \in U$ – is the set of control actions of the system that ensure functional stability, $v \in V$ — is the set of objects of the system, the * sign determines belonging to the CIO, Q — is the permissible range of values of the function f characterizing the functioning of the system, that is, the fulfillment of its intended purpose.

Conditions for ensuring functional stability

$$\forall v \in V, v^* \in V, d \in D, y(x,t) \in Y \exists x \in X, u \in U: f(y,d,u,v) \in Q. \tag{2}$$

To describe the communication system, consider the graph $P_v = \{V, S\}$, where V – is the set of graph vertices characterizing the system elements, S – is the set of graph arcs characterizing the connections between the communication system elements. A functional-dynamic complex system will be functionally stable if, in the event of a malfunction of any element, there is at least one path that allows it to move from one vertex to another. The ability to perform functions by the system is determined by the graph $P_f = \{Y, X\}$, where Y – is the set of graph vertices that characterize the system's performance of tasks,

functions, and goals, X – is the set of arcs that characterize the resource required to complete the task, function, goal.

The representation of the system in the form of graphs allows for a quantitative assessment of the system functional stability.

Ensuring the functional stability (2) of the communication system under conditions of functioning uncertainty and the impact of various destabilizing factors is an important technical problem and needs to be addressed.

The use of graph theory and matrix theory allows one to quantify the functional stability of a system for simple systems. For systems with a hierarchical structure, it is necessary to separate the elements according to their influence on the functioning of the system.

When considering functional stability, it is necessary not only to determine the presence of a failure and to counteract it, but also to predict the state of the system in the future, which implies the intellectualization of the system of government by complex functional dynamic systems.

To ensure functional stability and ensure the system resources management, it is necessary to concentrate complete information about the system state, its resources at anytime from all sensors, monitoring and control systems [5].

Modern methods and techniques for assessing the stability of functioning do not take into account the process dynamics of system functioning and the state uncertainty. The functioning process of the communication system must be represented in the form of a set of tasks – regulations determined by the resource and time required for their implementation [6,7].

References:

1. GOST 53111-2008 Stability of public communication network functioning. – M.: Standartinform, 2009. – 19 p.

2. *Petrenko S.A.* The cyber systems operability maintaining concept in conditions of information and technical influences // Proceedings of ISA RAS. – Volume 41. – 2009. – P. 175-193.

3. *Surmin Yu.P.* Systems theory and systems analysis: Uch. allowance. – K.: MAUP, 2003. – 368 p.

4. *Durnyak B.V., Mashkov O.A., Usachenko L.M., Sabat V.I.* Methodology for ensuring the functional stability of hierarchical

organizational control systems // The scientific articles collection: Institute of Modeling Problems in Energy, NAS of Ukraine. – V. 48. – 2008. – P. 3-21.

5. *Gruzdev D.A., Zakalkin P.V., Kuznetsov S.I., Teslya S.P.* The information and telecommunication networks monitoring // Communication educational institutions proceedings. – 2016. – Volume 2. №4. – P. 46-50.

6. Lepeshkin OM, Ostroumov OA, Savishchenko NV. The management process regulation implementation – a criterion for determining the criticality of the system / State and prospects for the development of modern science in the direction of "Information security". Collection of articles of the III All-Russian scientific and technical conference. – Anapa: Military innovative technopolis "ERA", 2021. – P. 625-634.

7. *Lepeshkin O.M., Ostroumov O.A., Chernykh I.S., Ostroumov M.A.* On the question of the critically important object concept / Problems of troops technical support in modern conditions. Proceedings of the VI Interuniversity Scientific and Practical Conference. – St. Petersburg: Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, 2021. – P. 17-20.

Кереселидзе Н.Г.

Новые модели распространения вируса SARS-CoV-2 и проблемы управления безопасностью

Аннотация: Предложена новая математическая и компьютерная модель распространения вируса SARS-CoV-2 с учетом протокола борьбы с эпидемией принятой властями Грузии. Ставится задача управления борьбы с эпидемией при вакцинации с временным иммунитетом.

Ключевые слова: математическая, компьютерная модель, SARS-Cov-2, управление, эпидемия

1. Введение

Моделирование процессов пандемии COVID19, вызванной вирусом SARS-CoV-2 представляет повышенный интерес. И это естественно, пандемия унесла немало жизней, увеличило число людей с различными заболеваниями, ухудшило благосостояние

людей и другое. На первом этапе борьбы с COVID19 главными средствами были организационные ограничения, медицинские маски и т.п. Порой приходилось объявлять в государстве полный локдаун. Это давало положительный результат – минимальное число заболевших и скончавшихся от нового коронавируса. Однако локдаун оказался слишком дорогим мероприятием и бюджет стран сильно страдал. Пополнения в казну катастрофически падали и средств на социальные нужды, в том числе и лечение заразившихся новым вирусом не хватало. Для оздоровления экономики был снят локдаун, но в итоге увеличилось число погибших и заразивших. Больных и в этом случае лечат за государственный счет. Таким образом, и в отсутствии локдауна финансовые расходы.

Таким образом, стоит задача принятия решения и надо определить, в какой мере, и как надо применять карантинные меры, чтобы не было резкого пика заболеваемости и экономика страны избежала кризиса. Надо решать задачу управления безопасности жизни населения и экономики государства.

После того, как появилось возможность вакцинации людей, задача управления безопасности жизни населения и экономики государства не стала менее актуальной. Отчасти из-за того, что вакцин было недостаточно, отчасти из за антиваксерного движения, отчасти из-за того, что эффективность вакцин оказалось ниже ожидаемого.

Задача управления безопасности жизни населения и экономики совершенствовалось по мере получения новых средств и знании в борьбе с пандемией. Проблему управления безопасности, без вакцинации было рассмотрено в [1], с вакцинацией в [2]. Однако в [2], предполагалось, что вакцинированные люди не заражались вирусом, однако в действительности, как показывают последние исследования, это не так, число зараженных вакцинированных людей немалое количество. Следовательно, в данной работе попытаемся поставить, усовершенствовать задачу управления безопасности жизни населения и экономики, с учетом уязвимости вакцинированных персон.

За основу построения математической модели распространения SARS-Cov-2 принят протокол выработанный системой здравоохранения Грузии, обязательны для исполнения всеми

властными органами страны. При построении модели были использованы идей изложены в [3-5].

2. Бизнес логика процесса борьбы с эпидемией

Пусть в момент времени t в стране находится $N(t)$ число граждан. В это же самое время в страну въезжает $N_e(t)$ число граждан. По протоколу всех их следует направлять в места, отведенные для карантина – гостиницы, санаторий, дома отдыха и т.д. Однако, допустим, что не все прибывшие граждане переводятся в карантин, некоторым удалось каким-то образом избежать этого. Т.е., из $N_e(t)$ граждан, $\alpha_{e1}(t)N_e(t)$ попали в карантин, а $\alpha_{e2}(t)N_e(t)$ удалось избежать карантин. Имеем $N_e(t)=\alpha_{e1}(t)N_e(t)+\alpha_{e2}(t)N_e(t)$. Или $1=\alpha_{e1}(t)+\alpha_{e2}(t)$. Заметим, что в стране имеется группа въезжающих людей - E, группа находящаяся в карантине – Q. Пусть в момент времени t на карантине находятся $N_q(t)$ число граждан. По прошествии некоторого времени определенное число людей, у которых тесты покажут положительный результат на наличие SARS-Cov-2 вируса переводят в стационар на лечение – они инфицированы, и об этом есть документальное подтверждение, эту группу людей обозначим через I. Пусть в момент времени t из карантина на лечение направляется $N_{qi}(t)$ число граждан, а $N_{qh}(t)$ число граждан отпускают из карантина и они пополняют группу граждан - HS, конкретно в группы здоровых людей без иммунитета – H, их число составляет $N_{hs}(t)$. После лечения из группы I выздоровевшие пациенты пополняю группу здоровых людей с иммунитетом HI, их число составляет $N_{hi}(t)$, к сожалению, определенное число пациентов $N_{di}(t)$ не удается спасти. Группу, скончавшихся от вируса, обозначим через D. Заметим, что помимо заведомо инфицированных людей, в обществе имеется группа S больных людей носящий вирус, но об этом не имеется

документальное подтверждение, число этих людей обозначим через $N_s(t)$. Как раз члены из группы S и являются основным распространителями вируса, они свободно контактируют с членами группы здоровых людей без иммунитета - H, в котором $N_h(t)$ граждан заражая их. Сложность ситуации в том, что соответствующие органы не знают точно ни число этих людей, но и самих распространителей инфекции. Заметим, что группа HS является объединением групп H и S, $N_{hs}(t) = N_h(t) + N_s(t)$.

Эпидемиологические службы определяют из группы S инфицированных $N_{si}(t)$ людей и переводят их в стационары на лечение, пополняя тем самым группу I. Вместе с тем определяется круг их контактов, пусть в количестве $N_c(t)$ людей из группы HS и переводят их в карантин, пополняя группу Q, соответственно $N_{ch}(t)$ - из группы H, и $N_{cs}(t)$ из группы S, $N_c(t) = N_{ch}(t) + N_{cs}(t)$. К сожалению, в группе S также имеется случай кончины от вируса, обозначим их число через $N_{ds}(t)$, которые пополняют группу D. Мы будем предполагать, что люди переболевшие новым корона вирусом приобретают иммунитет, но могут заразится вновь. При вакцинации люди из группы H переходят в HI. Т.е. в процессе вакцинации людей из группы здоровых людей без иммунитета, привитые люди из H переходят в группу здоровых людей с иммунитетом HI. то обозначим их число в момент времени t через $N_{hit}(t)$.

По последним данным, несмотря на вакцинацию, некоторые члены группы HI, общаясь с членами группы S, могут быть инфицированными. Поэтому, часть из них направляется на лечение I, а часть в карантин Q. Замети, что количество членов групп E,Q,I,HI,D,HS известно в каждый момент времени t. Однако, точно не известно количество членов групп H и S соответственно. Между тем, контакты членов групп H и S могут ухудшить эпидемиологическую ситуацию, так, как больные из S могут заразить здоровых из H.

Построим схему борьбы с эпидемией и ее бизнес логику в виде ориентированного графа:

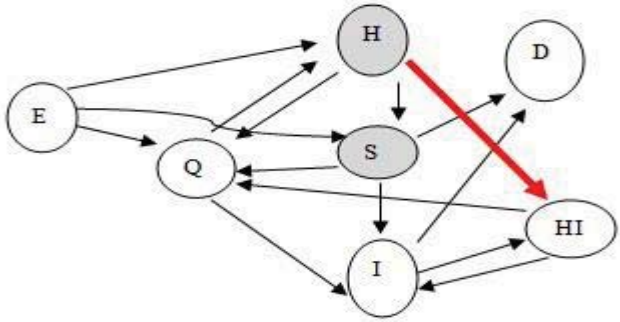


Рисунок 1 – Ориентированный граф борьбы с эпидемией

3. Построение модели

В ориентированном графе на рисунке 1 дуга EH имеет вес $\alpha_{e21}(t)N_e(t)$ а дуга ES - $\alpha_{e22}(t)N_e(t)$. Дело в том, что некоторые граждане въехавшие в страну и не попавшие в карантина могут быть и здоровыми, и инфицированными - больными. Точно их число не известно, однако известно, что $\alpha_{e21}(t)+\alpha_{e22}(t)=\alpha_{e2}(t)$. Но вместе они пополняют HS=HUS группу, объединение групп H и S.

Скорость изменения числа группы здоровых людей без иммунитета - $N_h(t)$ из группы H зависит от интенсивности: контактов между членами групп H и S; пополнения группы Q из группы H $N_{ch}(t)$ людьми; пополнения группы H из группы Q $N_{qh}(t)$ людьми, пополнения группы H из группы E $N_e(t)$ людьми. Поэтому имеем:

$$\frac{dN_{hi}(t)}{dt}=\alpha_{qh}N_{qh}(t)+\alpha_{eh}(t)\alpha_{e21}(t)N_e(t)-\alpha_{ch}N_{ch}(t)-\alpha_{hs}N_h(t)N_s(t) \quad (1)$$

где α_{qh}, $\alpha_{eh}(t)\alpha_{e21}(t)$, α_{ch}, α_{hs} соответствующие коэффициенты. Скорость изменения числа группы здоровых людей с иммунитетом

- $N_{hi}(t)$ из группы HI зависит от интенсивности: выздоровления больных из группы I (увеличивает), вакцинации в группе H (увеличение), контактов между членами групп HI и S (уменьшает) – при этом часть из группы HI переходит в группу Q, а часть в I. В результате получим:

$$\frac{dN_{hi}(t)}{dt} = \alpha_{ihi}(t)N_i(t) + \alpha_{vac}(t)N_h(t) - \alpha_{qshi}N_s(t)N_{hi}(t) - \alpha_{ishi}N_s(t)N_{hi}(t) \quad (2)$$

Аналогично рассуждая можно выписать соотношения на подобие (1) и для скорости изменения численности групп Q, I, S. В результате получим систему обыкновенных дифференциальных уравнений:

$$\begin{cases} \frac{dN_h(t)}{dt} = \alpha_{qh}(t)N_q(t) + \alpha_{eh}(t)\alpha_{e21}(t)N_e(t) - \alpha_{hc}(t)N_h(t) - \\ \quad - \alpha_{hs}(t)N_h(t)N_s(t) - \alpha_{vac}(t)N_h(t), \\ \frac{dN_q(t)}{dt} = \alpha_{hc}(t)N_h(t) + \alpha_{eq}(t)\alpha_{e1}(t)N_e(t) + \alpha_{sc}(t)N_s(t) - \\ \quad - \alpha_{qh}(t)N_q(t) - \alpha_{qi}(t)N_q(t) + \alpha_{qshi}N_s(t)N_{hi}(t), \\ \frac{dN_s(t)}{dt} = \alpha_{hs}(t)N_h(t)N_s(t) + \alpha_{es}(t)\alpha_{e22}(t)N_e(t) - \\ \quad - \alpha_{si}(t)N_s(t) - \alpha_{sc}(t)N_s(t) - \alpha_{sd}(t)N_s(t), \\ \frac{dN_i(t)}{dt} = \alpha_{si}(t)N_s(t) + \alpha_{qi}(t)N_q(t) - \alpha_{ihi}(t)N_i(t) - \alpha_{id}(t)N_i(t) + \\ \quad + \alpha_{ishi}N_s(t)N_{hi}(t), \\ \frac{dN_d(t)}{dt} = \alpha_{id}(t)N_i(t) + \alpha_{sd}(t)N_S(t), \\ \frac{dN_{hi}(t)}{dt} = \alpha_{ihi}(t)N_i(t) + \alpha_{vac}(t)N_h(t) - \alpha_{qshi}N_s(t)N_{hi}(t) - \\ \quad - \alpha_{ishi}N_s(t)N_{hi}(t). \end{cases} \quad (3)$$

где коэффициенты в системе неотрицательны, наблюдение эпидемией происходит на отрезке времени $[t_0;T]$. В (3) функция

$N_e(t)$ в принципе известна – количество въезжающих граждан. В начальный момент времени t_0 известны:

$$N_q(t_0) = N_{q0}, \quad N_i(t_0) = N_{i0}, \quad N_d(t_0) = N_{d0}, \quad N_h(t_0) + N_s(t_0) = N_{00}. \qquad (4)$$

Система (3) с начальными условиями (4) составляют математическую модель эпидемии SARS-Cov-2 вируса.

4. Задача управления эпидемией

Анализируя протокол борьбы с эпидемией и ее математическую модель, следует отметить, что контроль за распространением инфекций имеет особые рычаги управления. Так, например, усовершенствуя контроль за прибывшими гражданами, можно практически исключить проникновение больных граждан в общество, минуя карантин. В модели, например, следует уменьшить значения коэффициентов $\alpha_{e21}(t), \alpha_{e22}(t)$. Также подбирая значения коэффициента $\alpha_{hs}(t)$ фактически можно достичь жесткий локдаун, или либеральную политику сдерживания эпидемии. Пусть при подборе $\alpha_{e21}(t)$ – воздействие на бюджетные расходы составляют $B: \alpha_{e21}(t) \to R$, а расходы при лечении инфицированных можно выразить через $W: \int_{t_0}^{T} N_i(\tau) d\tau X \alpha_{hs}(t) \to R$, то общие расходы на выявление инфицированных и их лечение, с учетом их минимизации можно выразить так:

$$J(\alpha_{e21}(t), \alpha_{hs}(t)) = B(\alpha_{e21}(t)) + W\left(\int_{t_0}^{T} N_i(\tau) d\tau, \alpha_{hs}(t)\right) \to \inf. \qquad (5)$$

Минимизация функционала (6) нужно достичь при условиях (3),(4) и ограничении:

$$B(\alpha_{e21}(t)) \geq L > 0. \qquad (6)$$

Ограничение (6) означает, что бюджетные расходы на эти мероприятия не могут быть меньше определенной величины. Ясно, что имеем ограничения и сверху - бюджетные средства ограничены!

Заметим, что в функционале $W(*)$ учтено и то, что подбирая значения коэффициента $\alpha_{hs}(t)$ (тем самым определяя уровень

локдауна) мы фактически изменяем финансовые поступления - конкретно уменьшаем их. Поэтому нам нужно минимизировать и эту величину.

Для управления безопасности жизни населения и экономики государства рассматривается экстремальную задачу типа (5), (6), (3), (4).

При этом появляется еще одно ограничение, целью которого является достижения коллективного иммунитета:

$$N_{hi}(T) = N_{hit}(T) + N_{hiv}(T) \geq 0,7N(T). \quad (7)$$

Компьютерная реализация модели (3),(4) и экстремальной задачи (5),(6) была проведена в среде MatLab для различных значениях постоянных коэффициентов системы (3), начальных условиях (4) и конкретных функционалов B,W .

6. Выводы

Вычислительный эксперимент, проведенный на компьютерной модели, построенной на основе математической модели (3), (4) при постоянных коэффициентов позволяет заключить, что при помощи подбора значении параметров α_{e21} и α_{is} можно подобрать такое число инфицированных граждан, $N_i(t)$, при котором экономика не нуждается в локдауне, и прогноз выздоровления заразившихся благоприятен.

Литература:

1. *Кереселидзе Н.Г.* Модели распространения вируса SARS-CoV-2 и проблемы управления безопасностью / Материалы XXVIII Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС-2020) (16 декабря 2020 г. Москва). – М.: ИПУ РАН, 2020. – С. 77-83.

2. *Kereselidze N.G.* Forecasting of Key Indicators of the Manufacturing System in Changing External Environment // IFAC-PapersOnLine. – 2021. – Volume 54. Issue 13. – P. 617-621.

3. *Kermack W.O., McKendrick A.G.* A contributions to the mathematical theory of epidemics / Proceedings of the Royal Society of London. Series A. Containing Papers of a Mathematical and Physical Character. – Aug. 1, 1927. – Vol. 115. №. 772. – P. 700-721.

4. *Kereselidze N.* Combined continuous nonlinear mathematical and computer models of the Information Warfare // International journal of circuits, systems and signal processing. – 2018. – Vol. 12. – P. 220-228.

5. *Кереселидзе Н.Г.* Модели распространения ложной информации / Материалы XXVII международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС-2019) (18 декабря 2019 г. Москва). – М.: ИПУ РАН, 2019. – С. 167-172.

Соколов А.В., Ройзензон Г.В., Комендантова Н.П.

Технология создания систем мониторинга и прогноза состояния опасных явлений и объектов (на примере эпидемии COVID-19)

Аннотация: В работе показано, как накопление информации (статистических данных и знаний) о пандемии COVID-19 приводит к уточнению математических моделей, к расширению области их использования. Построенная (на основе технологии сбалансированной идентификации [1]) модель удовлетворительно описывает динамику заболеваемости COVID-19 в г. Москва с 19.03.2020 по 22.10.2021 и может использоваться для прогноза с горизонтом в несколько месяцев. Основным внутренним механизмом, определяющим динамику модели, является коллективный иммунитет.

Ключевые слова: моделирование, сбалансированная идентификация, управление рисками, искусственный интеллект

Оценка эффективности

Важным направлением в рамках мониторинга и противодействия пандемии COVID-19 является разработка методологии оценки эффективности от введения дополнительных ограничительных мер, что предполагает разработку специальных систем критериев, по которым можно будет судить о степени достижения поставленных задач (целей). При этом критерии могут быть условно разделены на три большие группы. Первую группу образуют критерии, позволяющие для противодействия пандемии

COVID-19 оценивать имеющийся ресурс (количество больничных коек, приборов ИВЛ, медицинского персонала, медикаментов и т.п.). Вторая группа критериев позволяет оценивать скорость расходования и прироста ресурса во времени (возможность использования медицинских специалистов смежных специальностей, ускоренный ввод в эксплуатацию объектов медицинской сферы, возможности закупки лекарств и оборудования за рубежом и др.) необходимого для борьбы с пандемией COVID-19. Наконец, третья группа критериев позволяет сделать вывод о степени достижения поставленных целей (например, предполагается, что в течение определенного срока (например, года) вирусом заразиться не более 2 процентов населения, или процент падения ВВП и т.п.). Таким образом, оценки по указанным составным критериям, позволят сделать вывод насколько принятые меры, и полученные результаты, являются эффективными. С точки зрения методов теории принятия решений такую проблему (оценки эффективности) можно поставить как задачу многокритериальной порядковой классификации. В качестве классов решений будут выступать показатели эффективности (например, класс 1 – высокоэффективные меры, класс 2 – меры средней эффективности, класс 3- малоэффективные меры). Среди методов вербального анализа решений (ВАР), которые непосредственно можно использовать для решения поставленной задачи можно отметить методы ОрКласс и ЦИКЛ. К положительным сторонам использования методов ВАР, прежде всего, можно отнести то, что к исходным данным не применяются никакие операции по их переводу в количественную форму. Известно, что перевод вербальных измерений в «цифру» зачастую весьма субъективен и не имеет строгого математического обоснования. Кроме того, методы ВАР позволяют получить объяснения принятых решений (интерпретация результата) в терминах предметной области, здесь – в терминах описания критериев оценки эффективности противодействия пандемии COVID-19. В качестве недостатков методов ВАР можно отметить большие трудозатраты эксперта или лица, принимающего решения, при работе в признаковом пространстве большой размерности. В этом случае необходимо применять различные методы снижения его размерности. Использование многокритериальных методов (в

частности, методов ВАР) для оценки эффективности противодействия пандемии COVID-19 позволяет не только классифицировать меры (например, по степени эффективности), но и позволяет выработать механизмы анализа на основе применения продукционных правил. Такой подход позволяет выработать сценарии, позволяющие проанализировать по каким критериям и как необходимо улучшить оценки, для того чтобы те или иные не вполне эффективные меры, можно было «перевести» в более предпочтительный класс. При этом, для успешного решения такой задачи, совсем не обязательно улучшать оценки сразу по всем критериям, а можно ограничиться только каким-то подмножеством критериев, позволяющим минимизировать расход того или иного ресурса, что, в свою очередь, позволяет использовать предложенный механизм для создания системы поддержки принятия решений (СППР).

Создание систем мониторинга и прогноза состояния опасных явлений и объектов

Эффективное проведение мониторинга состояния и прогноза поведения опасных явлений или объектов предполагает широкое использование математических моделей. Цели мониторинга и прогноза ставятся с учетом наличия математических моделей, сложность, подробность и надежность которых в свою очередь определяются количеством и качеством (точностью) экспериментальных данных (наблюдений) и знаний о функционировании объекта.

Иногда построение системы мониторинга и прогноза начинается с нуля и по мере накопления данных и знаний и построения все более подробных и точных моделей, возможности мониторинга и прогноза возрастают. В доступных рядах данных проявляется все больше эффектов, что позволяет усложнять соответствующие математические модели. Такому усложнению способствует и появление новых знаний об исследуемых процессах, которые, иногда, могут частично заменить цифровые данные.

Динамика эпидемии определяется процессами взаимодействия вируса, человеческого организма и общества. Различные процессы имеют различные характерные времена, причем, чем больше характерное время процесса, тем больше времени требуется для его

проявления, тем длиннее должны быть ряды наблюдений, необходимые для определения его характеристик.

Для пандемии COVID-19 характерные времена различных процессов могут быть оценены следующим образом:

- 15 дней – заразность и манифестация (выявляемость) как функции длительности заболевания;
- 30 дней – текущий индекс репродукции (контактное число) и индекс выявления (и последующей изоляции);
- 60 дней – зависимость индекса выявления от количества проведенных тестов;
- 90 дней – влияние естественного (после болезни) коллективного иммунитета;
- 200 дней – влияние ослабления естественного иммунитета со временем;
- 100 дней – влияние вакцинации;
- 180 дней (предварительная оценка) – влияние ослабления искусственного (после вакцинации) иммунитета,
- 365 дней – сезонность заразности.

Горизонт прогноза определяется погрешностью модели, которая определяется точностью описания отдельных процессов, которая в свою очередь определяется длинной рядов наблюдений (и их надежностью). Таким образом, длительность мониторинга определяет, какие процессы могут быть оценены (с характерными временами меньше этой длительности) и, следовательно, определяют горизонт и точность прогноза. С этой точки зрения становится понятной неудача попытки прогноза динамики пандемии, предпринятой Н. Фергюсоном. Его группа в начале 2020 года активно обосновывала тотальный карантин, «прогнозируя» (на несколько месяцев вперед) 500 тыс. смертей в Англии и 2 млн. в США (за лето 2020 года) [2].

Мониторинг и построение моделей осуществлялись с марта 2021г. Через несколько месяцев на основе анализа выявленных количеств зараженных для семи популяций удалось определить (идентифицировать) некоторые биологические функции, в том числе заразность как функцию длительности болезни (рисунок 1А), а еще через месяц, связать интенсивность выявления заболевших с количеством проведенных тестов (рисунок 1Б).

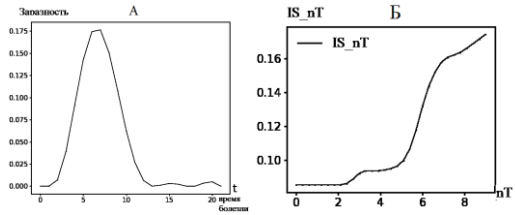
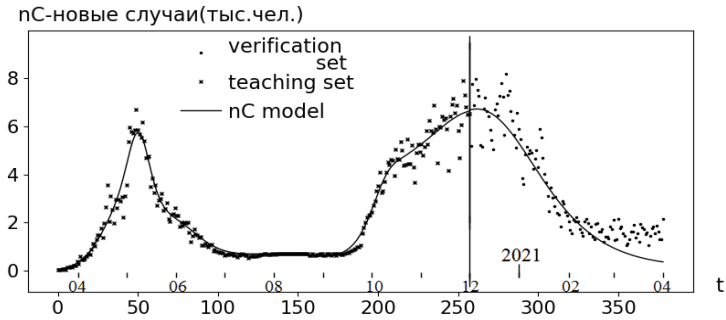


Рисунок 1 – А. Нормированная (на единицу) заразность как функция от длительности заражения (дни). Б. *IS_nT* – функция эффективности выявления больных в зависимости от количества тестов на тысячу человек (*nT)* в г. Москва

Первые прогнозы удалось сделать в 01.12.2021 (рисунок 2), когда удалось интегрировать в модель процесс накопление естественного (переболевших) коллективного иммунитета и его ослабление.



Крестики – обучающий набор (до вертикальной линии), кривая – модель, точки – верификация (после вертикальной линии)

Рисунок 2 – Прогноз новых случаев заражения в Москве от 01.12.2020

В апреле 2021 учли вакцинацию. Прогноз от 15.04.2021 приведен на рисунке 3.

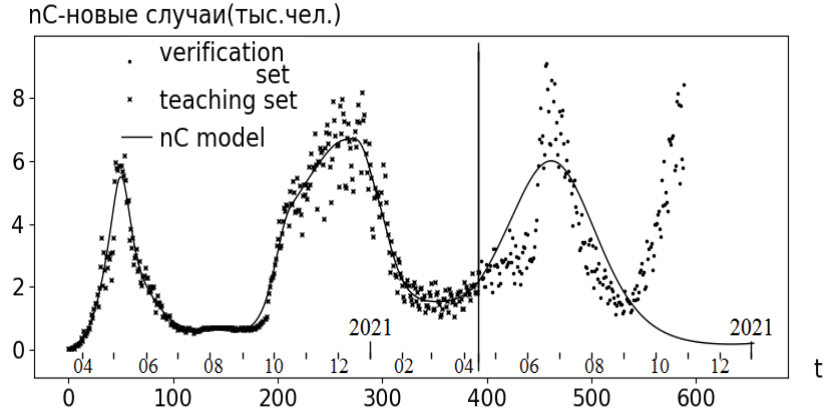


Рисунок 3 – Прогноз новых случаев заражения в Москве от 15.04.2021

И, наконец, учли ослабление иммунитета иммунизации – прогноз от 20.10.2021 (рисунок 4). Согласно этому прогнозу, до 01.01.2022 будет выявлено около 600 тыс. новых зараженных и около 950 т. – до 01.04.2022.

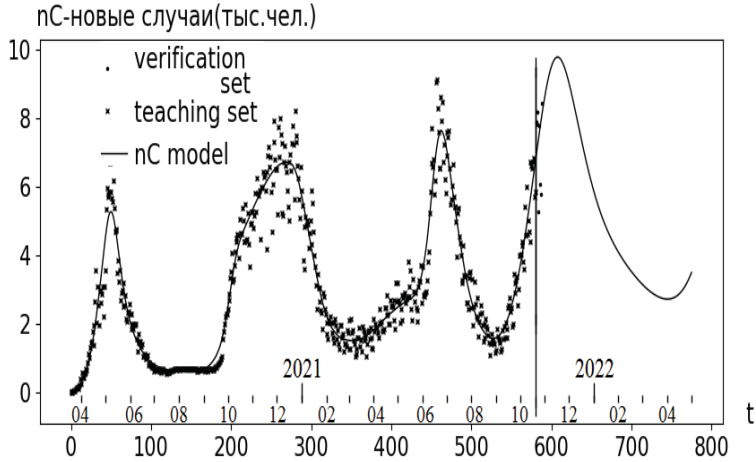


Рисунок 4 – Прогноз новых случаев заражения в Москве от 20.10.2021

Заключение

К настоящему моменту разработано четыре основных способа оценки рисков, а именно: вероятностный (инженерный), модельный, экспертный и социологический. Важной особенностью представленной работы является разработка методологии и инструментария систем мониторинга и прогноза динамики пандемии. Система развивается и интегрирует в себя новые проявляющиеся процессы.

Исследование выполнено при финансовой поддержке РФФИ проекты 20-57-82004, 20-07-00701 и 19-07-00522

Литература:

1. *Sokolov A.V., Voloshinov V.V.* Model Selection by Balanced Identification: the Interplay of Optimization and Distributed Computing // Open Computer Science. – 2020. – Volume 10. Issue 1. – P. 283-295.

2. Report 9: Impact of non-pharmaceutical interventions (NPIs) to reduce COVID-19 mortality and healthcare. – URL: https://www.imperial.ac.uk/media/imperial-college/medicine/mrc-gida/2020-03-16-COVID19-Report-9.pdf (дата обращения 15.10.2021).

Грабчак Е.П., Логинов Е.Л.

Подготовка системы государственного управления России к сверхкритическим ситуациям природного и техногенного характера

Аннотация: Рассматриваются проблемы подготовки системы госуправления нашей страны к ситуациям, в которых состояние ключевых профилей жизнеобеспечения может оказаться ниже критической точки управляемости. Предлагается принятие в России упреждающего комплекса мер резко повышающих эффективность госуправления в отношении перечня регулируемых ресурсных, экономических, технических, социальных и иных параметров с учетом внешних и внутренних факторов функционирования суперсистемы.

Ключевые слова: государственное управление, риски, угрозы, анализ, моделирование, информационная система

Сверхкритическая ситуация – это такое состояние экономики в ее совокупных проявлениях и взаимовлиянии, при котором состояние ключевых профилей жизнеобеспечения находится ниже критической точки управляемости.

Можно предложить следующие укрупненные группы мер по подготовке системы госуправления нашей страны к таким ситуациям:

– разработка сценариев последствий возможных управляющих воздействий со стороны органов государственной власти на институциональную и конъюнктурную среду, органы власти разного уровня и хозяйствующие субъекты с целью поддержания устойчивости экономики России в условиях сверхкритической ситуации природного или техногенного характера и периода восстановления пострадавших территорий [1];

– разработка мер по повышению эффективности управляющих воздействий со стороны органов государственной власти с целью поддержания устойчивости экономики России в условиях сверхкритической ситуации природного или техногенного характера и периода восстановления пострадавших территорий;

– диагностика экономической (в т.ч. энергетической, продовольственной и пр.) безопасности России в условиях сверхкритической ситуации природного или техногенного характера и периода восстановления пострадавших территорий;

– анализ влияния рисков внешних угроз экономической безопасности страны вследствие сверхкритической ситуации природного или техногенного характера, в т.ч. введения карантина, на функционирование экономики и, в том числе, энергетики, в условиях нарушения кооперационных, экономических и социальных связей, а также на эффективность работы и развития отдельных секторов экономики, в т.ч. выполнение инвестиционных программ [2];

– построение карты рисков развития экономики и, в том числе, энергетики, в условиях сверхкритической ситуации природного или техногенного характера в увязке с ситуацией и возможного поведения других стран – покупателей наших ресурсов и поставщиков необходимой продукции и с учетом наибольшего влияния их как в отдельности, так и в совокупности на

устойчивость российской суперсистемы [3], построение сценарного «дерева рисков».

– разработка системных механизмов подержания работы систем жизнеобеспечения в условиях сверхкритической ситуации природного или техногенного характера и периода восстановления пострадавших территорий с детализацией по основным технологическим профилям и техническим подсистемам;

– определение необходимых мер для снижения негативного воздействия сверхкритической ситуации природного или техногенного характера на работу отраслевых и территориальных технологических комплексов с учетом их технологических, организационных и экономических взаимосвязей.

– анализ и систематизация опыта СССР (нормативные акты и фактические организационные мероприятия) по массовой эвакуации и возвращению хозяйственных объектов (оборудования) в период Великой отечественной войны.

– анализ и систематизация опыта СССР по перемещению промышленных объектов из зоны Чернобыльской аварии; анализ последствий землетрясения в Спитаке; разработка рекомендаций по адаптации этого опыта к современным условиям глобальных природных и техногенных катастроф (наводнение, землетрясение, авария на АЭС и пр.) в отношении хозяйственных, а также социальных и иных объектов в России;

– анализ особенностей и проблем функционирования экономики и, в том числе, энергетики, в особый период (военные действия, зональная активизация террористической активности, массовые беспорядки и пр.) с учетом накопленного опыта решения этих проблем в условиях рыночной экономики в постсоветский период (проблемы: технические, логистические, финансово-экономические, кадровые и т.п.) [4];

– разработка рекомендаций по адаптации имеющихся организационных и информационных механизмов взаимодействия федеральных, региональных и муниципальных властей и корпоративного управления для обеспечения устойчивой работы органов власти разного уровня и хозяйствующих субъектов в условиях сверхкритической ситуации природного или техногенного характера и периода восстановления пострадавших территорий [5];

– расчеты комплексного ресурсного и топливно-энергетического балансов на различных уровнях управления

(Российская Федерация, субъект Российской Федерации или крупное муниципальное образование, территория) [6];

– построение продуктовых моделей (математическое моделирование, описание функционирования комплекса анализируемых объектов, прогнозирование, в т.ч. при «внешних» воздействиях на ресурсный и топливно-энергетический балансы, в т.ч. в условиях сверхкритической ситуации природного или техногенного характера [7].

Целесообразно формирование Единой отраслевой (межотраслевой) платформы управления данными как интегрированной защищенной информационной платформы, адаптированной к работе в условиях чрезвычайных ситуаций и особого периода, объединяющей по группе информационных и коммуникационных сервисов ситуационные центры федеральных, региональных и муниципальных органов власти, с последующим информационным подсоединением к ситуационным центрам Правительства Российской Федерации и Совета Безопасности России [8].

Таким образом, для преодоления дестабилизационных трендов сверхкритической ситуации природного или техногенного характера необходимо упреждающее принятие в России комплекса мер резко повышающих эффективность госуправления в отношении перечня регулируемых ресурсных, экономических, технических, социальных и иных параметров, с вписыванием механизмов и процедур госуправления в рыночные механизмы и структуру формирования бюджета с учетом внешних и внутренних факторов жизнедеятельности суперсистемы.

Литература:

1. *Макаров В.Л., Бахтизин А.Р., Сушко Е.Д., Агеева А.Ф.* Агент-ориентированная модель Евразии и имитация реализации крупных инфраструктурных проектов // Экономика региона. – 2018. – Т.14. № 4. – С. 1102-1116.

2. *Грабчак Е.П., Логинов Е.Л.* Анализ и прогнозирование критических ситуаций в электро- и теплоэнергетике России на основе внедрения инновационных информационных сервисов // Инновационная деятельность. – 2019. – № 4 (51). – С. 24-28.

3. *Райков А.Н., Шкута А.А.* Управление экономикой России в условиях с предельно большой компонентой неопределенности

развития чрезвычайных ситуации и критического недостатка информации // Проблемы безопасности и чрезвычайных ситуаций. – 2019. – № 4. – С. 104-110.

4. *Loginov E.L., Grigoriev V.V., Shkuta A.A., Bortalevich V.Y., Sorokin D.D.* The use of artificial intelligence's elements to block the manifestations of individuals' behavioral activity going beyond the quasi-stable states / IOP Conference Series: Materials Science and Engineering. Materials Science and Engineering. – Volume 516. – III International Conference "Cognitive Robotics" (22-24 November 2018 Tomsk). – 2019. – Article 012028.

5. *Райков А.Н., Шкута А.А.* Планирование мер поддержания интерактивной коммуникации информационных систем с учетом угроз возможного коллапса управления экономикой в особый период // Проблемы безопасности и чрезвычайных ситуаций. – 2019. – № 3. – С. 79-86.

6. *Loginov E.L., Grigoriev V.V., Shkuta A.A., Bortalevich V.Y., Sorokin D.D.* Intelligent monitoring, modelling and regulation information traffic to specify the trajectories of the behaviour of organizational agents in the context of receipt of difficult-interpreted information // IOP Conference Series: Materials Science and Engineering. – Volume 516. – III International Conference "Cognitive Robotics" (22-24 November 2018 Tomsk). – 2019. – Article 012015.

7. *Григорьев В.В.* Алгоритмы решения одной задачи определения оптимальной совокупности многоотраслевых комплексов. – М.: Вычислительный центр АН СССР. – Москва, 1984. – 28 с.

8. *Грабчак Е.П., Григорьев В.В., Логинов Е.Л., Деркач А.К.* Формирование территориально распределенной сети катастрофоустойчивых дата-центров: концентрация защищенных систем управления в энергетике, адаптированных для работы в условиях чрезвычайных ситуаций и в особый период // Проблемы безопасности и чрезвычайных ситуаций. – 2020. – № 5. – С. 75-81.

Кротова М.В.

Возможности применения анализа вызовов, угроз и рисков с динамических позиций

Аннотация: Обеспечение безопасности организаций, являющихся стратегическими для экономики России, т.е. сложных систем, существенно зависит от своевременности принятия решений в сложной, высоко конкурентной международной среде. Фундаментальное свойство всех управленческих и менеджерских дисциплин, связанных с управлением интегрированными компаниями стратегического значения для России, и важное для модернизации отечественной экономики, это постулат о том, что начало процессов и получение результатов всегда имеют временную привязку, т.н. «тайминг» (англ. timing).

Ключевые слова: риск, угроза, вызов, инновационный менеджмент, фактор времени

В силу фактора времени, любое решение менеджера следует оценивать:

- с точки зрения своевременности его принятия;
- с точки зрения ожидаемых сроков выполнения, т.е. реалистичности и создания точек избыточного напряжения в системе;
- с точки зрения длительности параллельно идущих в системе других процессов и их взаимовлияния с новым решением, принятым с заданный момент времени, а также долгосрочных последствий решений, принятых в определенный момент времени;
- с точки зрения наличия у менеджера достоверной, точной, полной и релевантной информации в нужный момент времени, доступности информации для менеджера в определенный момент времени, а также – появления принципиально новой информации, в том числе, и недостоверной, способной в течение короткого отрезка времени повлиять на процесс принятия решений; данное свойство информации в менеджменте изучается в таких сферах, как торговля на бирже или использование методов информационной войны, недобросовестной конкуренции и т.п.

Сама суть процессов менеджмента как управления на уровнях предприятия, интегрированной компании, государственной корпорации и национальной экономики, в т.ч. в макроэкономическом и отраслевом «ракурсах», – т.е. для крупных социально-экономических систем, формирующих экономику РФ, дает основания считать, что «тайминг», т.е. момент принятия любого, даже обоснованного «в статике» управленческого решения, может изменить его сущность. Также сам момент принятия решений способен оказаться причиной возникновения новых, дополнительных рисков, угроз и даже стратегических вызовов. «Тайминг» принятия управленческих решений, если рассуждать эмпирически, возможно оценивать со следующих позиций:

– соответствия решения актуальным проблемам организации, деятельность которой носит стратегический характер;

– состоянию ресурсного потенциала организации;

– релевантности принимаемого решения текущему уровню опасности в свете ожидаемых, просчитываемых действий конкурентов, в т.ч. международных компаний и иностранных правительств, которые, в свою очередь, могут выражаться в форме эмбарго, запретов на экспорт технологий, а для высокотехнологичных компаний – в одновременном перенасыщении рынка близкой по свойствам высоко конкурентной продукцией; например, телефоны Apple и Samsung, вакцины Sputnik V и AstraZeneca.

Фактор времени на стратегическом горизонте проявляется в том, что структура и ресурсы самой организации, работоспособные или идеальные при одном соотношении внешних сил, превращаются в проблему при их изменении. Уже здесь по меньшей мере спорной оказывается заимствованная из западной практики концепция менеджмента как адаптации (преимущественно пассивной) системы управления крупной производственной компанией к внешним обстоятельствам, т.н. «реактивности», т.е. компания не будет предпринимать изменения раньше, чем произойдет изменение в окружающих ее внешних силах и ресурсах.

Тем не менее, адаптивный подход является стандартом для стратегического менеджмента и государственного регулирования. В настоящее время для организаций существует стандартная схема паспортизации рисков, утвержденная в [1].

Идентификация опасных событий – ключевой элемент паспортизации рисков, который, в свою очередь, подразделяется на следующие разделы, каждый из которых требует собственных методик и стандартов оценки:

– индивидуальный идентификатор опасного события;

– краткое наименование опасного события и его описание;

– этап жизненного цикла продукции (услуги), на котором может возникнуть опасное событие;

– причина опасного события;

– возможные воздействия и последствия опасных событий на деятельность организации;

– предупреждающие средства контроля и методы управления;

– средства контроля и методы управления по реагированию на опасное событие восстановлению деятельности;

– уровень применяемых предупреждающих средств контроля и методов управления;

– уровень применяемых средств контроля и методов управления по реагированию на опасное событие и восстановлению деятельности.

Как видно из перечисленного списка основных контрольных параметров, к динамическим аспектам паспортизации рисков может быть отнесена только стадия жизненного цикла продукта. Все остальные параметры носят статичный характер, и в силу этого даже реалистичный, не формальный анализ паспорта риска организации на предмет достаточности мер и мероприятий может оказаться недостаточным, если не проводится (неформально, либо в качестве внутрикорпоративных мероприятий и документов) хотя бы минимальный анализ на своевременность решений, принимаемых в сложной ситуации.

Рассмотрим с точки зрения своевременности и соответствии реальному состоянию дел на рынках международных инноваций и промышленной продукции – некоторые опубликованные проекты документов. Созданию условий и регулированию инновационной деятельности был посвящен проект Стратегии инновационного развития Российской Федерации на период до 2020 г., или «Инновационная Россия-2020» (далее – ИР-2020), текущий адрес документа в Интернете: [2], который был одобрен президиумом Правительства РФ в сентябре 2011 г. ИР-2020 создавалась в

развитие положений Концепции долгосрочного развития Российской Федерации (КДР) на период до 2020 г. Несмотря на то, что сама концепция ИР-2020 так и не была утверждена в качестве официального документа, а КДР фактически исчерпала свой срок, различные положения проекта до сих пор вызывают интерес у специалистов в качестве примера написания документа, непосредственно регулирующего инновационное развитие и инновационный менеджмент.

Рассмотрим раздел IX. Участие в глобальной инновационной системе. Россия, согласно общим положениям ИР-2020, должна стать одним из геополитических полюсов в формирующемся многополярном мире с занятием к 2020 году существенной доли (в 5-10%) рынках высокотехнологичных по 5-7 позициям, увеличение в полтора раза доли высокотехнологичного сектора в ВВП (с 13% до 17-18%). В качестве средств реализации предполагалось «…устранение ограничений, препятствующих выходу российской высокотехнологической продукции на внешние рынки, … участию российских компаний в мировой конкуренции … на уровне бизнес-проектов, и через межправительственные инициативы с ключевыми, с точки зрения технологического сотрудничества, странами». Для этого предполагались политико-дипломатическая поддержка, поддержка экспорта и упрощение режима выхода на внешние рынки, в т.ч. экспортного контроля за продукцией двойного назначения, организационная поддержка крупных инвесторов, а также расширение научных стажировок и устранение административных барьеров, мешающих международному сотрудничеству.

В целом, эти методы являются стандартными для большинства экономик средне- и высокоразвитых стран [3] с открытой экономикой. И уже на этом временном горизонте видно, что спустя 3-4 года, после обострения международной обстановки вокруг Украины, введения большинством стран НАТО ряда финансовых и технологических ограничений на кооперацию с РФ, подобная модель участия нашей страны в глобальной инновационной системе требовала корректировки в сторону: а) снижения общей открытости в регулировании международной научной, информационной и промышленной кооперации; б) активизации использования сильных

сторон и возможностей для самой России – вместо импорта недостающих технологий и ресурсов.

В таблицу 1 сведены спорные или представляющие стратегические риски положения из ИР-2020, с их оценкой условной релевантности ситуации в 2011 и 2021 гг., и их своевременности.

Таблица 1 – Характеристики отдельных положений программы «Инновационная Россия» в международной сфере

Содержание положений	**Релевантность, 2011 г.**	**Релевантность, 2021 г.**
Упрощение процедур экспортного контроля	угрозы и риски утечки технологий	допустимо только для союзников РФ
Государственная поддержка экспортеров, в т.ч. совместных предприятий	эффект не является автоматическим	сокращение расходов бюджета на экономику
Вхождение компаний РФ в капитал зарубежных технологических лидеров	риски долгосрочной технологической зависимости	неоднозначные процессы выстраивания отношений с подобными компаниями
Стимулирование международной кооперации, включая программы Евросоюза	нет механизма расторжения кооперации при усложнении международных отношений	возможно только после распада НАТО
Направление до 50% молодых ученых на стажировку за рубеж	риски связаны с человеческим фактором	решение нерелевантное, носит формальный характер

В качестве выводов к изложенному материалу следует отметить следующее. Крупные компании и госкорпорации, формирующие промышленный и технологический потенциал России, имеют достаточно ресурсов для того, чтобы действовать проактивно, см. например, об этом в [4]. По сути, именно проактивного менеджмента, опережающего обоснованные сроки адаптации, требует от стратегических предприятий и компаний «Стратегия научно-технологического развития Российской Федерации», утвержденная Указом Президента Российской Федерации № 642 от 1 декабря 2016 года [5]. Развивая управленческую трактовку «тайминга», проактивный менеджмент следует определять как реорганизацию компании раньше, чем она столкнется с изменениями во внешней среде и ресурсах.

Литература:

1. ГОСТ Р 51901.22-2012. Менеджмент риска. Реестр риска. Правила построения (Переиздание) от 29 ноября 2012. – URL: https://docs.cntd.ru/document/1200100075 (дата обращения 14.10. 2021).

2. «Инновационная Россия-2020». Стратегия инновационного развития Российской Федерации на период до 2020 года. – URL: https://cluster.hse.ru/mirror/pubs/share/209522123 (дата обращения 10.01.2021).

3. Инновационная экономика: Энциклопедический словарь-справочник/Комков Н.И., Селин В.С., Цукерман В.А. Науч. рук. Ивантер В.В., Суслов В.И.; ИНП РАН. – М.: МАКС Пресс, 2012. – 542 с.

4. *Владимиров В.А., Малинецкий Г.Г., Махутов Н.А. и др.* Управление риском. Риск. Устойчивое развитие. Синергетика. – М.: «Наука», 2000. – 431 с.

5. Указ Президента Российской Федерации № 642 от 1 декабря 2016 года «О Стратегии научно-технологического развития Российской Федерации». – URL: http://www.kremlin.ru/acts/bank/41449 (дата обращения 05.09.2021).

Абдулова Е.А.

Об одном подходе к управлению рисками критической инфраструктуры

Аннотация: В работе рассматривается подход к управлению рисками критической инфраструктуры. Предлагается пятиэтапный подход, включающий конкретизацию целей и задач процесса, определение инфраструктуры, оценку и анализ риска, мероприятия по управлению рисками и измерения.

Ключевые слова: критическая инфраструктура, риск, управление рисками, оценка и анализ риска, угрозы, последствия

Критические инфраструктуры (КИ) играют жизненно важную роль в обществе, обеспечивая выполнение многих ключевых функций и услуг [1]. Концепция «критической инфраструктуры» постоянно развивается, отражает текущие проблемы и реагирует на новые вызовы, особенно с точки зрения кибербезопасности и устойчивости. Критические инфраструктуры, включая энергетические, коммуникационные и банковские сети, механизмы общественного здравоохранения и безопасности, как правило, представляют собой совокупность функций, выполняемых широким кругом заинтересованных сторон. Поэтому управление рисками для этих инфраструктур является общей ответственностью, требующей тесного и постоянного сотрудничества между заинтересованными сторонами.

Эффективное управление рисками КИ фокусируется на повышении устойчивости на основе оценки критичности или важности данной инфраструктуры, а также характера и уровня рисков, с которыми она сталкивается. Заинтересованные стороны совместно определяют наиболее важные для них активы, а затем совместно оценивают, расставляют приоритеты и управляют соответствующими рисками.

Риск определяется как вероятность нежелательного исхода в результате инцидента, события или происшествия, определяемая его вероятностью и соответствующими последствиями [2]. На нее влияют характер и величина угрозы или опасности, уязвимости от

этой угрозы или опасности и возможные последствия. Информация о рисках позволяет заинтересованным сторонам, от владельцев объектов и операторов до федеральных агентств, определять приоритеты действия по управлению.

Особенно важное значение имеют критические информационные инфраструктуры (КИИ), т.е. обширные и пересекающиеся сети информационно-коммуникационных технологий, которые связывают и эффективно обеспечивают надлежащее функционирование других ключевых инфраструктур [3-6]. Фактически, КИИ не только поддерживают все другие критические инфраструктуры, но и способствуют наступлению «информационной эпохи».

В отличие от физических активов КИ, таких как здания, плотины или электростанции, критические информационные инфраструктуры являются виртуальными или «логическими» по своей природе. То есть они состоят из сложных, распределенных систем программного обеспечения, оборудования и услуг, функционирующих вместе для достижения желаемого результата.

В работе представлен подход к управлению рисками критической инфраструктуры, который имеет структуру, представленную на рисунке 1. Такая структура позволяет интегрировать стратегии, возможности и структуры управления, для принятия решений с учетом рисков, связанных с критической инфраструктурой. Данный подход к управлению рисками критической инфраструктуры может применяться ко всем угрозам и опасностям, включая киберинциденты, стихийные бедствия, антропогенные угрозы безопасности и террористические акты, хотя для понимания каждого из них могут использоваться разная информация и методологии.

Рисунок 1 – Структура подхода к управлению рисками КИ

Кроме того, подход к управлению рисками критической инфраструктуры дополняет и поддерживает процесс выявления и оценки угроз и опасностей. Этот процесс включает в себя идентификацию угроз и опасностей и то, как они могут повлиять на сообщество, и определение того, как лучше всего смягчить эти угрозы и опасности, исходя из текущих возможностей и требований к ресурсам.

Предлагаемый подход к управлению рисками критической инфраструктуры не предназначен для замены уже используемых моделей или процессов. Скорее, он поддерживает общий, унифицирующий подход к управлению рисками, который все заинтересованные стороны могут использовать, связывать и согласовывать со своими собственными моделями и действиями управления рисками.

Предлагаемый подход к управлению рисками критической инфраструктуры может быть адаптирован и применен к активу, системе, сети и т.д., в зависимости от фундаментальных характеристик решений, которые он призван поддерживать, и характера соответствующей инфраструктуры. Представленный ниже подход к управлению рисками критической инфраструктуры включает следующие этапы.

– Цели и задачи. На этом этапе необходимо определить результаты, условия, конечные точки или целевые показатели эффективности, которые в совокупности описывают эффективное и желаемое состояние управления рисками.

– Определение инфраструктуры. На этом этапе необходимо определить активы, системы и сети, которые вносят вклад в критически важные функции, а также необходимо собрать информацию, относящуюся к управлению рисками, включая анализ зависимостей и взаимозависимостей.

– Оценка и анализ рисков. На этом этапе проводится оценка риска с учетом потенциальных прямых и косвенных последствий инцидента, известных уязвимостей для различных потенциальных угроз или опасностей, а также имеющейся информации об угрозах. Риск для критической инфраструктуры является функцией угрозы, уязвимости и последствий, где: угроза относится к природным и антропогенным источникам, в части и их движущей силы, целей и возможностей, а также к вероятности того, что угроза существует или возникнет; уязвимость – это слабое место или ограничение,

которое может быть использовано угрозой; последствия – выражаются стоимостью для оценки риска. На рисунке 2 показана взаимосвязь между риском, угрозами, уязвимостью и последствиями.

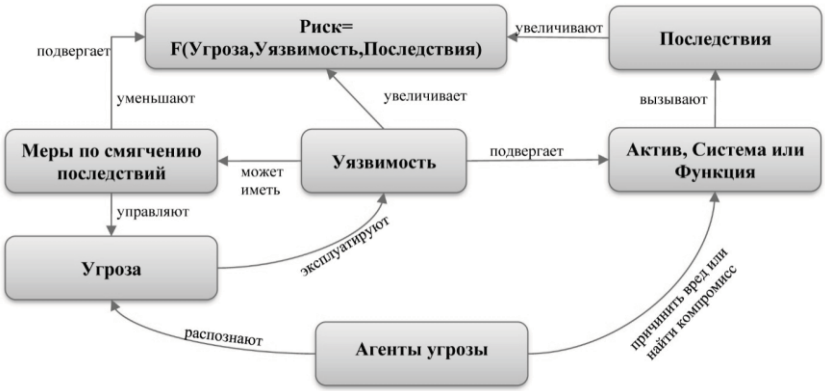


Рисунок 2 – Связь между риском, угрозами, уязвимостью и последствиями

Мероприятия по управлению рисками. На этом этапе принимаются решения и внедряются подходы к управлению рисками для контроля, принятия, передачи или предотвращения рисков. Подходы могут включать меры по предотвращению, защите, смягчению, реагированию и восстановлению.

Измерения. На основе использования метрик проводится определение прогресса и оценки эффективности усилий по обеспечению и повышению устойчивости критической инфраструктуры.

Используя показатели для оценки эффективности усилий заинтересованных сторон по достижению приоритетов в рамках критической инфраструктуры, заинтересованные стороны могут корректировать и адаптировать свои подходы к безопасности и устойчивости с учетом достигнутого прогресса, а также изменений в угрозах и других средах. Метрики используются для сосредоточения внимания на конкретных вопросах безопасности и устойчивости, которые требуют дополнительных.

Метрики также служат механизмом обратной связи для других аспектов подхода к управлению рисками критической инфраструктуры. Они отображают прогресс в достижении целей и предоставляют аналитикам информацию для корректировки оценок рисков. Например, метрики показывают эффективность действий по обеспечению безопасности и устойчивости, а также степень, в которой эти действия снижают риски.

Представленный подход поддерживает интегрированный и непрерывный процесс с циклами обратной связи и повторяющимися шагами, что позволяет лицам, принимающим решения, отслеживать прогресс и реализовывать действия по повышению безопасности и устойчивости критической инфраструктуры с течением времени. Физические, кибернетические (виртуальные) и человеческие элементы критической инфраструктуры следует рассматривать как часть каждого этапа подхода к управлению рисками КИ.

Литература:

1. *Markopoulou D., Papakonstantinou V.* The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular // Computer Law & Security Review. – 2021. – Vol. 41. – Article 105502.

2. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2020. – 20 с.

3. *Калашников А.О., Сакрутина Е.А.* Модель оценки рискового потенциала объектов критической инфраструктуры атомных электростанций / Труды 11-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD’2018) (1-3 октября 2018 г. Москва). – М.: ИПУ РАН, 2018. – Т. 2. – С. 457-461.

4. *Калашников А.О., Сакрутина Е.А.* Модель прогнозирования рискового потенциала значимых объектов критической информационной инфраструктуры // Информация и безопасность. – 2018. – Т. 21. № 4. – С. 465-470.

Широкий А.А.

Модели и методы естественных вычислений в управлении рисками сложных систем

Аннотация: Под естественными вычислениями (natural computing) принято понимать совокупность моделей и вычислительных методов, вдохновленных природой, а также рассматривающих происходящие в живой природе явления с точки зрения обработки информации. Поскольку жизнедеятельность живых организмов происходит в условиях переменного окружения, являющегося как источником всевозможных угроз, так и возможностей для развития, идея применения биоинспирированных подходов для решения задач управления рисками сложных систем является вполне естественной. Настоящий материал посвящен выявлению моделей и методов естественных вычислений, наиболее подходящих для решения фундаментальных и прикладных задач управления рисками сложных систем.

Ключевые слова: риск, сложные системы, управление рисками, естественные вычисления, задача эффективного управления, задача минимизации риска

Термин «*естественные вычисления*» обычно определяют как область исследований, изучающую модели и вычислительные методы, вдохновленные природой, а также исследующую происходящие в природе явления с точки зрения обработки информации [1]. Задача выживания в условиях переменного окружения, являющегося источником как предсказуемых, так и непрогнозируемых угроз, которую постоянно решают живые организмы, является частным случаем управления рисками. При этом демонстрируемые ими модели поведения, применяемые механизмы защиты от внешних угроз и формируемые структуры группового управления характеризуются высокой эффективностью, достигнутой в ходе эволюционного развития.

В настоящей работе представлен результат анализа основных известных видов естественных вычислений на предмет их применимости в задачах управления рисками. Краткий обзор

моделей и методов естественных вычислений, вывод критериев применимости, а также результаты исследования сравнительной распространенности этих подходов представлены в [2].

Под сложными системами мы будем понимать системы с бесконечным разнообразием реакций на внешние воздействия. Задача управления сложной системой в общем случае заключается в нахождении множества *эффективных* управляющих воздействий, переводящих ее в целевое состояние.

Риск системы определим согласно [3] как системный параметр, свойство системы управления, в частности ЛПР, принимать решения в условиях неопределенности, которые могут повлечь за собой как нежелательные (опасные), так и существенно выигрышные последствия.

Можно показать эквивалентность математических постановок задачи управления сложной системой в условиях неопределенности и задачи минимизации риска – см., например, [4].

Задачи управления рисками сложных систем можно разделить на две большие группы:

1) фундаментальные задачи;
2) прикладные и технологические задачи.

К первой группе отнесем задачу идентификации компонентов системы (1), задачу моделирования поведения объектов, являющихся ее частью (2), задачу выявления аномалий в их поведении (3), а также задачу прогнозирования развития системы. Постановки этих задач не зависят от специфики управляемой системы.

Ко второй группе задач относится задача параметризации пространства состояний системы (1), задача классификации объектов системы и ее окружения (2), задача поддержки принятия решений по управлению рисками (3), а также задача разработки алгоритмического и программного обеспечения для управления рисками. Эти задачи ставятся с учетом специфики рассматриваемой системы.

Исходя из особенностей постановок перечисленных выше задач, можно сформулировать критерии отбора моделей и методов, подходящих для их решения, а именно:

1) универсальность применения, т.е. возможность реализовать произвольный алгоритм или приблизить произвольную функцию с заданной точностью;

2) наличие формальной модели в основе метода;

3) обучаемость;

4) наличие технической реализации.

Теперь, на основе представленных критериев, проанализируем применимость моделей и методов естественных вычислений для решения задачи управления рисками сложных систем. Их подробный обзор можно найти, например, в [5]. Здесь же просто приведем их список и их *краткие обозначения*, которые будем использовать в дальнейшем:

Формальные грамматики:

1) мембранные вычисления (P-системы) | *P-sys*;

2) системы Линденмайера (L-системы) | *L-sys*.

Элементные базы:

1) ДНК-вычисления | *DNA*;

2) амебные вычисления | *Physarum*;

3) бактериальные вычисления | *Bacterial*.

Математические модели:

1) клеточные автоматы | *CA*;

2) искусственные нейронные сети | *ANN*;

3) хаотические вычисления | *Chaos*;

4) вычисления «реакция-диффузия» | *Chem*;

5) вычисления, основанные на столкновениях | *Billiard*.

Эвристические алгоритмы или их семейства:

1) искусственные иммунные системы | *AIS*;

2) роевой интеллект | *Swarm*;

3) аморфные вычисления | *Amorphous*;

4) эволюционные вычисления | *Evolutionary*.

В работе [2] все вышеперечисленные модели и методы подробно проанализированы с точки зрения их применимости для решения фундаментальных и прикладных задач управления рисками сложных систем. В таблице 1 представлен консолидированный результат этого анализа.

Таблица 1 – Перечень моделей и методов естественных вычислений с указанием выполнения критериев применимости для решения задач управления рисками сложных систем

Вид вычислений	Универсальность применения	Формальная модель в основе	Обучаемость	Наличие технической реализации
P-sys	UC	Да	Нет	Программная
L-sys	SC			
DNA	UC	Да	Нет	Самособирающиеся ДНК-плитки
Physarum	UC	Нет	Нет	Вычислительная система с амебой *Physarum polycephalum* (L.)
Bacterial	UC (?)	Нет	Нет	Модиф. *E. Coli* (L.)
CA	UC	Да	Адаптивность	Программная
ANN	UC	Да	Да	Аппаратная и программная
Chaos	UC	Да	Нет	Аппаратная и программная
Chem	UC	Да	Нет	Программная
Billiard	UC	Да	Нет	Программная
AIS	UA (?)	Да	Да	Программная
Swarm	UA (?)	Нет	Нет	Программная
Amorphous	UC	Нет	Нет	Программная
Evolutionary	N/A	Да	Нет	Программная

Обозначения:

UC – универсальный вычислитель,

UA – универсальный аппроксиматор,

SC – символьный вычислитель,

(?) – вопрос не исследовался, либо отсутствует строгое доказательство.

Таким образом, с точки зрения сформулированных выше критериев, для решения задач управления рисками сложных систем наилучшим образом подходят искусственные нейронные сети, клеточные автоматы и искусственные иммунные системы. Отметим, что первый подход получил широкое распространение в обсуждаемой области, тогда как последние два сравнительно менее популярны. В связи с этим, представляется целесообразным развить методы управления рисками сложных систем на основе клеточных автоматов и искусственных иммунных систем в будущих исследованиях.

Литература:

1. Handbook of Natural Computing/Rozenberg, G., Bäck, T., Kok, J.N. (eds.). – Berlin: Springer Berlin Heidelberg, 2012. – 2105 p.

2. *Широкий А.А., Калашников А.О.* Применение методов естественных вычислений для управления рисками сложных систем // Проблемы управления. – 2021. – № 4. – С. 3-20.

3. *Кононов Д.А.* Исследование безопасности систем управления на основе анализа их системных параметров / Материалы XXVIII Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС-2020) (16 декабря 2020 г. Москва). – М.: ИПУ РАН, 2020. – С. 102-108.

4. *Калашников А.О.* Управление информационными рисками организационных систем: общая постановка задачи // Информация и безопасность. – 2016. – Т. 19. № 1. – С. 36-45.

5. *Nemade M.N., Rane M.D.* A Review on Bio-Inspired Computing Algorithms and Application / Proceedings of National Conference on Recent Trends in Computer Science and Information Technology (NCRTCSIT-2016). – Nagpur, India, 2016. – P. 12-19.

II. Проблемы обеспечения экономической и социально-политической безопасности

Володина Н.Н., Комков Н.И., Сутягин В.В.

Проблемы управления развитием крупномасштабных социально-экономических систем

Аннотация: Рассматриваются проблемы управления развитием иерархических социально-экономических систем. Отмечается сложность согласования потенциала и масштабов развития подсистем научного уровня. Показано отличие моноцентрического и равнозначного подхода к распределению потенциала развития. Обозначены основные механизмы к управлению развитием одноуровневых подсистем.

Ключевые слова: развитие, иерархические социально-экономические системы, подсистемы, целевые проекты

Иерархическая организация сложных многоуровневых социально-экономических систем отличается большим разнообразием и отсутствием общего мнения относительно влияния какого-либо из уровней на устойчивость и прогрессивность развития всей СЭС в целом. Существуют оценки приоритетного влияния на структурную устойчивость. К ним, прежде всего, относится наличие сильных структур, (регионов, отраслей), поддерживающих и обеспечивающих скрепы между ее составными частями. К ним, прежде всего, относится распределение финансовых и материальных (в основном материальных) потоков. В России такими центрами накопления потенциала развития являются Москва, С.Петербург, Казань, Екатеринбург. Также правомочно мнение о целесообразности равномерного распределения всех составляющих, которое способствует их согласованному развитию. К такому мнению, например, приходят специалисты по проблемам регионального устройства Федеральной Республики Германии.

Равномерное распределение потенциала развития между составными частями СЭС, т.е. между ее регионами во многом объясняется возможностью формирования дополнительной синергии, содействующей не только развитию всех региональных структур, но также влияет на сохранение структурной устойчивости конструкции равномерного распределения потенциала развития.

На формирование моноцентричного или равномерного распределения потенциала развития структурных частей СЭС во многом влияет их обеспеченность природными ресурсами, наличие плодородных земель для развития сельского хозяйства, распределение промышленного потенциала, возможностей для развития туризма, лечения и отдыха и до [1]. Перераспределение потенциала развития между структурными частями СЭС во многом зависит от выбора и реализации структурной политики, а ее реализация, прежде всего, возможна на основе выбора целевых проектов развития составных частей СЭС.

Проектное управление развитием широкомасштабных систем известно и успешно развивается в мире с середины прошлого века. Первоначально в СССР оно было связано с освоением методов сетевого планирования и управления (СПУ), а основное внимание первоначально было сосредоточено на завершении проектов в намечаемый срок. Далее в процессе развития СПУ стали учитываться стоимость реализации проекта и возможные риски при их выполнении. Позже стали обращать внимание на качество выполняемых работ и технологию их выполнения. Одновременно с развитием статистического подхода к оценке длительности и стоимости выполнения работ получили развитие процессы управления активными системами [2], учитывающими интересы и возможность интенсификации выполнения работ. Увеличение количества проектов, их стоимости, размеров потерь из-за их несвоевременного выполнения сформировали проблему обоснования, подготовки и отбора проектов разного назначения.

В прошлом веке проблема формирования целей и перспектив развития СЭС не рассматривалась как масштабная, многосвязная и много объектная, то уже в начале XXI века количество возможных целей развития современных СЭС существенно возросло, а их рассмотрение, согласование и отбор постепенно превратилось в проблему, требующую современного методического и

информационного обеспечения. Постепенно от традиционных вопросов «что, когда и сколько» пришлось перейти к поиску ответов: «зачем и кому это выгодно?», что характерно для двухсекторной рыночно-государственной экономики. В связи с этими условиями проектное управление все больше ориентируется на обоснование целевой составляющей, технологической и организационно-финансовой компоненте.

Управление проектами (инновационными, инновационно-инвестиционными, инвестиционными) нередко предлагается рассматривать как самоорганизующуюся сложную систему, где каждый ее компонент попарно взаимодействует друг с другом, содействуя достижению общей цели, при условии ее непротиворечивого и бесконфликтного задания с учетом интересов всех активных участников (руководителя проекта, координатора проекта, регулирующего взаимодействие участников, базовых исполнителей работ, ответственного за материально-техническое и информационное обеспечение проекта и др.). К такому мнению приходят Уитти и Мейлор [3], полагая, что целевой проект – это сложная система, состоящая из множества взаимодействующих компонентов, поведение которой является эмерджентным. Сложность системы проявляется в эмерджентности ее взаимосвязанных частей, когда некоторая часть в отдельности не обладает свойством положительной (содействующей развитию) эмерджентности, т.е. целостности и системности.

Накопленный мировой опыт управления проектами может быть полезно использован при разработке современных основ проектного управления в РФ.

Несмотря на пандемию и падение ВВП РФ в 2020 году на 3,1% экономисты и руководители крупных компаний уверены в возможности роста экономики РФ в ближайшие годы [4,5].

Эта уверенность основана на объективной оценке располагаемого экономического потенциала, понимании накопленных ранее «узких мест» и возможных способов их преодоления [6]. Главным изменением в механизме управления развитием на макроуровне, является переход к стратегическому планированию развития на основе освоения проектного подхода, который может быть основой при формировании стратегий. Такой подход обеспечивает взаимосвязь намечаемых целей развития,

ожидаемых результатов их достижения, необходимых для этого ресурсов, нормативных и административных мер поддержки.

В качестве методической основы формирования развития СЭС может быть использован матричный проектно-целевой подход к определению возможного перечня проектов. Особенности такого подхода применительно к региональному и муниципальному уровню рассмотрены в работе [7]. Далее излагаются особенности проектно-целевого подхода применительно к макроуровню. Переход от одной матрицы к следующей, с одной стороны, основан на использовании дополнительной информации о проекте в следующей матрице, полученной на пересечении строк и столбцов предыдущей. При этом предполагается использование новой информации в качестве одной из компонент при построении следующей матрицы.

С другой стороны, накопление информации о проекте соответствует увеличению синергии, т.е. росту потенциала проекта. В качестве допустимой логической последовательности определения компонент проекта может быть принята следующая: тренды и «узкие места» → способы их преодоления (технология) → точки роста → цели национального развития → эффективные проекты → ресурсы.

Основой формирования целей развития являются прогнозы социально-экономического развития в среднесрочной перспективе. Прогнозы основываются на анализе текущего состояния, мировых и российских трендах социально-экономического развития, возможностях преодоления сложившихся и ожидаемых в перспективе «узких мест», включая большие вызовы.

Формирование последовательности действий по переходу от прогнозов социально-экономического развития к перечню проектов на макроуровне на основе целевого подхода и анализа возможностей, удобно представить в виде последовательности матриц с учетом увеличения синергии, где начальной является матрица «тренды и «узкие места» х точки роста». В результате ее анализа на основе сопоставления перспективных трендов развития с составом накопившихся и возможных в перспективе «узких мест» формируется множество точек перспективного развития. Такие точки могут быть отображены в виде перспектив достижения различными секторами экономики и видами экономической

деятельности дополнительных объемов производства и (или) нового качества выпускаемой продукции.

Вторая матрица «точки роста х технологические возможности» предполагает поиск возможных технологических способов реализации целей обозначаемых точками роста. Технологические возможности отражают технологии, распределенные по четырем народнохозяйственным комплексам, а также наличие освоенных и осваиваемых технологий для определенных технологических переделов. Следует подчеркнуть, что, например, количество освоенных российских технологий в области нефтехимии и нефтепереработки не превышает 80-ти, в то время как количество технологий стран ЕС в этих отраслях превышает этот уровень почти на порядок.

Возможные точки роста, достижимые на основе возможных технологических способов, формируют основу проектов развития, включающих цель, исходное состояние и технологию достижения установленной цели, которые могут быть получены на основе третьей матрицы: «цель проекта х технология ее достижения». Такой анализ позволяет определить состав технологически возможных проектов, способных достичь намечаемых в проекте целей с требуемым качеством и принятыми целевыми нормативами, обеспечивающими полезность и эффективность проекта.

Четвертая матрица «намечаемые проекты х цели национального развития» позволяет установить возможности влияния ожидаемых результатов выполнения каждого проекта на приближение к достижению соответствующей национальной цели. Если обозначить множество проектов $N = n_{1,} n_2,.., n_h$, а множество целей как $M = m_{1,} m_2,.., m_h$ то оценку уровня соответствия каждого n_i проекта (при условии аддитивности полезности целей) множеству целей M можно обозначить как

$$Q_i = \sum_{j=1}^{h} q_{ij}, \qquad (1)$$

где q_{ij} – уровень значимости n_i проекта для достижения m_j цели. В качестве возможного варианта оценки $\{q\}$ удобно использовать порядковую шкалу q= 0,1,2,3, что означает 1 –

положительное влияние, 2 – сильно положительное влияние, 3 – безусловно, положительное влияние.

Несмотря на хозяйственную самостоятельность, российские компании подчиняются в соответствии с п. 75.1 Конституции России правилам ведения бизнеса и перспективам социально-экономического развития страны. В соответствии с Законом о стратегическом планировании, выбор целей и стратегии развития компании должен быть согласован со стратегией развития экономики в целом. В качестве основы для этого могут служить цели развития экономики на ближайший период, обозначенные в Указе о национальных проектах. При этом как принятые ранее, так и вновь формирующиеся проекты национального уровня, должны учитывать принятые ранее цели и ожидаемые результаты.

Пятая матрица «эффективные проекты х ресурсное обеспечение проектов» предполагает рассмотрение требований к ресурсному обеспечению каждого эффективного проекта к его ресурсному обеспечению. Под ресурсным обеспечением, прежде всего, понимаются необходимые финансовые ресурсы, выделяемые из бюджета, а также средства компаний заинтересованных в участии в проекте (программе) и в использовании результатов проекта (программы) в интересах компании. В итоге должна быть получена таблица, в которой для каждого проекта указана потенциальная эффективность достижения целей социального развития, а также размеры финансирования проекта за счет госбюджета и средств заинтересованных компаний.

Основная идея на начальном этапе механизма согласованного управления проектами в иерархической социально-экономической системе состоит в следующем: выявить и упорядочить по предпочтению проекты развития каждого уровня. Для этого каждый проект необходимо оценить с точки зрения вклада в достижение цели соответствующего уровня, необходимых затрат и величины риска. Все проекты оцениваются в рамках трехлетнего периода. Далее используется совокупная оценка эффективности проектов верхнего уровня, а также оценка уровня регионов в совокупности муниципалитетов. Затем дается сравнительная оценка проектов развития с прошлым трехлетним периодом и оценка динамики изменения потенциала развития для каждого уровня. После этого

формируются оценки выявленной динамики развития всей иерархической СЭС.

Стратегический план на макроуровне должен быть основан на перспективных проектах, обеспеченных ресурсами, а цели проектов должны соответствовать национальным целям. Стратегия, как инструмент управления ресурсами для достижения перспективных целей, имеет конкретное значение для различных мировых экономик. При этом различают европейский подход, сложившийся в странах ЕС (Германия, Франция, Великобритания) и восточный подход, принимаемый рядом стран АТР (Корея, Япония, современный Китай и др.). В странах ЕС предпочтительной считается стратегия, основанная на последовательной реализации намечаемых целей, с учетом возможности использования полученных результатов при формировании и достижении новых целей. В восточных странах главный акцент делается на гармоничности развития, где учитываются разные составляющие развития (экономика, промышленность, общественное развитие, экология и др.). Если с этих позиций оценивать намеченные и реализуемые цели развития СССР и России, то принимавшиеся стратегии можно условно назвать поступательно-возвратными, когда намеченной цели не всегда удавалось достичь результатов в полном объеме, а частично достигнутые результаты не использовались при обосновании и достижения новых целей.

В перспективе при формировании стратегии развития нашей страны желательно совместить европейский и восточный подходы, а стратегию развития считать адаптационной и гармоничной, способной в процессе ее реализации учесть перспективы развития основных составных частей: экономики, состояние общества, науки и технологии, экологии и интересы будущих поколений.

Заключение

1. Формирование и целевое управление инвестиционными проектами и развитием иерархических СЭС может быть эффективно использовано в качестве методической основы формирования стратегии и стратегических планов.

2. В качестве основы обоснования целей, состава и содержания проектов может быть использован подход к формированию информационных матриц, с помощью которых последовательно

определяется содержание и формируются оценки целей и основных компонент проектов.

3. Использование матричного подхода позволяет последовательно получать нормативные экспертные и статистические оценки с учетом общей логики формирования проектов, а также привлекать необходимых экспертов для углубленного анализа проектов различных уровней.

Литература:

1. *Михеева Н.И.* Пространственные аспекты разработки экономических прогнозов. Научный доклад ИНП РАН. – М.: ИНП РАН, 2021. – 122 с. – URL: https://ecfor.ru/publication/prostranstvennye-aspekty-razrabotki-ekonomicheskih-prognozov/ (дата обращения 10.10.2021).

2. *Бурков В.Н.* Основы математической теории активных систем. – М.: Наука, 1977. – 255 с.

3. *Whitty S., Maylor H.* And then came complex project management // International journal of project management. – 2009. – Volume 27. Issue 3. – P. 304-310.

4. *Аганбегян А.Г.* Кризис как основа возможностей // Научные труды Вольного экономического общества России. – 2020. – Т. 223. №3. – С. 47-69.

5. *Широв А.А.* Возможности и риски посткризисного восстановления экономики // Научные труды Вольного экономического общества России. – 2020. – Т. 223. №3 – С. 75-80.

6. *Комков Н.И.* Условия и возможности преодоления экономического кризиса // МИР (Модернизация. Инновации. Развитие). – 2021. – Т.12. № 3. – С. 206-221.

7. *Комков Н.И., Лазарев А.А., Романцов В.С.* // МИР (Модернизация. Инновации. Развитие). – 2018. – Т. 9. № 4. – С. 560-575.

Chilachava T., Pochkhua G., Rusetsky A.

Mathematical model of conflict region in case of three population groups with different priorities

Abstract: The paper proposes a new nonlinear mathematical model, describing in a certain politically conflicting region of a certain state the presence of three population groups with different political priorities. One part of the population (unionists) is politically oriented towards the preservation of the region within the former state, the second part of the population of the region supports the idea of separatism, the separation of the region from the state in order to form a new independent state (separatists), the third part of the population of the region supports the idea of irredentism of the region, that is, secession in order to join another, possibly bordering state (irredentists). A weak (simple majority of the population of the region) and strong (qualified majority of the population of the region) conditions are proposed, which in the legal sense may not have direct consequences, but may determine the aspirations of the majority of the population of the region. The model is described by a nonlinear three-dimensional dynamic system with variable coefficients. Under some assumptions on model parameters, exact analytical solutions were found. Additional conditions were found under which: the region remains within the previous state; possible separation of the region; the irredentism of the region, that is, its accession to another state, is possible.

Keywords: mathematical model, unionists, separatists, irredentist, conflict

An innovative approach seems to us to study a number of actual social processes, such as the assimilation of languages, globalization, the settlement of political conflicts, the separation of regions, the territorial integrity of states, etc.

From our point of view, the only scientific approach to an adequate quantitative and qualitative description of these complex processes is their mathematical modeling, i.e. the creation of appropriate mathematical models, in the form of multidimensional nonlinear dynamic systems.

We have previously proposed original mathematical models: linguistic globalization, which establishes, within the framework of the model, the possibility of globalization in English [1]; two and three levels of assimilation of languages (peoples) by more common languages [2-4].

We also proposed mathematical models for the settlement of political (not military confrontation) conflicts through the economic cooperation of parts of the populations of the sides with the participation of international organizations and relevant investment funds [5,6].

Over the past few decades, due to the desire of some political players to redistribute the world map, issues related to the self-determination of nations and the possibility of creating independent states have become relevant.

The paper [7] proposes a general nonlinear mathematical model, which describes the process of the possibility of secession of a particular region from a certain state. The model assumes that only two categories of citizens live in a particular region of a state: the first category, which is a supporter of the center (unionists) and opposes the secession of the region; the second is a supporter of the secession of the region (secessionists, separatists), i.e. its separation from the center, with the aim of forming a new independent state.

We propose a new mathematical model, which is described by the following nonlinear dynamic system

$$\begin{cases} \frac{du(t)}{dt} = \alpha_1(t)u(t) + \big(\beta_1(t) - \beta_2(t)\big)u(t)v(t) + \big(\beta_1(t) - \beta_3(t)\big)u(t)w(t) - \\ \qquad -\gamma_5(t)u(t) - \gamma_3(t)u(t) + \gamma_1(t)v(t) + \gamma_2(t)w(t) \\ \frac{dv(t)}{dt} = \alpha_2(t)v(t) + \big(\beta_2(t) - \beta_1(t)\big)u(t)v(t) + \big(\beta_2(t) - \beta_3(t)\big)v(t)w(t) + \\ \qquad +\gamma_3(t)u(t) - \gamma_1(t)v(t) - \gamma_6(t)v(t) + \gamma_4(t)w(t) \\ \frac{dw(t)}{dt} = \alpha_3(t)w(t) + \big(\beta_3(t) - \beta_1(t)\big)u(t)w(t) + \big(\beta_3(t) - \beta_2(t)\big)v(t)w(t) + \\ \qquad +\gamma_5(t)u(t) + \gamma_6(t)v(t) - \gamma_2(t)w(t) - \gamma_4(t)w(t) \end{cases} \quad (1)$$

with initial conditions

$$u(0) = u_0,\ v(0) = v_0,\ w(0) = w_0, \quad (2)$$

where

$u(t)$ is the number of supporters of the center (unionists) in the region at time t,

$v(t)$ is the number of supporters of separation from the center in order to create a new independent state (separatists) at the moment t,

$w(t)$ is number of supporters of separation from the center in order to join another state (irredentists) at a time t,

$\alpha_1(t), \alpha_2(t), \alpha_3(t) -$ are demographic factors of the corresponding parts of the population of the region,

$\beta_1(t), \beta_2(t), \beta_3(t) -$ are factors of influence on opponents, in order to attract them to their side (unionism, separatism, irredentism),

$\gamma_1(t), \gamma_2(t) -$ factors of influence of the federal side (the central government of the state) on separatists and irredentists, respectively, in order to attract them to the unionist side,

$\gamma_3(t), \gamma_4(t) -$ factors of influence of external (contributing to separatism) and internal (de facto government) forces on unionists and irredentists, respectively, in order to attract them to the separatist side,

$\gamma_5(t), \gamma_6(t) -$ factors of influence of external interested forces (other state) on unionists and separatists, respectively, in order to attract them to irredentism (reunification with another state),

$[0, T] -$ time interval, model review.

In the model, it is more logical (adequacy of the model) to assume that at the initial moment of time unionists outnumber the total number of separatists and irredentists

$$u_0 > v_0 + w_0. \tag{3}$$

We will consider the weak and strong conditions under which separation of the region is possible, with the aim of creating an independent state (separation of the region) or joining another state (irredentism), which implies the fulfillment of the following inequalities

$$\frac{v(t)}{u(t) + v(t) + w(t)} > \frac{1}{2}, \qquad t > t_1, \tag{4}$$

$$\frac{v(t)}{u(t) + v(t) + w(t)} > \frac{2}{3}, \qquad t > t_2, \tag{5}$$

$$\frac{w(t)}{u(t)+v(t)+w(t)} > \frac{1}{2}, \qquad t > t_3, \tag{6}$$

$$\frac{w(t)}{u(t)+v(t)+w(t)} > \frac{2}{3}, \qquad t > t_4. \tag{7}$$

Weak conditions (4), (6) imply that more than half of the population of the region supports separatism or irredentism, respectively, and strong conditions (5), (7) – more than two thirds of the population of the region (a qualified majority) supports the idea of separating the region and creating a new independent state or reunification with another state.

If none of the inequalities (4)-(7), taking into account (3), then the separation and irredentism of the region is impossible and the conflict region remains part of the previous state.

Consider a special case where there is no influence of forces external to the region (outside the state, as well as the federal center), and unionists, separatists and irredentists only decide among themselves on the choice of the path of political development of the region.

In this case, in the system of equations (1), it is necessary to assume

$$\gamma_i(t) \equiv 0, \qquad i = \overline{1,6.} \tag{8}$$

Suppose also that the demographic factors of the three parts of the population of the region are zero

$$\alpha_j(t) \equiv 0, \qquad j = \overline{1,3.} \tag{9}$$

The nonlinear system of differential equations (1) (nonlinear three-dimensional dynamic system), taking

$$\begin{cases} \frac{du(t)}{dt} = \big(\beta_1(t) - \beta_2(t)\big)u(t)v(t) + \big(\beta_1(t) - \beta_3(t)\big)u(t)w(t) \\ \frac{dv(t)}{dt} = \big(\beta_2(t) - \beta_1(t)\big)u(t)v(t) + \big(\beta_2(t) - \beta_3(t)\big)v(t)w(t)\,. \\ \frac{dw(t)}{dt} = \big(\beta_3(t) - \beta_1(t)\big)u(t)w(t) + \big(\beta_3(t) - \beta_2(t)\big)v(t)w(t) \end{cases} \tag{10}$$

From (10), (2), we get the first integral of a three-dimensional dynamic system

$$u(t) + v(t) + w(t) = u_0 + v_0 + w_0 \equiv p. \tag{11}$$

Consider a special case

$$\beta_1(t) \equiv \beta_2(t) \neq \beta_3(t), \qquad t\epsilon[0,T]. \tag{12}$$

Considering (12), the second first integral (10), (2) has the following form:

$$v(t) = qu(t), \qquad q = \frac{v_0}{u_0}. \tag{13}$$

The first two integrals (11), (13) of the dynamic system (10), (2), allow us to find its exact analytical solution

$$\begin{cases} u(t) = \dfrac{pu_0 e^{p\int_0^t(\beta_1(\tau)-\beta_3(\tau))d\tau}}{w_0 + (u_0+v_0)e^{p\int_0^t(\beta_1(\tau)-\beta_3(\tau))d\tau}}. \\ v(t) = qu(t) \\ w(t) = p - (q+1)u(t) \end{cases} \tag{14}$$

Consider a second special case

$$\beta_1(t) \equiv \beta_3(t) \neq \beta_2(t), \qquad t\epsilon[0,T]. \tag{15}$$

Considering (15), the second first integral (10), (2) has the following form:

$$v(t) = q_1 w(t), \qquad q_1 = \frac{w_0}{u_0}. \tag{16}$$

The first two integrals (11), (16) of the dynamic system (10), (2), allow us to find its exact analytical solution

$$\begin{cases} u(t) = \dfrac{pu_0 e^{p\int_0^t(\beta_1(\tau)-\beta_2(\tau))d\tau}}{v_0 + (u_0 + w_0)e^{p\int_0^t(\beta_1(\tau)-\beta_2(\tau))d\tau}}. \\ v(t) = q_1 w(t) \\ v(t) = p - (q_1 + 1)u(t) \end{cases} \quad (17)$$

Analysis of the obtained exact analytical solution of the Cauchy problem (10), (2) for a nonlinear three-dimensional dynamic system, under the natural assumption (3) (unionists prevail in the region at the initial moment of time) shows that:

In case of execution of inequality system

$$\begin{cases} \beta_1(t) \geq \beta_2(t) \\ \beta_1(t) \geq \beta_3(t) \end{cases}, \quad t\epsilon[0,T] \quad (18)$$

separation or irredentism of the region is impossible and the region in the legal sense remains within the former state.

In case of execution of system

$$\begin{cases} \beta_1(t) \equiv \beta_2(t) \\ \beta_3(t) > \beta_1(t) \end{cases}, \quad t\epsilon[0,T] \quad (19)$$

according to (14), regional irredentism is possible (fulfillment of condition (6) or (7)), wherein time t_3 or t_4 is determined from integral relations

$$\begin{aligned} \int_0^{t_3} \big(\beta_3(\tau) - \beta_1(\tau)\big)d\tau &= \frac{ln\frac{u_0 + v_0}{w_0}}{p}, \\ \int_0^{t_4} \big(\beta_3(\tau) - \beta_1(\tau)\big)d\tau &= \frac{ln\frac{2(u_0 + v_0)}{w_0}}{p}. \end{aligned} \quad (20)$$

In case of execution of system

$$\begin{cases} \beta_1(t) \equiv \beta_3(t) \\ \beta_2(t) > \beta_1(t) \end{cases}, \quad t\epsilon[0,T] \quad (21)$$

according to (17), it is possible to separate the region (condition (4) or (5)), wherein time t_1 or t_2 is determined from integral relations

$$\int_0^{t_1}\big(\beta_2(\tau)-\beta_1(\tau)\big)d\tau=\frac{ln\dfrac{u_0+w_0}{v_0}}{p},$$
$$\int_0^{t_2}\big(\beta_2(\tau)-\beta_1(\tau)\big)d\tau=\frac{ln\dfrac{2(u_0+w_0)}{v_0}}{p}. \qquad (22)$$

In conclusion, we would like to note that the proposed mathematical model (1), (2) is common and with variable coefficients of a dynamic system can well describe many conflict regions existing in the world. At the same time, specific conflicts have their own specific sides, characterized by the historical past, the character and mentality of the politically opposing sides (peoples), the geopolitical location and economic potential of the region, the interest of the bordering states, etc., which can be taken into account by the variable parameters of the model.

Naturally, with variable coefficients of the mathematical model (1), (2), its analytical solution is impossible, so it is necessary to use computer modeling, using tested computer computing programs.

References:

1. *Temur Chilachava.* Research of The Dynamic System Describing Globalization Process / Springer Proceedings in Mathematics & Statistics, Mathematics, Informatics and their Applications in Natural Sciences and Engineering. – 2019. – Vol. 276. – P. 67-78.

2. *Temur Chilachava, George Pochkhua.* Research of a three-dimensional nonlinear dynamic system describing the process of two-level assimilation // 4open. – 2020. – Vol. 3. №10. – P. 1-8.

3. *Temur Chilachava, Sandra Pinelas, George Pochkhua.* Research of four-dimensional dynamic systems describing processes of three level assimilation // Differential and Difference Equations with Applications. Springer Proceedings in Mathematics & Statistics. – 2020. – Vol. 333. – P. 281-297.

4. *Temur Chilachava, George Pochkhua.* The mathematical model of the survival of small nations. Tskhum-Abkhazian Academy of Sciences Proceedings Books. – 2020. – Vol. XIX-XX. – P. 219-229.

5. *Temur Chilachava, George Pochkhua.* Mathematical and Computer Models of Settlements of Political Conflicts and Problems of Optimization of Resources // International Journal of Modeling and Optimization. – 2020. –Vol. 10. №4. – P. 132-138.

6. *Temur Chilachava, George Pochkhua.* Conflict resolution models and resource minimization problems / Applications of Mathematics and Informatics in Natural Sciences and Engineering. Springer Proceedings in Mathematics & Statistics. – 2020. – Vol. 334. – P. 47-59.

7. *Temur Chilachava, George Pochkhua, Alexander Rusetsky.* Mathematical model of secession of the region / Problems of management of safety of difficult systems. The XXVIII International Conference (Moscow). – M.: Institute of Control Sciences of RAS, 2020. – P. 353-359.

Сутягин В.В., Усманова Т.Х.

Социальная безопасность в развитии экономики

Аннотация: Формирование стратегий экономического развития в рамках государственного регулирования должна отвечать целям и задачам гуманистического планирования. Во главе угла гуманистического планирования должен стоять человек и его интеллектуальное и физическое развитие. Социальные показатели социально-экономического развития должны отвечать высоким стандартам развития человека. Актуально создание комфортных условий труда с учетом технических, медицинских, этических, психофизиологических и даже эстетических составляющих. В современных условиях хозяйствования важны уровни демократизации управления и качество человеческих отношений: свобода, ответственность, справедливость, мораль. Инновации должны способствовать достижению целей и задач, которые определяются разумом и волей человека.

Ключевые слова: экономика, эффективность, система, развитие, население, социальная сфера, безопасность

В большинстве стран мира подтверждена прямая зависимость уровня развития экономики от совершенства инновационной политики. Однако отмечено, что в успешности достижения инновационного технологического прогресса социальный статус населения, уровень его жизни играют важную роль.

Развитие важнейшей составной части социально-экономической системы (СЭС) экономики зависит от качества ее взаимодействия с другими направлениями: социальной сферой, научным инновационно-технологическим сектором, экологической средой. Объединение этих направлений обеспечивает эмерджентность, синергию в развитии СЭС [1]. Сложность анализа закономерностей развития СЭС заключается в необходимости учета трансформации самих СЭС.

При формировании стратегий экономического развития и путей их реализации на уровне государственного планирования или частных компаний личные интересы политиков часто препятствуют проявлению их честности и способности к гуманистическому социальному планированию.

Человек, приспосабливаясь к социальным условиям, развивает в себе те черты характера, которые побуждают его желать действовать именно так, как диктуют ему условия, в которых приходится действовать. Поскольку структура личности большинства людей в обществе имеет социальный характер, она приспособляется к решению тех объективных задач, которые индивид должен выполнять в обществе. В этом процессе психологическая энергия людей может последовательно превращаться в производительную силу, способствующую повышению эффективности экономики.

Для достижения максимальной эффективности экономики условия труда и жизнедеятельности человека, а также эффективность управления во внешнем и внутреннем административных уровнях имеют особое значение,

Концентрированным выражением внутреннего производственного уровня является процесс создания для человека максимально благоприятных условий труда, которые касаются всей совокупности деятельности человека: трудового процесса, окружающей (производственной) среды, внешнего оформления места работы, отношения работника к выполняемой работе. Эти

факторы оказывают влияние на функциональное состояние организма человека: его здоровье, продолжительность жизни, работоспособность, удовлетворенность трудом, его эффективность, а также воспроизводство рабочей силы.

Совершенствование трудового процесса начинается с технологий, которые являются связующим звеном между работниками и материально-вещественными элементами трудового процесса, т.е. с предметами и средствами труда. Технологии ориентированы на обеспечение удовлетворенности человека содержанием и методами труда, на используемую технику, возможность развития профессионально-квалификационного потенциала, а также на обеспечение безопасности труда и устранение негативного воздействия технологии и применяемого оборудования на окружающую среду. Социальным требованиям в большей степени отвечают такие технологические решения, которые предусматривают автоматизацию производственных процессов, в результате чего человек выводится из зоны воздействия различных неблагоприятных факторов. Возможны и другие подходы, предусматривающие разработку социально-технологических моделей построения трудовых процессов, как изменение форм организации трудовой деятельности или, например, повышение уровня эргономичности используемых технических средств и оборудования и др.

При определении критериев влияния трудового процесса на организм человека целесообразно рассматривать всю эту организационную систему с участием в ней самого человека, с точки зрения воздействие на человека следующих психофизиологических факторов:

1. Ориентировочная оценка по критерию тяжести труда.

2. Оздоровление окружающей (производственной) среды, обеспечение благоприятной для человека микроэкологии труда, формирующейся под воздействием технологических факторов (применяемых материалов, оборудования, режимов производственного процесса), а также общего состояния окружающей атмосферы.

3. Эстетизация места работы. Как известно, качество оформления интерьера, рабочих мест и спецодежды играет далеко

не последнюю роль в формировании благоприятной атмосферы для производительного труда работников и сохранения их здоровья.

4. Мотивация самоохраны труда, ориентирующая работников на формирование у них заинтересованного отношения к выполняемой работе, улучшению условий и охраны груда на рабочих местах.

Миссия улучшения условий труда состоит в том, чтобы вводить элементы комфорта, избавляясь от элементов риска. На это должны быть направлены совместные усилия предпринимателей, профсоюзов и органов государственной власти.

Важное значение имеют индикаторы уровня жизни населения, по которым можно косвенно оценивать степень развитости экономики.

Специальная комиссия ООН и другие международные организации дают частные индексы, оценивающие состояние человеческого потенциала, например, возможность для граждан участия в процессе принятия решений, трудовые мотивации, невмешательство государства в развитие бизнеса и т.д.

Объективность социальных показателей и выбор их адекватной, репрезентативной системы значительно осложнен необходимостью учета того факта, что каждая страна или группы стран, близких по качеству жизни, культурным традициям, менталитету, имеет свои показатели, опирающиеся на собственные социальные и культурные ценности.

Одни и те же показатели в различных странах могут формировать различную информацию. Трудовые мотивации различны в развитых и периферийных странах. Отличается понимание роли государства в экономике, уровень демократизации управления и качество человеческих отношений: свобода, ответственность, справедливость, мораль.

Особенно важно учитывать это обстоятельство в том случае, когда социальные индикаторы играют роль механизма управления экономическим развитием.

Необходимой базой социально-экономического развития является принцип гуманизации, который является интегральным социокультурным результатом экономической, финансовой, структурной и инвестиционной политики, системы принятия и исполнения законов, обеспечивающих воспроизводство

человеческого потенциала – важнейшего фактора эффективного экономического развития [1].

Существующие методы оценки социально-экономического развития меняются и не могут быть универсальными. Для получения объективных результатов оценки, целесообразно проводить мониторинг индикаторов, отражающих процесс развития.

По сути дела, одни и те же показатели в различных странах могут формировать различную информацию. Трудовые мотивации различны в развитых и периферийных странах. Отличается также понимание роли государства в экономике, уровень демократизации управления и качество человеческих отношений: свобода, ответственность, справедливость, мораль.

В прошедшие исторические периоды в России для развития экономики власти определяли действительно актуальные в каждый период цели. В период плановой экономики это энергетика, включая производство электроэнергии и добычу минеральных ресурсов (угля, нефти, газа). В период перехода от плановой к рыночной экономике это финансовые средства, аккумулированные в банках и финансовых структурах. В последнее десятилетие – противодействие инфляции; обеспечение макроэкономической стабильности [1].

Однако в течение этих исторических периодов экономического развития фактически не уделялось внимания росту социального уровня населения, хотя в законодательных документах это практически всегда находило отражение. На наш взгляд, такая ситуация явилась основной причиной случаев массового недовольства населения [2].

Избежать такой ошибки в развитии экономики удалось власти Китая [3,4].

Эффективность экономики Китая была обеспечена рациональным государственным управлением с ориентацией на повышение уровня жизни населения. Экономический успех был достигнут благодаря эффективному государственному регулированию, включающему использование рыночных мотиваций с одновременным ограничением деятельности бизнеса.

Заключение

1. При формировании стратегий экономического развития и путей их реализации на уровне государственного планирования или частных компаний, личные интересы политиков часто препятствуют проявлению их честности и способности к гуманистическому планированию. Подобная опасность может быть значительно уменьшена или вообще исключена, если граждане смогут более активно участвовать в процессе принятия решений. Если можно будет найти какие-либо приемлемые способы и методы, с помощью которых планирование будет контролироваться теми, ради тех, для кого это планирование осуществляется.

2. Не столько техника, сколько сам человек должен стать единственным источником ценностей. Оптимальное развитие человека, а не максимальная производительность должны служить критерием для всех видов планирования и развития экономики.

3. Социальные параметры должны оказать влияние на формирование социальных стратегий, их первоочередной коррекции. Для этого в соглашениях по социальному партнерству необходимо обеспечить возможность установления конкретных социальных показателей.

4. Справедливость и безопасность условий труда в современном мире должна быть связана не только с соблюдением технических и медицинских норм безопасности труда, но и с созданием комфортных (в широком смысле) условий труда с учетом технических, медицинских, этических, психофизиологических и даже эстетических составляющих.

5. Одни и те же социальные показатели в различных странах могут формировать различную информацию. В развитых и периферийных странах различны трудовые мотивации. Отличается понимание роли государства в экономике, уровень демократизации управления и качество человеческих отношений: свобода, ответственность, справедливость, мораль.

6. Инновации должны рассматриваться не только, в общем, как средство экономического роста, но и как средство для достижения целей, определяемых разумом и волей человека. Ценности, влияющие на планирование и развитие экономики, должны реализоваться на основе знания человека, различных его особенностей, оптимального его развития, а также реальных потребностей, способствующих этому развитию. Именно в этом

проявляется социальная безопасность в процессе экономического развития.

Литература:

1. *Комков Н.И.* Проблемы управления развитием крупномасштабных социально-экономических систем: анализ, опыт, методические основы и перспективы. – Москва: ООО Издательский дом «Наука», 2020. – 152 с.

2. *Иноземцев В.Л.* «Борьба амбиций: как за 30 лет Китай догнал и перегнал Россию». – URL: https://www.rbc.ru/opinions/economics/21/02/2017/58abf4239a7947ffded4e0c5 (дата обращения 12.10.2021).

3. Китай усилил давление на олигархов. России пора брать пример. – URL: https//vk.com›wall185402730_130962 (дата обращения 12.10.2021).

4. *Морозов М.П.* Секрет успеха Китая – обеспеченный народ, а не верхушка власти. – URL: https://news.rambler.ru/world/46869447/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения 12.10.2021).

Тимошенко А.А.

Криптовалюты как угроза национальной безопасности России: юридические механизмы противодействия

Аннотация: В работе на основе анализа данных об уровне распространенности криптовалют, их востребованности в сфере теневой экономики предпринята попытка обозначить ключевые способы юридического противодействия данной угрозе национальной безопасности.

Ситуация осложнена невозможностью технологически обеспечить исполнение правового запрета на использование данного альтернативного средства платежа.

Только анализ множества факторов трансформации сложной системы социума позволит в конце концов выработать эффективные средства правовой защиты интересов государства и общества от попытки бесконтрольного воздействия на ключевые сферы

общественных отношений: государственное управление, экономику, реализацию прав и свобод индивида.

Ключевые слова: блокчейн, уголовное право, уголовное судопроизводства, криптовалюта

Следует с очевидностью признать, что к настоящему времени мир в лице криптовалют получил инструмент выстраивания альтернативных финансовых отношений между индивидами, их объединениями, а в некоторых случаях и государственными образованиями (речь, прежде всего, идет о государствах, признавших данное средство платежа в качестве официально допустимого – Эстония, Украина, отдельные штаты США и другие).

Сама по себе криптотехнология, лежащая в основе этого вида цифровых финансовых активов относительно проста: обеспечивается распределенное хранение данных на множестве носителей, что делает невозможным подделку общего реестра с использование изначально ограниченного доступа к средствам ввода информации в общий реестр [1-4].

При образовании криптовалют информация, значимая для создания базы данных на основе технологии блокчейн, состоит из записей о количестве операций, совершенных лицами, имеющими криптодоступ к ее содержанию. В результате их суммарного математического исчисления можно определить статус электронных кошельков с присвоенными владельцам условными денежными единицами (токенами: биткоинами, эфиром и т.д.).

За счет простоты собираемых сведений объем всех записей, к примеру, самой популярной мировой криптовалюте с 2009 года по настоящее время не превышает 400 Гб [5].

Появление данного механизма расчетов, его активная пропаганда на протяжении прошедшего десятилетия происходила на фоне все усиливающейся роли государства и его финансовых институтов по контролю за осуществлением платежей.

Является криминалистической аксиомой утверждение, что эффективный способ обнаружения лиц, совершивших корыстные преступления, связан с установлением выгодоприобретателей похищенного имущества. Данное действие выполнить проще, если

расчеты осуществлялись в безналичной форме: достаточно определить конечного получателя денежных средств.

Конечно, в своей практической деятельности правоохранительные органы сталкивалась с фактами запутывания финансовых операций, когда после вывода со счета жертвы деньги в целях распыления перечислялись на тысячи банковских счетов фирм-однодневок, перемешивались с другими денежными потоками и затем выводились на подконтрольные участникам организованных групп офшорные компании с целью аккумулирования и обналичивания.

В ряде случае выявлялись специализированные группировки, создававшие альтернативные официальным системы теневого бухгалтерского учета и управления расчетами, доступ и функционирование которых обеспечивалось с применение «облачных» компьютерных технологий.

С внедрением блокчейн-реестров финансовой информации в таком сложном механизме надобность отпала. Владельцы электронных криптовалютных кошельков изначально анонимны, а распространение теневых способов конвертации между цифровыми активами и официальными валютами делает использование биткоинов, эфира и других токенов идеальным способом расчета между участниками.

Стоит отметить, что у данного феномена есть и обратная сторона: периодически, при использовании услуг криптобирж предположительно их владельцы обеспечивают произвольное списание активов клиентов и прямой вывод ресурсов по собственному усмотрению. В настоящее время эффективных способов оспорить такие злоупотребления в мировой практике не выработано.

К примеру, по данным специализированных интернет-порталов, подобные инциденты происходят на крупнейших мировых криптобиржах [6].

Следует также отметить, что распространена практика использования цифровой валюты для оплаты криминальных услуг, а также для приобретения запрещенных товаров. К примеру, в Москве в 2018 году было совершено убийство следователя. В качестве вознаграждения киллеры получили 2 биткоина [7].

Ситуация усугубляется на фоне COVID-19 ростом (в России в 4 раза) киберпреступности, что позволило специалистам обозначить феномен в качестве киберпандемии [8].

Данное обстоятельство заставляет государственную власть задумываться о регулировании отношений по поводу криптовалют.

Во-первых, биткоин или любой другой токен может стать предметом взятки или способом аккумуляции похищенного имущества, в результате чего очевидна потребность в его аресте для обеспечения последующих взысканий.

Во-вторых, активность хозяйствующих субъектов или отдельных граждан в международных экономических отношениях и распространенность в мире вложения активов компаний в криптовалюты делает очевидным стремление к накоплению имущества, полностью исключенного от налогового или иного государственного учета.

В настоящее время в России в соответствии со ст. 14 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [9] допускается оборот криптовалют, зарегистрированных только в доменном пространстве Российской Федерации.

Между тем судебная практика более широко толкует данный подход и признает биткоины, выпущенные на зарубежных доменах, имуществом, в том числе для целей его ареста [10].

Однако исполнить его возможно только в случае получения доступа к криптокоду, открывающему соответствующий электронный кошелек.

В доктрине также единого мнения по данному вопросу не сложилось. В большинстве своем авторы предлагают урегулировать официальное использование универсальных цифровых валют, включая их анонсирование и выпуск [11-13].

Выделяется в целом положительное отношение к данной технологии. Так, например, специалисты в области криминологии, анализируя развитые блокчейн технологии 4-го поколения, предполагают, что в будущем при помощи этого инструмента можно поставить под контроль все цифровые финансовые активы, включив их упоминание в единый распределенный реестр данных

[14]. Однако конкретных путей выход из современных проблемных ситуаций авторы не называют.

Таким образом, на примере сложных вопросов оборота криптовалют со всей очевидностью вырисовывается множество факторов, подлежащих учету при их надлежащем юридическом регулировании.

Вот некоторые из них:

– потребность в установлении во внутреннем законодательстве правил обращения с общепризнанными криптовалютами;

– необходимость налаживания совместной работы правоохранительных и контролирующих органов по установлению обстоятельств обращения с криптовалютой и обеспечением деаномизации владельцев электронных кошельков;

– внедрение эффективных средств контроля за финансовыми операциями, совершаемыми с применением технологии блокчейн;

– создание государственной системы учета криптовалют для целей их мониторинга и анализа использования (с учетом изначальной открытости баз данных по всем существующим криптовалютам);

– внедрение реестра электронных кошельков и создание государственных криптобирж;

– борьба с теневыми крипторасчетами;

– обеспечение разъяснительной работы среди населения с целью исключить распространение финансовых пирамид, созданных под предлогом осуществления криптоторгов.

Данные меры станут более эффективными, если для их внедрения будет создана надлежащая правовая база.

Среди первоочередных правовых актов (решений), подлежащих принятию следует обозначить следующие:

– внесение изменений в Стратегию экономической безопасности Российской Федерации на период до 2030 года, утвержденную Указом Президента РФ от 13.05.2017 № 208 с введение в нее раздела, посвященного криптовалютам;

– подготовка поправок в Уголовный и Уголовно-процессуальный кодексы Российской Федерации, а также иные процессуальные кодексы в части ужесточения ответственности за

нарушение законодательства о цифровых финансовых активах, а также с целью установления механизмов ареста цифровых валют;

– наделение Правительства Российской Федерации и профильных ведомств полномочием регулировать и вносить оперативные изменения в порядок обращения с цифровыми финансовыми активами, подлежащими в Российской Федерации государственному контролю (по аналогии с действующим порядком установления видов наркотических средств и психотропных веществ, без изменения федеральных законов).

Только обеспечение принятия оперативных юридических мер – ответов на вызовы криптовалютного рынка с обязательным мониторингом обратной реакции системы общественных отношений позволит эффективно реализовать государственную политику по обеспечению национальной безопасности.

Исследование выполнено при поддержке РФФИ в рамках научного проекта № 18-29-16151 мк

Литература:

1. *Поппер Н.* Цифровое золото. – М.: «Диалектика», 2016. – 368 с.

2. *Криштаносов В.Б.* Блокчейн: технологический и экономический аспекты // Труды Белорусского государственного технологического университета. Серия 5. – 2020. – № 2 (238). – С. 13-32.

3. *Винья П., Кейси М.* Машина правды. Блокчейн и будущее человечества. – М.: Манн, Иванов и Фербер, 2018. – 320 с.

4. *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. – С. 37-42.

5. Блокчейн платформа. – URL: https://www.blockchain.com/ (дата обращения 14.10.2021).

6. Крупнейшая криптобиржа рухнула после скачка биткоина свыше 20 000 долларов США. – URL: https://www.finanz.ru/novosti/valyuty/krupneyshaya-kriptobirzha-rukhnula-posle-skachka-bitkoina-vyshe-$20-000-1029898903 (дата обращения 14.10.2021).

7. *Антонова Т.* Убийце следователя Шишкиной дали 14 лет. – URL: https://www.mk.ru/incident/2020/11/17/ubiyce-sledovatelya-shishkinoy-dali-14-let-zhutkie-smski-ravnodushie-policii.html (дата обращения 14.10.2021).

8. *Жданов Ю.Н., Кузнецов С.К., Овчинский В.С.* COVID-19: преступность, кибербезопасность, общество, полиция. – М.: Международные отношения, 2020. – С. 244-252.

9. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». – URL: http://www.consultant.ru/document/cons_doc_LAW_358753/(дата обращения 14.10.2021).

10. Постановление Девятого арбитражного апелляционного суда от 15.05.2018 № 09АП-16416/2018. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=MARB&n=1444056#lUkTnnSiWTBooxkI1 (дата обращения 14.10.2021).

11. *Арсланов К.М.* О правовом регламентировании блокчейн-отношений // Вестник Саратовской государственной юридической академии. – 2019. – № 6 (131). – С. 181-185.

12. *Кузнецов А.Г.* Криминальные риски использования блокчейн-технологий и криптовалюты на территории государств-участников СНГ // Вестник Поволжского института управления. – 2021. – Т. 21. № 1. – С. 48-55.

13. *Шайдулина В.К.* Криптовалюта как новое экономико-правовое явление // Вестник университета. – 2018.– № 2. – С. 137-142.

14. *Суходолов А.П., Антонян Е.А., Рукинов М.В., Шамрин М.Ю., Спасенникова М.Г.* Блокчейн в цифровой криминологии: постановка проблемы // Всероссийский криминологический журнал. – 2019. – Т. 13. № 4. – С. 555-563.

Усманова Т.Х., Володина Н.Н.

Влияние ограничений из-за коронавируса COVID-19 на безопасность экономических систем

Аннотация: Коронавирус COVID-19 внес значительные коррективы в развитие экономических систем. Существующие проблемы социально-экономического

развития граничили с серьезными угрозами в части безопасности экономических систем. Новые проблемы возникли из-за ограничений в рамках борьбы с коронавирусом COVID-19. Шок от ограничений из-за коронавируса в экономической политике еще больше внус разбалансированность в развитие отраслей национального хозяйства. Ограничения из-за коронавируса показали имеющиеся серьезные проблемы, которые необходимо решать на государственном уровне.

Ключевые слова: коронавирус COVID-19, экономические системы, научно-технологическое развитие, разбалансированность

За последнее время ограничения из-за коронавируса COVID-19 привели к снижению экономической активности не только малых и средних предприятий, но и крупных корпораций. Снизились доходы граждан не только в России, но и во всем мире. При этом тарифы на различные услуги не только не уменьшились, но и увеличились. В рамках тарифной политики Федеральной антимонопольной службы для каждого субъекта Российской Федерации установлены предельные индексы повышения тарифов. Ежегодное повышение тарифов в условиях ограничений экономической деятельности негативно сказалось на социально-экономическом состоянии населения и развитии человеческого потенциала в стране. Даже сохранение тарифов на уровне 2019 года в условиях снижения доходов населения могли привести к неплатежам за коммунальные и иные услуги. Пример к тому, существенные доначисления для граждан в рамках отклонений от Правил предоставления услуг и их оплаты добросовестным плательщикам могут создать для населения дополнительные проблемы. Правительство Российской Федерации запретило применять различного рода ограничения в оказании услуг в условиях пандемии коронавируса COVID-19. Тем не менее, очень много случаев, когда население остается наедине с постоянно меняющимся нормативно-правовым регулированием оказания услуг [1].

За последние годы стало выгодно заключать концессионные соглашения в сфере водоснабжения. При этом не везде повышается

качество оказываемых услуг и энергоэффективность. Расходы на компенсацию за электроэнергию за общее пользование для населения увеличиваются, тем самым ухудшается положение населения, а также предприятий из-за увеличения перекрестного субсидирования. В свою очередь, как страна экспорта энергетического сырья, Российская Федерация сохраняет за собой высокое второе место по добыче нефти после США [2]. За последние годы технологии в добыче нефти шагнули резко вперед, хотя в условиях ограничений из-за коронавируса были своего рода спады добычи нефти.

При этом в условиях ограничений из-за коронавируса происходило сокращение выручки и уменьшение количества самих организаций и предприятий малого и среднего бизнеса. Многие закрытые на время коронавируса малые и средние предприятия не открылись вновь или были вынуждены сокращать численность персонала почти в 2-3 раза, сокращать расходы на выплату заработной платы на 40-70%. В мае 2020 года расходы на выплату заработной платы резко менялись во времени. Многие предприятия и организации малого и среднего бизнеса вынуждены были приостановить деятельность, которая критично отразилась на финансовых результатах. Существенно пострадали те отрасли, где вовлечены в производственную деятельность значительные основные средства, транспортные средства и т.д. Кредитные организации также пострадали вследствие ограничений из-за коронавируса и понесли потери как в доходах, так и в финансовых результатах. С марта месяца по июнь 2020 года в Москве ограничения из-за коронавируса нанесли существенный ущерб экономике [3]. Все эти факторы повлияли на бюджетные поступления и на экономическое состояние в целом.

По данным информации Росстата, «Сальдированный финансовый результат (прибыль-убыток) организаций за 1 полугодие 2020 года», резко ухудшились финансовые результаты организаций. За 1 полугодие 2019 года сальдированный финансовый результат составлял около 8 трлн. рублей (8084, 5 млрд. рублей), а за 1 полугодие составил всего 4,3 трлн. рублей (4308, 9 млрд. рублей). Столь резкое ухудшение сальдированного финансового результата негативно отразилось на экономике страны в целом.

Также, по данным Росстата, приведен сальдированный финансовый результат (прибыль-убыток) по некоторым отраслям народного хозяйства за 1 полугодие 2020 года, который показывает существенное сокращение финансовых результатов по экономическим видам деятельности.

При этом самое плачевное состояние за экономическим драйвером – это направление научных исследований и разработок [4]. Неэффективная экономическая политика показала бесперспективность проводимых реформ в России. В современных условиях развивается жесткая конкуренция во всем мире в сфере научных исследований и разработок[5].

Информация об ухудшении экономического состояния разных стран показывает влияние на экономику определенной надстройки. Надстройкой в данном случае явились ограничения из-за коронавируса COVID-19. В свою очередь, в России для формирования предсказуемых экономических условий необходимо изменение бюджетных правил, которые могли бы резко смягчить результаты различных ограничений экономической деятельности организаций и компаний. Существующая конструкция «бюджетных правил» не позволяет обеспечить экономический рост страны, так как работают принципы установленной сбалансированности на основе минимальных стандартов для населения. Происходит ограничение финансирование научных и технологических разработок по многим отраслям. Поддержки малого и среднего бизнеса в настоящее время не происходит.

Действующее законодательство подготовлено таким образом, что технологичным стартапам очень сложно начинать свою деятельность. Малый и средний бизнес зависим от цен на энергоносители, которые также связаны с изменением цен на нефть, газ и электроэнергию. При этом бюджетное правило и здесь имеет существенное вмешательство, которое не на пользу малому и среднему бизнесу. Конструкция бюджетного правила направлена на ограничение расходов на развитие малого и среднего бизнеса в пользу крупного бизнеса ТНК. Особенно поражает умы экономистов тот фактор, который регулирует бюджетное правило – это покупка иностранной валюты в эквивалентных объемах от дополнительных нефтегазовых доходов свыше 40 долларов США за баррель. Как бы пригодились эти суммы для развития малого и

среднего бизнеса в России! Но бюджетное правило не позволяет использовать рентные нефтегазовые доходы на развитие экономики в стране. Бюджетное правило направлено на то, чтобы бюджетно-налоговая политика России была полностью встроена в структуру мировой финансовой системы, то есть финансовые результаты и состояние любой отрасли, даже если она не связана с нефтегазовым экспортом, все равно попадает в зависимость от существующей динамики контрактных цен на нефть и газ. Ухудшает экономическую ситуацию зависимость курса рубля от контрактных цен на нефть и газ. Такая конструкция бюджетного правила негативно отражается на всей экономике страны. При этом научно-технологические разработки в России ежегодно сводятся к минимуму. При такой конструкции бюджетного правила трудно рассуждать о росте благосостояния населения за последние годы. Благосостояние населения прямо пропорционально научно-технологичному развитию страны, которое в последние годы идет только на убыль.

Резко сократились сбережения у населения, так как минимальный доход россиянина, который мог бы обеспечить более-менее средний достаток, составляет около 60 тысяч рублей. При этом более половины россиян такого дохода не имеют, а более 20% сталкиваются с проблемами приобретения самого необходимого из перечня жизненно важных. При этом бюджетное правило предусматривает не поддержание большинства россиян в достатке, а наоборот, покупку валюты, которая опять направляется на выравнивание цен на нефть и газ.

Пока Правительство России не предпримет усилия по изменению ситуации в стране число населения без нормального достатка будет только расти. Несправедливое распределение доходов в стране может измениться только с пересмотром существующей конструкции бюджетного правила. У населения встает логичный вопрос: почему планировать столько средств бюджета на комплекс масштабной борьбы с коронавирусом COVID-19? Бытует мнение: лучше бы увеличили доходы граждан, чтобы население в свою очередь могло повысить свой иммунитет и свое благосостояние!

Бюджеты многих стран зависят от цен на нефть, газ и электроэнергию. При этом Правительствами регулируется добыча,

продажа и потребление энергоресурсов, то есть базовые, дополнительные, выпадающие нефтегазовые доходы, затем утверждается сам бюджет. При этом чутко охраняются процедуры бюджетного правила. Для повышения нефтегазовых доходов рассматриваются различные сценарии: снижение теневой экономики, повышение доходов от управления государственными активами, повышение собираемости налогов. В условиях ограничений из-за коронавируса COVID-19 бюджет пополнялся за счет штрафов и сборов за нарушение режима ограничений со стороны как физических лиц, так и юридических лиц. Активная цифровизация последних лет позволила за счет улучшения администрирования доходами увеличить поступление налогов и сборов в бюджет. Цифровизация также способствует сокращению теневой экономики и получению большей информации о конкурентной среде в бизнесе. Продолжаются слияния и поглощения, тем самым крупный бизнес укрупняется еще больше! Эффективный собственник показывает лучшие результаты путем сокращения расходов на зарплату и социальное содержание работающих.

Благосостояние граждан также зависит от дивидендной политики в целом. Многие акционерные общества и крупные российские компании ежегодно банкротятся, а стоимость акций как государственных компаний, так и других акционерных обществ остаются на прежнем уровне первичной регистрации, хотя при этом было множество переоценок и изменений в хозяйственной деятельности этих компаний. Дивиденды выплачиваются минимальные или вообще не выплачиваются основной массе акционеров. Примером являются многие публичные компании. Акции Газпрома за последние годы не показывали резкого скачка и повышения, кроме отдельного недавнего повышения [6]. При этом стоимость акций такого крупного монополиста так и не были переоценены за период реформ.

Динамика выручки и прибыли ПАО «ИнтерРАО» во 2 квартале 2020 года также показывает ухудшение результатов хозяйственной деятельности [7]. Финансовые результаты резко понизились вследствие ограничений из-за коронавируса COVID-19. Существенное ухудшение финансовых результатов коснулось даже такой крупной корпорации, не говоря уже о малых и средних

компаниях, многие из которых обанкротились. В такой ситуации вероятность того, что может быть сформирована инвестиционная активность или разработаны новые научные технологии, которые смогут стать драйверами экономики, остается под большим сомнением. Резкое снижение выручки и прибыли также сказывается и на дивидендной политике крупных корпораций. Результаты ущерба ограничений из-за коронавируса COVID-19 еще будут иметь последствия и далее, так как средства массовой информации пестрят заголовками, что могут быть еще и другие волны усиления пандемии. Такое повторное пришествие коронавируса ничего хорошего для экономического развития не обещает.

За последние годы не удавалось обеспечить устойчивые темпы роста экономики, поэтому рассчитывать на рост благосостояния населения было невозможно.

Таким образом, в работе анализируются проблемы, которые возникли из-за ограничений, последовавших в рамках борьбы с коронавирусом COVID-19. Шок от ограничений из-за коронавируса в экономической политике еще больше вносит разбалансированность в развитие отраслей народного хозяйства. В такой ситуации ломаются ориентиры прогнозирования и планирования деятельности отраслей и корпораций. Ограничения из-за коронавируса показали имеющиеся серьезные проблемы, которые необходимо решать на государственном уровне.

Литература:

1. *Аганбегян А.Г.* Для выхода из стагнации нужны коренные изменения // Научные труды Вольного экономического общества России. – 2019. – Т. 217. № 3. – С. 28-39.

2. *Глазьев С.Ю.* Российская экономика в начале 2020 года: о глубинных причинах нарастающего хаоса и комплексе антикризисных мер // Российский экономический журнал. – 2020. – № 2. – С. 3-39.

3. Эксперты назвали сферы с наибольшим сокращением зарплаты. – URL: https://www.rbc.ru/economics/15/06/2020/5ee5a3159a7947ed0e5c599c (дата обращения 30.09.2021).

4. Структурно-инвестиционная политика в целях устойчивого роста и модернизации экономики. Научный доклад / Руководитель

и отв. редактор: академик В.В. Ивантер. – М.: ИНП РАН, 2017. – 34 с. – URL: https://ecfor.ru/publication/strukturno-investitsionnaya-politika-v-tselyah-ustojchivogo-rosta-i-modernizatsii-ekonomiki/ (дата обращения 29.09.2021).

5. *Усманова Т.Х.* Механизмы проектной и программной реализации стратегий социально-экономического развития / Россия: тенденции и перспективы развития. Ежегодник. – М.: Институт научной информации по общественным наукам Российской академии наук, 2018. – С. 126-129.

6. Динамика курса акций ПАО Газпром (руб., MOEX). – URL: https://yandex.ru/news/quotes/29.html (дата обращения 29.09.2021).

7. Прибыль Интер РАО упала на 56% во II квартале. – URL: https://bcs-express.ru/novosti-i-analitika/pribyl-inter-rao-upala-na-56-vo-ii-kvartale (дата обращения 28.09.2021).

Лещенко В.В.

Обеспечение национальной безопасности в сфере интеллектуальной собственности в России

Аннотация: Изложены результаты научно-исследовательской работы по решению проблемы деградации производства и применения результатов интеллектуальной деятельности (РИД) и связанными с ними угрозами национальной безопасности России. Предложен выход из кризиса посредством использования инструментов и механизмов получения и применения РИД в различных научных, конструкторских, академических и образовательных организациях при выполнении научно-исследовательских и опытно-конструкторских работ.

Ключевые слова: результаты интеллектуальной деятельности, национальная безопасность, интеллектуальная собственность, патентные исследования, изобретения, управление результатами интеллектуальной деятельности, антикризисное управление, научно-исследовательские работы, опытно-конструкторские работы

На протяжении последнего столетия в мире интенсивно и экстенсивно развивается процесс производства и применения результатов интеллектуальной деятельности (РИД) в различных сферах деятельности человеческого общества.

Степень безопасности жизнедеятельности человечества и в частности, и в целом, все более зависит от производства и применения РИД.

Одним из аспектов глобального кризиса и соответствующих угроз национальной безопасности России является деградация процессов производства и применения РИД.

По данным Всемирной организации интеллектуальной собственности [1], представленным на рисунке 1, в 2020 году было подано около 275900 международных заявок PCT, что на 4% больше, чем в 2019 году. Несмотря на объявленную глобальную пандемию, рост количества заявок, начиная с 2010 года, сохраняется.

Наибольшее количество заявок по процедуре PCT подали заявители из Китая.

США, Япония, Республика Корея и Германия вошли в список пяти лучших стран происхождения заявок. На 10 ведущих стран пришлось 88,5% от общего числа заявок в 2020 году. Россия не вошла даже в первую двадцатку таких стран.

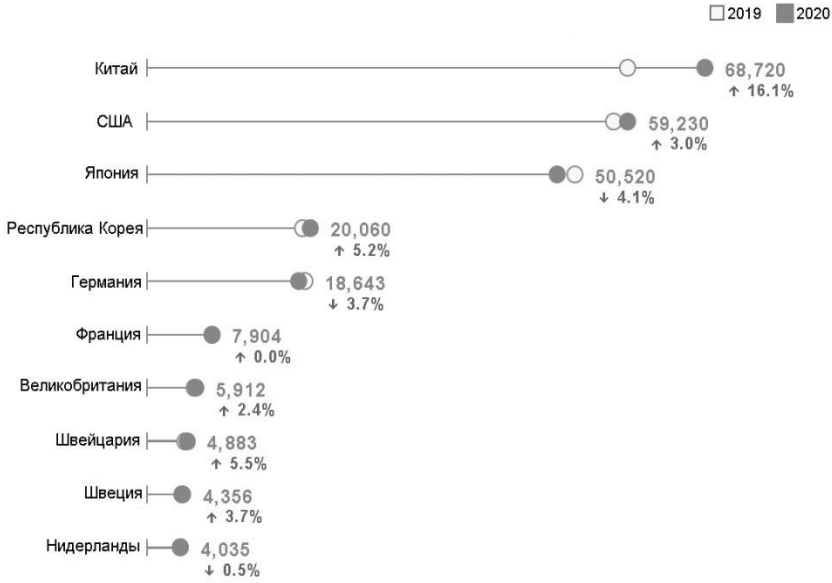


Рисунок 1 – Статистика подачи международных заявок PCT

Согласно отчету Роспатента за 2020 год [2] о результатах работы с РИД в России, представленных на рисунке 2,40% патентов на изобретения в Российской Федерации выданы иностранным заявителям.

Показатели	2016	2017	2018	2019	2020
Выдано патентов, всего	33536	34254	35774	34008	28788
из них:					
российским заявителям	21020	21037	20526	20113	17181
иностранным заявителям	12516	13217	15248	13895	11607

Рисунок 2 – Динамика выдачи патентов на изобретения в России

Для выхода России из кризисного положения в сфере интеллектуальной собственности в данной работе предложено использование инструментов и механизмов получения и применения РИД в различных научно-исследовательских, проектных, конструкторских, научно-производственных,

академических, образовательных и инновационных организациях в России (далее – Организации).

Для осуществления в Организации создания и развития РИД при патентовании изобретений, полезных моделей, промышленных образцов или в иной форме государственной регистрации объектов РИД – программ для ЭВМ, баз данных и топологий интегральных микросхем, предлагаю реализовать следующие 20 мероприятий.

1. Создать в Организации систему делопроизводства для сопровождения работы с объектами РИД, регистрируемыми в Роспатенте. На каждый объект РИД должно быть заведено дело, которое регистрируют в журнале учета дел объектов РИД. В эти дела направляют документы или копии документов, касающиеся конкретного объекта РИД. Каждое дело объекта РИД обязательно должно иметь формуляр с перечнем помещенных в него документов или копий документов самого различного содержания и происхождения, относящихся к объекту.

2. Сформировать и сопровождать библиотеку РИД, копий договоров (контрактов), технических заданий, отчетов о патентных исследованиях [3], расчетно-калькуляционных материалов для научно-исследовательских работ (НИР) и опытно-конструкторских работ (ОКР), выполненных в процессе НИР, ОКР и других договоров (контрактов). В библиотеке также должны быть копии договоров и соглашений между авторами объектов РИД и Организацией, бухгалтерских расчетов вознаграждений авторам за создание и внедрение служебных РИД.

3. Разработать электронный каталог и электронный основной фонд библиотеки, упомянутой выше в п. 2, для автоматизации поиска необходимых документов и обеспечения доступа к ним, с возможностью вывода и сохранения источников, хранящихся в библиотеке, в электронной форме или их распечатки.

4. Разработать и внедрить в Организации автоматизированную информационную систему (АИС) для патентования и других форм государственной регистрации объектов РИД в Роспатенте, с целью повышения производительности и качества работы с объектами РИД. АИС должна автоматически формировать документы, обеспечивающие делопроизводство при государственной регистрации объектов РИД в Роспатенте и при служебной переписке внутри Организации. АИС должна по командам

оператора проводить расчеты сумм платежей пошлин, выполнять операции с аналитическими данными для подготовки статистической отчетности, отображающей ход работы с объектами РИД. С помощью АИС необходимо формировать бюджет расходов Организации на предстоящий период работы с объектами РИД.

5. Разработать и внедрить нормативную документацию Организации в виде группы стандартов организации по работе с системой обеспечения нормативными документами процесса работы с объектами РИД (обеспечения жизненного цикла объектов РИД).

6. Создать электронный каталог и основной фонд библиотеки нормативной документации Организации, межгосударственных, государственных и национальных стандартов для работ по выявлению и регистрации служебных объектов РИД.

7. Совместно с научными подразделениями Организации регулярно выполнять работы по оперативному выявлению объектов РИД, их патентованию и другими формами государственной регистрации в Роспатенте.

8. Регистрировать в Роспатенте объекты РИД в момент их выявления при выполнении НИР или ОКР, при авторском надзоре Организации за объектами РИД и при выполнении поисковых экспериментальных работ, выполняемых в инициативном порядке.

9. Обеспечить предоставление из подразделений Организации рабочих материалов для оформления государственной регистрации объектов РИД.

10. Организовать научно-технический совет для принятия решения о государственной регистрации объекта РИД в Роспатенте, оформлении заявки в Роспатент на государственную регистрацию объекта РИД с дальнейшим сопровождением процесса регистрации РИД, включая расчеты с помощью АИС пошлин, уплачиваемых в бюджет, и их оплату бухгалтерией Организации.

11. Разработать и внедрить в Организации актуальную версию Регламента правовой охраны и использования служебных результатов интеллектуальной деятельности (далее – Регламент) с учетом соответствующего постановления Правительства России [4]. Это обеспечит привлечение средств заказчика НИР или ОКР за служебные РИД, созданные при их выполнении, для материального стимулирования изобретателей Организации в форме

вознаграждения за изобретения, полезные модели и промышленные образцы в сумме трех среднемесячных зарплат каждому из авторов.

12. Для реализации описываемых здесь мероприятий и решения проблем, возникающих при работе с РИД, создать Научно-технический центр управления результатами интеллектуальной деятельности (НТЦУРИД).

Созданный НТЦУРИД совместно с научными подразделениями будет проводить патентные исследования [3] при выполнении НИР или ОКР и готовить отчеты о них. При формировании отчетов должны быть использованы рабочие материалы ранее разработанных отчетов о патентных исследованиях из библиотеки отчетов о патентных исследованиях (см. п. 2). Таким образом, будет обеспечена экономическая эффективность создания патентных отчетов с помощью ранее созданных рабочих материалов патентных исследований.

13. Ресурсы НТЦУРИД необходимо использовать не только для НИР и ОКР, выполняемых внутри Организации, но и для выполнения патентных исследований для внешних организаций, по договорам с ними в порядке аутсорсинга, когда могут быть использованы имеющиеся в Организации рабочие материалы по ее основному направлению деятельности.

14. Дополнительно ресурсы НТЦУРИД с участием сотрудников научных подразделений целесообразно использовать для доработки, оформления и государственной регистрации объектов РИД для работников Организации в процессе повышения их научной квалификации, например, диссертационных работ. Для защиты диссертаций в технических науках в качестве публикаций засчитываются патенты на изобретения, полезные модели, промышленные образцы и свидетельства на программы для ЭВМ, базы данных, топологии интегральных микросхем. Для защиты на степень кандидата наук достаточно 3-х зарегистрированных РИД, для докторской – 10 зарегистрированных РИД. Срок получения свидетельства на программу для ЭВМ в настоящее время может достигать 9 дней, патента на изобретение – 9 месяцев.

15. Необходимо отметить, что в отдельных случаях рентабельнее использовать попытки патентования объектов РИД для определения их патентной чистоты с использованием государственной патентной экспертизы ФИПС Роспатента.

16. Создание в НТЦУРИД рабочей группы по поиску и расширению возможных областей внедрения объектов РИД, принадлежащих Организации, позволит тиражировать уже разработанные объекты, и получать значительный чистый финансовый доход от такого рода деятельности.

17. Проведение обучения способам разработки и внедрения объектов РИД позволит получить дополнительный финансовый доход и расширение круга потенциальных заказчиков услуг в продвижении работы с объектами РИД других компаний.

18. Необходимо создать в Организации систему рационализаторской работы. В ряде случаев рационально было бы преобразовывать рационализаторские предложения в патенты на полезные модели.

19. Необходимо организовать поиск возможностей внедрения объектов РИД Организации для разработки и изготовления товаров широкого народного потребления.

20. В процессе интенсивного развития изобретательской деятельности в Организации целесообразно привлечь преподавателей и студентов через такие организационные формы, как базовые кафедры вузов на предприятиях и малые инновационные предприятия (см. ст. 103 в [5]), деятельность которых заключается в практическом применении (внедрении) РИД, и участие образовательных организаций высшего образования в хозяйственных обществах и хозяйственных партнерствах.

Выполнение предложенных мероприятий и создание Научно-технического центра управления результатами интеллектуальной деятельности в Организации станет неотъемлемой частью антикризисного управления для обеспечения национальной безопасности в сфере интеллектуальной собственности в России.

Литература:

1. WIPO statistics database. Last updated: August 2021. – URL: https://www.wipo.int/edocs/infogdocs/en/ipfactsandfigures/ (дата обращения 16.09.2021).

2. Годовой отчет 2020. – М.: Роспатент, 2020. – С. 142.

3. ГОСТ Р 15.011-96 Система разработки и постановки продукции на производство. Патентные исследования. Содержание

и порядок проведения. – М.: ИПК Издательство стандартов, 1996. – 23 с.

4. Постановление Правительства Российской Федерации от 16.11.2020 № 1848 «Об утверждении Правил выплаты вознаграждения за служебные изобретения, служебные полезные модели, служебные промышленные образцы». – URL: http://publication.pravo.gov.ru/Document/View/0001202011190009 (дата обращения 20.09.2021).

5. Федеральный закон от 29.12.2012 № 213-ФЗ «Об образовании в Российской Федерации». – URL: http://www.consultant.ru/document/cons_doc_LAW_140174/ (дата обращения 20.09.2021).

Лантер Н.Н.

Структурная устойчивость Арктики как экономической территориальной экосистемы

Аннотация: Рассмотрены методы анализа структурной устойчивости, противодействующих процессов в Арктике в разрезе энергетической, социально-культурной и экономической устойчивости системы на основе российских и зарубежных исследований. Выявлено, что глобально структурная устойчивость Арктики должна удовлетворять нужды текущих и будущих поколений в среде растущих угроз. Отмечена важность доступности ресурсов экологически безопасными технологиями, встраивания критерия роста адаптивности и самоорганизации Арктики в проекты разного уровня.

Ключевые слова: глобальная структурная устойчивость, самоорганизация Арктики, адаптивность, энергетическая устойчивость, синергетические эффекты, арктические кластеры, полярный индекс, безопасность, управление критическими повреждениями арктической системы, экополярные услуги

В условиях резкого усложнения внешней среды растет глобальное и национальное значение Арктики. Кумполярные и некумполярные страны активно разрабатывают новые арктические

программы освоения или доступа к арктическим ресурсам, растет число желающих передела Арктики. Отсутствие четкого административно-территориального статуса Арктики ведет к утрате равновесия, потенциала развития и самосохранения системы (ресурсная база, комплексные ожидания выгод, синергетические эффекты). Арктика становится объектом воздействия разнонаправленных сил внешней среды [1]. По закону равновесия Ле Шателье [2] для систем равновесия, сохраняющих свое строение (структуру) в среде, важно сохранить структурную устойчивость макрорегиона путем управления процессами, направленными на противодействие этому изменению.

Структурная устойчивость базируется на потенциале устойчивого развития глобального, межрегионального и национального пространств, а также отраслевом, кластерном, корпоративном уровне и микроуровне (объектном, проектном). Арктика как структура способна наращивать потенциал защищенности, прогрессировать и трансформировать мировое пространство с учетом роста потребности на энергоносители. Укрепление структурной устойчивости ограничено противоречием – беспрерывной добычей ресурсов и сохранением биоразнообразия и качества окружающей среды. На практике структурная устойчивость зависит не только от ее компонентов и концентрата активностей в них, но и от способа их сочетания и характера их организационной связи. Полагаем, что структурную устойчивость Арктики можно выразить количественно через критерии: 1) оценка конструкции арктической системы относительно приспособленности к окружающей среде (динамическая устойчивость к вызовам среды во времени), 2) уровень самосохранения, выживания Арктики (саморазвития) через оценку дельты изменения потенциала созидания и потенциала саморазрушения. В итоге целесообразно вывести критерии суммарной устойчивости Арктики с учетом того, что суммарная структурная устойчивость целого определяется наименьшей его частичной устойчивостью. Тем не менее, следует учитывать и математические подходы к фундаментальному свойству динамической системы – на качественное поведение траекторий не влияют малые возмущения внешней среды. Методологически полагаем целесообразным обозначить качественные свойства

структуры Арктики за неподвижные точки и определить их периодические орбиты через системы обыкновенных дифференциальных уравнений, векторных полей, варианты событий, систему целей развития, алгоритм сигнальных графов и другие методики расчета. Типичная динамика может быть очень сложной для анализа ввиду разного статуса входящих в нее девяти территорий и отсутствия четкой внутринациональной границы, единой администрации, централизованного стратегического планирования и контроля над исполнением принятых решений.

Глобальная структурная устойчивость Арктики должна позволить будущим поколениям удовлетворять их собственные нужды в среде растущих угроз. В 1997 г. 152 страны подписали Конвенцию ООН по морскому праву. «Концепция триединого итога» (как баланс экономической, социальной и экологической составляющих) требует внедрение новых технологий, доступ к которым РФ ограничен. РФ наращивает гуманитарный потенциал, технологии безопасности и выживаемости в АЗ РФ [3]. Полагаем, что структурная устойчивость базируется на потенциале устойчивого развития глобального, межрегионального и национального пространств, а также отраслевом, кластерном, корпоративном уровне и микроуровне (объектном, проектном).

Анализ уровня национального, регионального и проектного устойчивого развития в Арктике выполнен в 2018 году «ОПОРА» и МГУ в формате исследования «Полярный индекс. Компании» (ПАО «Лукойл», ПАО «Сибур Холдинг», ПАО «ГМК «Норильский никель», ПАО «Роснефть» и ПАО «АК «Алроса») на базе двух рейтингов устойчивого развития (рейтинг регионов АЗ РФ и рейтинг градообразующих и регионообразующих компаний). Эти компании инициативно и в рамках нацпроектов создают инфраструктуру в рамках жестких экологических норм. Так, реконструкция производства «Норникель» на 30% снижен выброс оксида серы в Норильске. Новый завод по улавливанию выбросов углекислого газа (Надеждинский металлургический завод) и реконструкция серного производства на Медном заводе снизят выбросы к 2023 г. на 75% от уровня 2015 г. Второй рейтинг проекта «Полярный индекс. Регионы» выявил регионы – лидеры АЗ РФ (Мурманская и Архангельская область, РС). Отметим новые тенденции в АЗ РФ.

1. Рост уровня проектной устойчивости в рамках кластерного под хода (лесопромышленный и арктический рыбопромышленный кластеры). Города-проекты становятся центрами новых технологических кластеров благодаря цифровизации страны. (Северодвинск – центр атомного судостроения, Мирный – центр космической отрасли). Также развивается проект приоритетного топлива – сжиженного природного газа.

2. Уникальная способность Арктики к самоорганизации и саморазвитию теряет способность противостояния тенденциям, разрушающим ее как систему, поскольку ряд ее элементов (экология, таяние льдов) обладают наименьшей устойчивостью.

3. Арктика усложняется технологически: единая экосистема распадается, появляются структурно самостоятельные бизнес-полигоны, растет гуманитарность проектов (очистка от мусора, сохранение культуры коренных народов).

Выявление причин упадка АЗ и точные расчеты доступности ресурсов экологически безопасными технологиями позволят встраивать критерии роста адаптивности и самоорганизации Арктики в проекты разного уровня. Также, следуя логике интеграционного подхода, на базе двух вышеназванных исследований индекса структурной устойчивости целесообразно ежегодно мониторить индекс социального благополучия, индекс устойчивости, экологической устойчивости АЗ РФ относительно арктических регионов других стран. Эти индексы комплексной устойчивости определяют текущие и будущие «узкие» места рынка.

Полагаем, что в основе закона самоорганизации системы лежит дуализм развития и второй закон термодинамики. Арктика как структура наращивает потенциал защищенности, прогрессирует и благоприятно трансформирует мировое пространство с учетом роста потребности на энергоносители (например, «Северный поток-2»). Формируются конкурирующие отраслевые кластеры, способные демонтировать текущую структуру арктического макрорегиона или дать ему мощный технологический толчок развития. Комплекс ожиданий прорыва может вступить в конфликт с целями Арктического Совета в части комплексной безопасности.

Отмечая основные проблемы (энергобезопасность, доступность энергии и экологическая устойчивость), Мировой Энергетический Совет ужесточил требования к бизнесу даже в условиях климата и

инфраструктурной изоляции. Важно провести индикативный анализ стратегических ориентиров для разработки национальных перечней оценки текущего уровня безопасности и прогноза перспективного уровня энергобезопасности стран. Так, Институт мировой энергетики в США на 1-ое место по уровню энергобезопасности поставил Норвегию. Среди 29 параметров: соотношение импорта нефти, газа и угля с их потреблением в стране, безопасность и разнообразие источников энергии, соотношение расходов на импорт энергоносителей с ВВП, цены на нефть и электроэнергию, потребление энергии в целом и на душу населения и потребление энергии транспортом страны. На втором месте находятся США, а РФ занимает 12-е место.

В 2014 году Мировой энергетический совет WET (World Energy Trilemma) при оценке энергетической безопасности по 6 параметрам поставил РФ на 2-ое место после Канады благодаря большим стратегическим запасам нефти и газа, доступности энергии потребителям, способности стран обеспечивать устойчивую энергетику через диверсификацию источников энергии. Среди индикаторов такого анализа: 1) отношение производства энергии к его потреблению, 2) диверсификация источников генерации электроэнергии, 3) потери в сетях (% от генерации электроэнергии в РФ выше, чем в Канаде), 4) среднегодовые темпы роста отношения энергопотребления к ВВП за пять лет, 5) запасов нефти и нефтепродуктов и т.д. Однако по новой методике расчета индекса в 2021 году способность РФ обеспечивать устойчивую энергетику определена уже на 29 месте из 108 стран с показателем 73,8, несмотря на то, что энергоресурсы составляют 2/3 объема экспорта РФ. В основе такого решения определены три базовых критерия: 1) энергетическая безопасность (эффективность управления внутренними и внешними источниками энергии, надежность и устойчивость энергетической инфраструктуры); 2) энергетическая справедливость (доступ к электричеству и чистому топливу, технологиям); 3) экологическая устойчивость энергосистем.

Ценнейшее исследование «Центра энергетики Московской школы управления «СКОЛКОВО» в 2020 году по оценке первого критерия WET -энергетической безопасности РФ по 10 -122 критериям выявило четкую ориентированность стран

циркумполярного мира на мощный рост энергоэффективности и самообеспечение энергоресурсами, их доступность по приемлемым ценам. Диверсификация, четкость поставок энергоресурсов с сохранением экологии – основа арктических стратегий.

Для повышения структурной устойчивости российской АЗ важно учитывать опыт конкурирующих стран. Приоритеты Финляндии – атомная энергетика, СПГ, чистые технологии, Норвегии – разумное потребление, экологические проекты, Канады – жесткое лицензирование и инфраструктура, Швеции – биотехнологии и экономика без нефтяной зависимости. Дания переходит к 2050 году на возобновляемые источники энергии. Исландия имеет до 99,99% возобновляемых источников энергии.

Энергетическая устойчивость Арктики

При разработке методологии управления АЗ РФ важно применять комплексный подход (энергетическая безопасность, энергетическая устойчивость и экологическая безопасность в качестве трех базовых параметров) на всех стадиях ПЖЦ проекта. При стремлении каждого параметра системы к росту структурная устойчивость системы стремится к максимуму. При максимальной эффективности взаимосвязей трех базовых параметров и функциональная устойчивость системы стремится к максимуму.

Важно учесть опыт международных прогностических организаций, использующих собственные интегрированные показатели для расчетов. Так, ООН при оценке эколого-экономической устойчивости систем опирается на экологически чистый адаптированный ЧВП (рассчитывается на основе стоимостной оценки истощения природных ресурсов и стоимостной оценки экологического ущерба). ВБ берет за основу показатель устойчивого социально-экономического развития «Истинные накопления» (GS) на основе 4 параметров (величину чистых внутренних сбережений (NDS), чистые внутренние сбережения (EDE), величину истощения природных ресурсов (DRNR) и величину ущерба от окружающей среды (DME)). ЕК использует «Индекс ущерба для здоровья населения от загрязнения окружающей среды». ВФДП рассчитывает общую устойчивость на основе индикаторов – «здоровье населения» и «экологический след». Йельский университет (США) определяет индекс социально-

экологической устойчивости по 5 основным группам показателей: 1) состояние окружающей среды; 2) уменьшение воздействия на экологические ресурсы; 3) уменьшение уязвимости человека; 4) социально-институциональный ответ на экологические вызовы и 5) возможности глобального контроля над экологией страны.

Проведенный анализ критериев для оценки устойчивости систем выявил десятки важных критериев, включая экологические индикаторы: площадь заповедных территорий (%), потребление энергии, темпы восстановления лесов в год, площадь земель, объемы опасных отходов, концентрация загрязняющих веществ окружающей среды, влияние загрязнения на здоровье людей, состояние флоры и фауны, объем запасов природных ресурсов, использование минеральных удобрений. Несомненно, данные экологические индикаторы чрезвычайно важны, ведь они напрямую позволяют оценить состояние окружающей среды на основе комплексного подхода, с учетом ПЖЦ системы.

Социально-культурная устойчивость Арктики

Для оценки социальной устойчивости ООН исследует структуру производства и потребления, уровень образования, утилизацию отходов и транспорт. ООН и ОЭСР используют социальные индикаторы реакции, жизнедеятельности человека: объемы отходов на душу населения, использование транспорта, расходы на сбор и обработку отходов, природоохранные налоги, структуру ценообразования, затраты на охрану окружающей среды, доля рынка экопродукции, уровень переработки отходов. ВБ определяет политико-институциональную устойчивость экономических территориальных систем на базе долга в ВНП и уровня инфляции на основе показателей эмиссии парниковых газов и концентрации приоритетных загрязняющих воздух веществ на городских территориях. Полагаем, что ключевой критерий социальной устойчивости Арктики – справедливое распределение благ в стабильной среде развития общественных отношений.

Экономическая устойчивость Арктики

Экономическую устойчивость ООН рассчитывает на основе временных параметров и индексов влияния на человеческое благосостояние. Экономическая структура включает три блока: 1)

экономика (ВВП на душу населения, доля инвестиций, % ВВП), 2) торговля (торговый баланс в товарах и услугах); 3) финансы (доля долга, % ВВП, получение или предоставление помощи, % ВВП). ОСЭР выделяет три приоритетных индикатора: 1) ВВП на душу населения, 2) индекс развития человеческого потенциала, 3) затраты на очистку сточных вод. ВБ использует три критерия: 1) ВВП на душу населения, 2) доля инвестиций в ВВП, 3) производительность труда. Таким образом, уровень экономической устойчивости развития включает экономическую, социально-культурную, политико-институциональную и экологическую устойчивость.

В целом, вышеназванные критерии оценки устойчивости Арктики как системы позволяют определить динамику потенциала экономики, внешней среды, населения и социальных отношений, выработать единые подходы к принятию решений на основе учета наиболее эффективных реакций системы для сохранения, прогресса, самосохранения и эволюции физической, социальной, политической, экологической, биологической и интеллектуальной целостности Арктики. Подпрограмма «Формирование опорных зон, создание условий для ускоренного социально-экономического развития региона» (раздача арктических гектаров, механизм ускоренной амортизации ОС, инвестиционный налоговый вычет) призваны усилить инвестиционную активность и уровень заселенности АЗ РФ. Также прогнозируем, что добыча ресурсов и магистральная логистика в Арктике для РФ станет более технологически затратной и сложной. Реализацию «Плана развития инфраструктуры СМП до 2035 г.» усложняют многие вызовы. Среди них: высокая энергоемкость и низкая эффективность добычи ресурсов, издержки арктического производства, неразвитость энергосистемы, нерациональная структура генерирующих мощностей, высокая себестоимость генерации и транспортировки электроэнергии и неготовность к переходу на инновационный путь развития АЗ РФ. Тем не менее, нацпроекты и программы призваны обеспечить рост устойчивости АЗ («Комплексный план модернизации и расширения магистральной инфраструктуры на период до 2024 г.» имеет бюджет проекта «СМП» 587,5 млрд. руб., прогноз роста перевозок – до 80 млн. т. к 2024 г.).

Отметим, что на устойчивость Арктики влияет и регресс мирового развития вследствие климатических катастроф и

пандемии COVID-19, изменивших структуру глобальной экономики. Диверсификация энергетических источников, сохранность структуры добычи и доставки энергии, ликвидация бедности и голода, борьба с изменением климата идут наряду с закреплением новых технологических компетенций и политических ролей за странами. Передел мира через новую систему лицензий трансформирует Арктику в закрытый клуб (кластер) отдельных ресурсных корпораций. Комплексные государственные экополярные услуги не доступны в необходимом для сохранения экосистемы Арктики объеме. Глобальная система управления в формате Арктического Совета фрагментирована, подвержена конфликтам участников и их союзников, отсутствует глобальная система сбора информации о критических повреждениях Арктики как экосистемы и энергосистемы.

Таким образом, укрепление структурной устойчивости в АЗ РФ ограничена противоречием – беспрерывной добычей ресурсов и сохранением биоразнообразия и качества окружающей среды. Необходимы единые критерии оценки структурной устойчивости арктической системы, усиление фундаментальных знаний об Арктике для прогнозирования, разработки комплексной системы коллективной безопасности и глобальной базы арктических технологий. Структурная устойчивость АЗ РФ зависит от структурной устойчивости всей Арктики, ответственного глобального арктического управления и новых экологически безопасных технологических прорывов.

Литература:

1. *Komkov N.I., Bondareva N.N.* Management of Technological Component in Development Programs of the Russian Arctic Zone / International Scientific Conference "Digital Transformation on Manufacturing, Infrastructure and Service" (21-22 November 2019 St. Petersburg). – URL: https://iopscience.iop.org/article/10.1088/1757-899X/940/1/012118 (дата обращения 10.10.2021).

2. *Гиббс Дж.В.* Термодинамика. Статистическая механика. – М.: Наука, 1982. – 584 с.

3. Основы государственной политики РФ в Арктике на период до 2020 года и дальнейшую перспективу, утвержденные Президентом РФ от 18 сентября 2008 №Пр-1969. – URL:

http://www.consultant.ru/document/cons_doc_LAW_119442/ (дата обращения 10.10.2021).

Авдеева З.К., Коврига С.В.

Прогнозирование целевых показателей в нестационарных процессах, движимое когнитивным моделированием ситуаций

Аннотация: В работе представлен подход к прогнозированию целевых показателей в нестационарных процессах, направленный на повышение ценности прогноза за счет построения и корректировки конкурирующих моделей на основе временных рядов в режимах цифрового мониторинга и ситуационного мониторинга. В режиме мониторинга ситуации корректирующие сигналы, отражающие значимые изменения внешней среды, формируются в результате когнитивного моделирования ситуации с использованием информации из разнородных источников.

Ключевые слова: нестационарные процессы, прогнозирование, временные ряды, мониторинг, когнитивное моделирование ситуаций

В настоящее время наблюдается бурный рост технологических и информационно-аналитических инструментов в области интеллектуального анализа данных для решения практических задач анализа и прогнозирования в различных сферах жизни общества (будь то экономическое и социально-политическое прогнозирование, прогнозирование товарных рынков, финансовое прогнозирование, прогнозирование изменений окружающей среды и др.). Накопление больших исторических данных способствует росту предложений по моделям и методам анализа и прогнозирования временных рядов. Являясь востребованным прогностическим инструментом работы с большими массивами данных, отражающих закономерности поведения исследуемых процессов, они используются для формирования прогнозов целевых показателей на различных временных горизонтах для принятия решений.

Однако, возможностей этих моделей и методов недостаточно для прогнозирования развития ситуации в условиях

непредсказуемости поведения исследуемого процесса, 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.

Таким образом, в ситуациях, характеризующихся высоким уровнем нестабильности и неопределенности, повышение ценности прогнозов невозможно без учета суждений ЛПР и экспертов, несмотря на растущее присутствие аналитики данных и других систем поддержки прогнозирования, основанных на статистических и математических моделях. Такая практика совместного прогнозирования (с привлечением оценочных экспертных суждений и количественных данных) широко признается специалистами, когда имеется достаточно данных для построения количественной модели для выявления регулярных компонентов (закономерностей) временного ряда, но недостаточно для прогнозирования нерегулярной компоненты и, более того, компонент, связанных с последствиями непредвиденных событий [1-3]. При этом в этой области можно выделить несколько общих подходов к прогнозированию [2,3]: подход 1 – априорное включение оценочных суждений в процедуру прогнозирования на этапе выбора и построения прогнозных моделей; подход 2 (комплексный) – одновременное включение, когда объединяются чисто статистические прогнозы и оценочные прогнозы для формирования окончательного прогноза; подход 3 – апостериорное включение оценочной корректировки статистически полученного прогноза, когда эксперты проверяют прогноз, а затем корректируют его на основе своих знаний и опыта.

Принимая во внимание необходимость включения экспертной оценки при формировании количественных прогнозов, Дж. Армстронг в работе [1] систематизировал ряд обобщений для повышения точности статистических прогнозов. В частности, он обосновал необходимость включения предметных знаний в формирование прогноза, структурирование знаний, использование причинно-следственных моделей для выявления факторов, влияющих на прогнозируемый процесс.

Следуя современным направлениям прогнозирования на основе оценочных суждений и статистических методов в трудно

предсказуемых ситуациях, мы развиваем подход к прогнозированию целевых показателей в нестационарных процессах, движимого когнитивным моделированием ситуаций. Данный подход ориентирован на учет информации, отраженной во временных рядах, и информации о возможных вариантах развития ситуации на основе выявления и обработки экспертных знаний и гипотез, разнородных источников информации посредством построения, анализа и моделирования на когнитивной карте ситуации (ККС) – формализованной модели причинно-следственных связей между значимыми системообразующими факторами ситуации. Когнитивное моделирование используется в качестве инструмента поддержки принятия решений на разных этапах прогнозирования за счет:

– структурирования предметной области и выявления значимых системообразующих факторов и процессов влияния на прогнозируемый процесс – на этапе построения прогнозных моделей (в соответствии с подходом 1). Особенностью ККС, позволяющей использовать ее на этом этапе, является то, что ККС – это средство вербализации и передачи ментальных моделей ЛПР, экспертов, прогнозистов, участвующих в процессе прогнозирования. Таким образом, ККС делает отдельные взгляды явными и проверяемыми. Это не только улучшает индивидуальное восприятие ситуации участниками прогнозирования, но также может способствовать общему пониманию ситуации при принятии решений. Кроме того, ККС может быть результатом комбинации экспертных суждений с информацией о факторах и взаимосвязях, выявленных методами поиска и анализа данных в открытом гетерогенном информационном пространстве [4]. Такая интеграция помогает повысить объективность и правдоподобность модели целостного представления ситуации;

– управления процессом получения сигналов из внешней среды (ситуационный мониторинг) об экспертно значимых (реальных или еще не произошедших) событиях (инфоповодах), которые могут повлиять на прогнозируемый процесс и связанные с ним процессы. Данную информацию можно использовать для корректировки прогнозов с обоснованием выбора количественных прогнозных моделей (в соответствии с подходом 3).

В рамках развиваемого подхода, процесс прогнозирования включает (рисунок 1):

– построение и корректировку ККС, основанной на сочетании экспертных суждений и информации из разнородных источников;

– определение параметров информационного поиска – потенциальных сигналов изменения причин воздействия на целевой показатель;

– построение и корректировку прогнозных моделей, и формирование прогнозов целевого показателя;

– цифровой мониторинг значений целевого показателя и влияющих на него количественных факторов;

– ситуационный мониторинг качественных изменений внешней среды и анализ их значимости на ККС.

Включение когнитивного моделирования в процесс прогнозирования обеспечивает глубокое понимание ситуации не только с целью систематизации экспертных знаний, но и организации направленного поиска и отбора наборов данных при мониторинге, где ККС представляет собой семантическую модель для наблюдения важных факторов, событий и тем в разнородных источниках информации. Такое включение когнитивного моделирования ситуации в типовую процедуру добычи данных обеспечивает соединение глубокого поиска в традициях интеллектуального анализа данных с глубоким пониманием на основе семантического распознавания под воздействием ККС – экспертной модели представления ситуации. Построение ККС предваряется определением общей направленности (целей) поиска информации и формированием укрупненной концептуальной модели предметной области. Такая концептуальная модель предназначена для определения границ «захвата» знаний по ситуации в модельном представлении в виде ККС [4].

Рисунок 1 – Общая схема прогнозирования

В рамках предложенного подхода реализуется принцип организации мониторинга в виде двухрежимного процесса: цифрового мониторинга и ситуационного мониторинга. Цифровой мониторинг отслеживает изменения во временных рядах, генерируя сигналы о наличии и идентифицируя тип изменений в целевом показателе и связанных с ним показателях. Актуализация таких сигналов на интервале прогнозирования свидетельствует об изменении структуры прогноза и/или формирующих его моделей. Для обнаружения этих сигналов в данных временных рядов используются методы последовательного анализа для выявления наличия причинно-следственной связи Грейнджера и коинтеграции, изменения волатильности; метод текущего обнаружения разладок при наличии структурных изменений в процессе [5]. Ситуационный

мониторинг предназначен для выявления информации о последствиях изменений внешней среды, которые отсутствуют в данных временных рядов в текущий момент (цифровой мониторинг может обнаружить эти изменения с запаздыванием). В результате мониторинга ситуации генерируются сигналы от динамического анализа и моделирования на ККС как оценки значимости изменений в системообразующих факторах (связанных с реальными или еще не произошедшими экспертно значимыми событиями во внешней среде) для изменения значений целевого показателя. Данный режим мониторинга направлен не только на выявление экспертно значимых событий во внешней среде (инфоповодов) и связанных с ними системообразующих факторов ситуации, отраженных в ККС, но и на формирование сценариев развития ситуации, к которым эти события могут привести. Таким образом, обоснованием выбора инфоповода для активации процедуры коррекции прогнозных моделей служат результаты структурного анализа и моделирования на ККС как оценки последствий от инфоповода на прогнозируемый процесс [6]. Такая оценка формируется на базе разработанных критериев, которые позволяют ранжировать системообразующие факторы ККС, связанные с инфоповодом, по (1) их значимости во влиянии на прогнозируемый целевой показатель и (2) по степени активности их проявления в инфоповоде.

Работоспособность представленного подхода проверена в рамках пилотного проекта по разработке системы стратегии закупок для трубопрокатного завода на задаче формирования закупочных цен на металлолом на вторичном рынке сырья [7]. Его применение позволило повысить точность прогноза. Средняя ошибка прогноза для модели без коррекции – 7%, максимальная – 23%; с коррекцией (на основе рекомендаций ККС) соответственно 5% и 15%.

Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011

Литература:

1. *Armstrong J.S.* The forecasting canon: nine generalizations to improve forecast accuracy // International Journal of Applied Forecasting. – 2005. – V.1. – P. 29-35.

2. *Cheikhrouhou N.* and other. A collaborative demand forecasting process with event-based fuzzy judgements // Computers & Industrial Engineering. – 2011. – Volume 61. Issue 2. – P. 409-421.

3. *Perera H.N.* and other. The human factor in supply chain forecasting: A systematic review // European Journal of Operational Research. – 2019. – V. 274(2). – P. 574-600.

4. *Avdeeva, Z.K., Kovriga, S.V.* Distributed environment of decision support centers: an interest representation model of virtual collaboration and technological basic // Procedia Computer Science. – 2020. – V. 176. – P. 3761-3770.

5. *Grebenyuk E.A.* Monitoring and identification of structural shifts in processes with a unit root / 13th International Conference "Management of large-scale system development" (MLSD) (28-30 Sept. 2020 Moscow). – URL: https://ieeexplore.ieee.org/document/9247829. (дата обращения 10.10.2021).

6. *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.

7. *Avdeeva Z.K., Grebenyuk E.A., Kovriga S.V.* Forecasting of key indicators of the manufacturing system in changing external environment. IFAC PapersOnLine. – 2020. – V. 53 (2). – P. 10720-10725.

Байрамов О.Б.

Методика выбора группы заемщиков в микрофинансировании

Аннотация: Процесс микрофинансирования рассматривается как динамическая задача дискретной оптимизации. Выделяется кредитный скоринг как важный этап процесса. Для небольшого МФО предлагается способ выделения потенциальных заемщиков.

Ключевые слова: микрофинансирование, МФО, кредитный скоринг, процентные ставки, заемщики, характеристики

Микрофинансирование позволяет гражданам и малому бизнесу быстро получать небольшие займы на короткие сроки. Получить их проще, чем кредит в банке, но ставки по таким займам выше.

Микрофинансовые институты – небольшой по объемам, но важный элемент финансовой системы. Они часто представлены в регионах, где мало банков и где поэтому сложнее получить кредит гражданам и малому бизнесу.

Как отмечалось в [1], роль процесса микрофинансирования и самих микрофинансовых организаций (МФО) в стабилизации экономики во всех странах мира в настоящее время (пандемия, вооруженные конфликты и др.) приобретают особую актуальность. Поддерживая бедные слои населения и начинающих предпринимателей, МФО одновременно занимаются реализацией своих основных задач получения прибыли в условиях определенного риска.

Основная задача микрофинансирования заключается в оценке риска кредитора.

Базовая математическая модель управляемого процесса взаимодействия кредитора в лице МФО и заемщика с учетом возможного сбоя в возврате кредитов была сформулирована в [1].

В деятельности МФО определяющими этапами являются решение о выделении кредита заемщику и определение процентных ставок по кредиту.

Алгоритмическое представление процесса микрофинансирования позволяет определить его как решение динамической задачи дискретной оптимизации с выделением свойства марковости [2] и описывается в классической форме

$$f(x^{\uparrow *}) = \max\{f(x): x \in X\}, \quad (1)$$

где $f(x)$ – целевая функция (прибыль МФО), X – допустимая область, в рассматриваемом случае x – процентные ставки для заемщиков.

Рассматриваемый процесс протекает в течение нескольких этапов и на каждом этапе (момент времени t) характеризуется состоянием y_t, $t = 0,1,\ldots,T$.

Это состояние может быть достигнуто с помощью выбора управления x_t, которое, если его подставить вместе с состоянием на предшествующем этапе в уравнение состояния

$$y_t = P_{t-1}(y_{t-1}, x_t), \quad (2)$$

переводит процесс в состояние y_t [2].

Решению о выдаче кредита заемщику предшествует формирование и изучение кредитной истории заемщика. На этом этапе определяющее значение имеет кредитный скоринг.

Кредитный скоринг – система оценки кредитоспособности (кредитных рисков) лица, основанная на численных статистических методах. Кредитный скоринг широко используется как крупными банками, МФО, так и в потребительском экспресс – кредитовании на небольшие суммы. Обычно выделяются несколько категорий оценок кредитных рисков: оценка кредитоспособности заемщиков для выдачи кредитов, оценки динамики состояния кредитного счета заемщика и кредитного портфеля в целом, определение кредитных дел и направлений работы с проблемными заемщиками, мониторинг задолженности и др. В последнее время внедрение систем искусственного интеллекта в одном из самых проблемных направлений банковского сектора – кредитном скоринге, получило дальнейшее развитие. Кредитные организации начали разработку собственных программных продуктов, основанных на собственных методиках. На рынке появились специализированные программные продукты, использующие различные математические модели. Информация, необходимая для оценки кредитоспособности заемщика, бралась не только из документов, предоставленных заемщиком, но также из баз данных кредитных организаций.

Рассмотрим случай обращения группы из *n* заемщиков в МФО для получения кредита. В свою очередь, МФО пользуясь приводимой ниже методикой частичного перебора характеристик определения степени кредитоспособности заемщика собирается выдать кредиты первым *m* заемщикам из этой группы.

Скоринг подразумевает, что прошлые связи между риском и характеристиками сохранятся и в будущем. Таким образом, исторический риск становится предиктивным [3].

Любой метод предсказания будущего риска на основе текущих характеристик с использованием информации о прошлых связях между риском и этими характеристиками называется скорингом [3].

Статистический скоринг предсказывает риск на основе количественных характеристик, содержащихся в базе данных. Связи между риском и характеристиками выражены как список правил или формулами, которые предсказывают риск в виде вероятностей.

Перечень сведений о заемщике, используемый в упомянутых методиках, охватывает исчерпывающую информацию, позволяющую оценить его кредитоспособность.

В настоящее время МФО располагает широким набором методик, в т.ч. и собственными разработками.

Пусть в распоряжении МФО одновременно имеется несколько методик.

Каждая из них по определенному набору q характеристик позволяет установить собственную картину кредитоспособности заемщика и оценить вероятность возврата займа. Обычно каждая характеристика оценивается в баллах, а суммарная оценка кредитоспособности выражается через вероятность.

Рассмотрев характеристики по конкретно выбранной методике, после обработки необходимой информации для группы из n заемщиков, МФО создает матрицу характеристик

$$A = \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1q} \\ r_{21} & r_{22} & \dots & r_{2q} \\ \vdots & \vdots & \dots & \vdots \\ r_{n1} & r_{n2} & \dots & r_{nq} \end{pmatrix}$$

В этой матрице r_{ij} – баллы i-го заемщика по j-й характеристике.

Продолжая формирование баллов по характеристикам, МФО определяет вероятность возврата кредита конкретным заемщиком.

В случае возникновения неопределенностей (например, сомнения в достоверности или отсутствии некоторых предоставленных данных, неоднозначности выбора заемщика и др.) МФО (сотрудник МФО, который в данном случае представляет субъективный скоринг [3]) может применить другую методику.

На этом этапе работы сотрудники МФО сталкиваются с небольшой переборной задачей определения первых m заемщиков

для выделения кредитов. Здесь представляется целесообразным предложить выбор заемщиков по неполному, но приоритетному перечню характеристик, а именно, МФО определяя приоритетные l, $l < q$ характеристики, по ним создает новую матрицу:

$$B = \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1l} \\ r_{21} & r_{22} & \dots & r_{2l} \\ \vdots & \vdots & \dots & \vdots \\ r_{n1} & r_{n2} & \dots & r_{nl} \end{pmatrix}$$

Если и на этом этапе не удастся выбрать первых m заемщиков, к последней матрице добавляются одна или несколько дополнительных характеристик l+1, l+2, и формируется новая матрица

$$C = \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1l} & r_{1l+1} \\ r_{21} & r_{22} & \dots & r_{2l} & r_{2l+1} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ r_{n1} & r_{n2} & \dots & r_{nl} & r_{nl+1} \end{pmatrix}$$

Если после этих действий удается выбрать первые $n1$, $n1<n$ заемщиков, приведенную процедуру можно применить для выбора оставшихся $n1$+1, $n1$+2,…, n потенциальных заемщиков

$$D = \begin{pmatrix} r_{n1+1,1} & r_{n1+1,2} & \dots & r_{n1+1,l} & \dots & r_{n1+1,q} \\ r_{n1+2,1} & r_{n1+2,2} & \dots & r_{n1+2,l} & \dots & r_{n1+2,q} \\ \vdots & \vdots & \dots & \vdots & \dots & \vdots \\ r_{n1} & r_{n2} & \dots & r_{nl} & \dots & r_{nq} \end{pmatrix}$$

Для небольших МФО подобная методика может оказать оперативную помощь сотруднику МФО.

Недостатком данного подхода является возможная потеря нескольких «хороших» клиентов на начальных этапах, а преимуществом – быстрый ответ и экономия времени сотрудника МФО ([3]). Также в последнем случае сотрудник МФО имеет возможность оценить вероятность наихудшего и других сценариев развития процесса, располагая вероятностями p_i, i=1,2,...,n, что тоже может быть ориентиром в выборе потенциальных заемщиков.

Литература:

1. *Бахметьева Г.Р., Ерешко Ф.И., Сытов А.Н.* Риск-менеджмент в микрофинансовых инвестиционных организациях // Труды 7-й Международной конференции «Системный анализ и

информационные технологии» (САИТ-2017). – М.: ФИЦ ИУ РАН, 2017. – С. 504-508.

2. *Рихтер К.* Динамические задачи дискретной оптимизации. – М.: «Радио и связь», 1985. – 136 с.

3. *Шрайнер М.* Кредитный скоринг: очередной прорыв в микрофинансировании // CGAP – 2003. – Специальный выпуск № 7. – С. 1-64. – URL: https://documents1.worldbank.org/curated/en/545371468340246527/pdf/334770RUSSIAN0OccasionalPaper1071Ru.pdf (дата обращения 12.02.2021).

III. Проблемы обеспечения информационной безопасности

Сиротюк В.О.

Цели, задачи и принципы обеспечения безопасности цифровых систем управления интеллектуальной собственностью

Аннотация: В работе рассмотрены особенности и характеристики систем управления интеллектуальной собственностью (ИС) в условиях их цифровой трансформации, описаны объекты ИС, угрозы и риски информационной безопасности объектов ИС. Сформулированы цели, задачи и принципы обеспечения информационной безопасности цифровых систем управления ИС. Предложенные принципы и задачи использовались при разработке мероприятий по обеспечению информационной безопасности системы управления ИС международной патентной организации.

Ключевые слова: система управления ИС, объект интеллектуальной собственности, база данных патентной информации, база данных научно-технической информации, угроза информационной безопасности, риск информационной безопасности, система информационной безопасности

Введение

Становление цифровой экономики является одним из приоритетных направлений научно-технического прогресса [1]. Переход к цифровой экономике предполагает цифровую трансформацию традиционных систем управления предприятиями и организациями или целой экономической отрасли на основе использования новых (в т.ч. формальных) моделей бизнес-процессов, менеджмента и способов производства и их оптимизации, применения современных информационно-телекоммуникационных (цифровых) технологий.

Под влиянием новой цифровой парадигмы происходят радикальные изменения в организации и методах проведения

научных исследований и опытно-конструкторских работ. Научное сообщество переходит к новой концепции проведения научных исследований и разработок, основанной на возможности доступа к разнообразным распределенным источникам научной, технической и патентной информации, их обработки и использования, интеллектуального анализа Больших Данных (Big Data) в различных предметных областях.

Цифровая трансформация системы управления интеллектуальной собственности (ИС) позволяет повысить эффективность и качество работы патентных и научных организаций, перейти на новые бизнес-модели и методы управления, избавить сотрудников от рутинных работ и повысить производительность труда и конкурентоспособность организаций. Цифровизация информационных фондов ИС, создание баз данных патентной и научно-технической информации, повышение их полноты, качества, защищенности и доступности является важной и актуальной задачей, решаемой в рамках перехода к цифровой экономике в одной из важных ее отраслей – управление ИС [2].

В работе рассмотрены характеристики системы управления ИС, особенности ее цифровой трансформации и связанные с этим угрозы и риски информационной безопасности объектов ИС; сформулированы цели и принципы информационной безопасности объектов ИС от преднамеренного или непреднамеренного несанкционированного доступа, модификации или разрушения данных; предложен перечень задач обеспечения информационной безопасности цифровой системы управления ИС.

Характеристики системы управления ИС. Угрозы, риски и уязвимые элементы информационной безопасности

Система управления ИС обеспечивает регистрацию, экспертизу и выдачу охранных документов, сопровождение, хранение и охрану объектов ИС с помощью патентов, авторского права и товарных знаков, что позволяет авторам добиваться признания или получать финансовое вознаграждение за свои изобретения или произведения. Обеспечивая баланс интересов изобретателей и широкой публики, система управления ИС способствует созданию условий для развития творчества и инноваций.

Объектами ИС являются результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана. К объектам ИС относятся изобретения, промышленные образцы, полезные модели, литературные, художественные и научные произведения, символика, названия и изображения, используемые в коммерческих целях. ИС охватывает широкий спектр деятельности и играет важную роль в научной, образовательной, культурной и хозяйственной жизни.

Цифровая трансформация традиционной системы управления ИС приводит к построению цифрового органа управления ИС. Эффективная цифровая система управления ИС должна создаваться на принципах и моделях клиентоориентированности и омниканальности, максимизации эффективности обслуживания запросов пользователей. Одной из главных функций цифровой системы управления ИС является формирование, сопровождение и развитие баз данных патентной (ПБД) и научно-технической информации (БД НТИ), информационного поиска по фондам патентной документации и научно-технической литературы.

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. С учетом наличия многочисленных разрозненных источников научно-технической и патентной информации инфраструктура цифровой системы управления ИС должна иметь распределенную структуру и обеспечивать оперативный доступ к локальным и внешним удаленным ПБД и БД НТИ и поиск информации через единый пользовательский интерфейс [2,3].

Цифровизация системы управления ИС, несмотря на все ее преимущества, несет потенциальные угрозы и риски информационной безопасности объектов ИС, поэтому возрастает потребность в надежных и эффективных методах и средствах защиты данных ПБД и БД НТИ, информационной и обеспечивающей инфраструктуры цифрового органа ИС [3].

Основными угрозами безопасности объектов ИС являются [4]:

- раскрытие конфиденциальной информации (кража информации, несанкционированный доступ, копирование данных),
- компрометация информации (внесение несанкционированных изменений в массивы данных и БД),
- несанкционированный обмен информацией,
- отказ от информации (непризнание получателем или отправителем фактов получения/отправки информации),
- отказ в обслуживании (отсутствие доступа к информации).

Уязвимыми элементами цифрового органа управления ИС являются содержимое БД, программное обеспечение, оборудование, пользователи, администраторы данных, документация.

Возможными путями утечки информации об объектах ИС могут быть:

- прямое хищение носителей информации и документов,
- копирование конфиденциальной информации,
- несанкционированное подключение к терминалу пользователей и незаконное его использование,
- несанкционированный доступ к данным.

Цели и принципы обеспечения информационной безопасности цифровой системы управления ИС

Главной целью информационной безопасности (ИБ) цифровой системы управления ИС является обеспечение конфиденциальности, достоверности, неизменности и доступности информационных материалов объектов ИС.

Частными целями и задачами защиты информации об объектах ИС могут быть:

– обеспечение заданного уровня безопасности ПБД и БД НТИ, соответствующего принятым нормативным документам;

– обеспечение экономической целесообразности при выборе защитных мер, основанном на анализе рисков ИБ;

– обеспечение высокого уровня безопасности информационной и обеспечивающей инфраструктуры цифрового органа управления ИС;

– обеспечение регистрации всех действий пользователей с информацией и ресурсами ПБД и БД НТИ;

– обеспечение эффективного анализа регистрационной информации, предоставление пользователям достаточной информации для поддержания режима безопасности;

– разработка планов восстановительных работ после аварий и иных критических ситуаций с целью обеспечения непрерывной работы цифровой системы управления ИС;

– обеспечение строгого соответствия нормативным актам и политике информационной безопасности.

Основными принципами обеспечения информационной безопасности цифровой системы управления ИС являются [3]:

1. *Принцип невозможности «обхода» средств защиты данных.* Означает, что все информационные потоки и пути доступа к данным должны контролироваться средствами защиты.

2. *Принцип слабого звена.* Предполагает в первую очередь усиление с точки зрения безопасности наиболее уязвимых элементов системы.

3. *Принцип гарантированного выполнения функций.* Означает, что при любых обстоятельствах (в том числе нештатных), система защиты информации должна полностью выполнять свои функции, либо полностью блокировать все возможные пути доступа.

4. *Принцип минимизации привилегий.* Предполагает выделение пользователям и администраторам системы только тех прав, которые необходимы им для выполнения служебных обязанностей.

5. *Принцип разделения обязанностей.* Предполагает при распределении прав и ответственности пользователей системы исключение возможности нарушения критически важных для системы функций и процессов одним человеком.

6. *Принцип многоуровневой защиты.* Гарантирует многоуровневую структуру систем обеспечения информационной безопасности с целью повышения ее надежности и эффективности.

7. *Принцип разнообразия средств защиты.* Предполагает одновременное использование различных по своей природе и принципам действия механизмов и методов защиты данных.

8. *Принцип простоты и управляемости.* Предполагает возможность анализа эффективности и доказательства корректности реализации функций автоматизированной системы в целом и используемых механизмов защиты.

9. *Принцип открытости.* Требует разработки комплекса организационных мер, направленных на обеспечение лояльности персонала, его обучение и повышение квалификации при работе с системой, разъяснения прав и обязанностей каждого пользователя.

10. *Принцип непрерывности защиты.* Означает, что информационная безопасность системы управления ИС должна обеспечиваться на всех стадиях жизненного цикла информационных систем.

11. *Принцип избирательного управления доступом.* Средства защиты должны контролировать доступ пользователей к объектам ИС.

Основные задачи информационной безопасности цифровой системы управления ИС

Исходя из необходимости обеспечения требований конфиденциальности, неизменности, достоверности и доступности информации ПБД и БД НТИ, основными задачами информационной безопасности (ИБ) цифровой системы управления ИС являются:

- определение границ системы ИБ;
- распределение обязанностей по обеспечению ИБ;
- подготовка персонала по поддержанию режимов ИБ;
- уведомление о случаях нарушения защиты;
- защита информации ПБД и БД НТИ от вирусов и спама;
- контроль копирования информации ПБД и БД НТИ;
- защита конфиденциальной информации от несанкционированного доступа;
- контроль соответствия принятой политике ИБ;
- управление рисками в области ИБ;
- выбор контрмер, обеспечивающих требуемый уровень ИБ;
- контроль функционирования и аудит системы ИБ.

Заключение

В работе сформулированы цели, принципы и задачи построения эффективной системы информационной безопасности цифровых систем управления ИС. Полученные результаты использовались при подготовке комплекса организационных, технических,

структурных и процедурных мероприятий по построению эффективной системы управления информационной безопасностью Евразийского патентного ведомства – международной региональной патентной организации [2,3].

Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011

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 14.10.2021).

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. *Сиротюк В.О., Грузман В.А., Косяченко С.А.* Структура и характеристики объектов информационной безопасности и классификация информационных ресурсов / Материалы XXVIII Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС-2020) (16 декабря 2020 г. Москва). – М.: ИПУ РАН, 2020. – С. 446-451.

Мелихов А.А.

Обеспечение непрерывной разработки программных продуктов, сертифицируемых по требованиям безопасности

Аннотация: В настоящей работе рассмотрена проблематика сертификации коммерческих программных продуктов по требованиям безопасности, предложена модель гибридного производственного цикла, обеспечивающего процесс непрерывной поставки обновлений.

Ключевые слова: гибкие методологии разработки, сертификация программных продуктов, импортозамещение, безопасная разработка, CI/CD, оптимизация производственных процессов

Сертификация программного обеспечения представляет собой независимую комплексную экспертизу на предмет соответствия требованиям нормативной документации по информационной безопасности. В рамках сертификации проверяются такие свойства программного продукта, как отсутствие недекларированных возможностей и известных уязвимостей в компонентах программного обеспечения, применение исключительно надежных криптографических средств и т.д. В этом процессе сертификационная лаборатория является внешней незаинтересованной стороной и функционирует в отличном от отраслевых стандартов разработки программного обеспечения режиме.

В случае, если производство сертифицируемых продуктов является для организации основным видом деятельности, данное обстоятельство не представляет собой серьезную проблему, т.к. весь процесс производства согласован с работой лаборатории. Однако если сертификация производится для определенной конфигурации некоторого базового продукта, создается эффект «бутылочного горлышка», когда производство стабильно выпускает обновления, при этом цикл подготовки к сертификации занимает больше времени, чем цикл подготовки релиза базовой версии. Как следствие, за время одного цикла сертификации продукт устаревает как минимум на один релиз относительно базового, а если

требуется выпуск продуктов по разным группам требований, то трудозатраты по подготовке возрастают кратно.

В рамках настоящей публикации рассмотрен подход к организации производственного цикла сертифицируемого программного обеспечения, в настоящий момент проходящий апробацию в кампании ООО «Новые Облачные Технологии». Целью подхода является снижение трудозатрат на производство сертифицируемого продукта при поддержании темпов его обновления.

Проблематика

Гибкие методологии разработки программного обеспечения получили широкое распространение в конце XX – начале XXI века как замена традиционных «водопадных» методов. Вне зависимости от конкретной реализации (RAD, SCRUM, экстремальное программирование) в их основе лежат единые принципы организации производственного процесса, такие как планирование короткими интервалами (спринтами), глубокая декомпозиция задач, акцент на самоорганизацию производственного коллектива [1]. Отдельная роль определена и для средств автоматизированной обработки информации: снижение накладных затрат на передачу контекста решаемых проблем (программного обеспечения для совместной работы, трекеры задач), бесшовная интеграция средств разработки, тестирования и развертывания программных продуктов.

В контексте разработки коммерческих программных продуктов, не требующих специальной сертификации, применение гибких методик позволяет работать с короткими релизными циклами (4 и более релиза в год) даже для крупных программных продуктов, однако особенности процедуры подготовки ПО к сертификации вступают в противоречие с фундаментальными принципами «легковесной» разработки (таблица 1).

Таблица 1 – Противоречия между принципами гибкой разработки ПО и требованиями к сертификации

Гибкие методологии	Требования по сертификации
Документация носит ситуативный характер, неконсистентна, фрагментарна, причем элементы обладают различной степенью полноты и дискурсивной связности. Может включать эрративы, семантические, синтаксические и орфографические ошибки специфическую терминологию	Документация выполнена в едином стиле, структурирована согласно ГОСТ 19 серии (ЕСПД), затрагивает конкретные аспекты сборки, настройки и эксплуатации продукта
Потребности заказчика/клиентов имеют высокий приоритет, вследствие чего долгосрочный план носит рекомендательный, а не императивный характер	Все имеющиеся на данный момент функции должны быть документированы, однозначны, непротиворечивы
Разработчик коммерческого продукта может применять актуальные версии инструментов и сторонних программных библиотек, обновляя и заменяя их по мере потери актуальности, нахождения уязвимостей, изменения политик лицензирования	Все программные компоненты, необходимые для компиляции и запуска продукта должны либо входить в дистрибутив (т.е. сертифицироваться совместно с продуктом как библиотеки третьих лиц), либо входить в состав среды выполнения
Процесс сборки может включать в себя обновление исходных кодов и самой среды сборки	Сборка осуществляется в изолированной среде с фиксированным набором инструментов. Обновление исходного кода в процессе сборки не допускается, автоматическое порождение кода нежелательно
Тестирование в среде исполнения производится в типовой ее конфигурации	Тестирование в среде исполнения производится с использованием средств защиты информации

На ранних этапах технологическая цепочка выпуска сертифицированного релиза выглядела следующим образом: 1) производится выпуск коммерческой версии продукта; 2) определяется вид сертификации и требования; 3) производится доработка продукта с учетом требований; 4) производится доработка документации с учетом внесенных изменений; 5) все необходимые артефакты передаются в сертификационную лабораторию; 6) по мере нахождения ошибок производится их устранение и повторная передача обновленных версий продукта и документации; 7) после прохождения соответствующих проверок выдается соответствующее заключение. Если далее требуется сертификация того же релиза в другой системе сертификации или по другим требованиям, цикл начинается заново, однако за счет накопленного опыта производится быстрее. Легко заметить, что этап устранения найденных проблем является итеративным и по своей сути является наименее предсказуемым по возможным временным и трудовым затратам.

Гибридная модель производственного цикла сертифицируемого ПО

Для решения указанных выше противоречий и снижения накладных расходов на подготовку сертифицируемых релизов, предлагается гибридная модель организации производственного цикла, учитывающая зависимость сертифицируемого продукта от базового. Основная идея реализуемого подхода состоит в определении степени этой зависимости и разделении задач по подготовке релизов.

Фактически, весь производственный процесс делится на два этапа, выполняемых коллективами с разными наборами компетенций: 1) выпуск базового продукта осуществляется в режиме принятой в организации гибкой методологии разработки, результатом прохождения этапа являются следующие артефакты: исходные коды продукта, конфигурация сборочной среды и список внесенных изменений; 2) выпуск сертифицированной версии осуществляется на основе полученных от основного производства артефактов путем доработки исходного кода, внесения изменений в среду сборки, сборки продуктов в требуемых условиях, тестирование продукта, доработку документации, передачу

требуемых артефактов сертификационной лаборатории, устранение найденных проблем и, собственно, получение сертификата.

Рассмотрим второй этап более подробно. В свою очередь, в нем можно выделить две стадии, выполняемые последовательно: адаптация сборочной среды вместе с доработкой исходного кода и создание артефактов для сертификации. На первой стадии производится внесение изменений в сборочную среду (добавление возможности отключения несертифицируемых модулей, изолированные сборки и т.п.), при этом от производства необходимо получить конфигурацию среды и исходные коды. Исходные коды размещаются в собственном репозитории, доступ к которому имеют разработчики только сертифицируемого продукта. После получения успешных сборок продукта, он считается готовым к проведению сертификации, конфигурация среды фиксируется. На второй стадии создаются финальные подготовленные сборки, дорабатывается документация, артефакты передаются в лабораторию. Первая стадия выполняется один раз для релиза, в то время как вторая может повторяться итеративно. По мере решения задач, повторяющиеся действия могут быть автоматизированы на более раннем этапе. К примеру, если на каком-либо этапе сборки будет применяться специфический инструмент, например svace, то имеет смысл заранее обеспечить его работоспособность на этапе подготовки среды.

В таком случае зоны ответственности разделяются между специалистами следующим образом: на первой стадии наиболее загруженными являются инженеры, отвечающие за техническую подготовку релиза, а на второй – документоведы и выходной контроль. Данный подход позволяет дать инженерам возможность доработки функциональности сборочных конвейеров, например, реализовав полностью автоматизированную сборку сертифицируемого продукта с нужными параметрами.

Отдельное внимание при внедрении данной модели технологического процесса необходимо уделить документированию. Документацию условно можно разделить на две категории [2]: выходная документация согласно ГОСТ и информационный ресурс, необходимый для обеспечения непрерывного производственного процесса. Такой ресурс может создаваться на базе уже имеющихся средств организации

коллективной работы в связке с трекером задач и включать в себя: лингвистическое обеспечение (глоссарии терминов, указания по именованию артефактов и т.п.), нормативно-правовую базу, описания сборочных сред, инфраструктурных сервисов, процессов сборки, рекомендации по устранению проблем, руководства по развертыванию инфраструктуры. Основным требованием к данному информационному ресурсу является соблюдение его консистентности, непротиворечивости и актуальности.

Для создания выходных документов согласно требованиям ЕСПД в автоматическом может применяться система издательского типа, например на базе LaTeX, обеспечивающая возможность повторного использования текстовых фрагментов в различных документах [3]. Такая система может быть интегрирована со средствами автоматизированной сборки и получать из нее в автоматическом режиме необходимые данные – списки файлов, контрольные суммы и т.п.

Выводы

Обеспечение непрерывности поставок сертифицированного программного продукта представляет собой комплексную проблему, требующую принятия организационно-технических мер, направленных на снижение временных и операционных издержек на доработку базового продукта согласно требованиям безопасности. Для решения данной проблемы была разработана гибридная модель производственного цикла, позволяющая выделить операции, выполняемые в процессе подготовки к сертификации и оптимизировать их с точки зрения трудозатрат за счет выявления повторяющихся однотипных действий. В настоящий момент модель находится в фазе апробации.

Литература:

1. *Мелихов А.А.* Проблематика применения методов автоматической обработки текстов в системах предотвращения утечки данных / Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам Международной научно-практической конференции (23 апреля 2019 г. Москва). – Москва: Российский государственный гуманитарный университет, 2019. – С. 108-114.

2. *Лобанов И.А., Мелихов А.А., Белавкин П.А.* Формирование иерархии синтаксических структур при управлении взаимодействием информационных потоков / Нейрокомпьютеры и их применение: тезисы докладов (13 марта 2018 года Москва). – Москва: Московский государственный психолого-педагогический университет, 2018. – С. 403-405.

Козлов А.Д., Нога Н.Л.

Достоверность информации как элемент обеспечения информационной безопасности и оценка ее уровня

Аннотация: В работе авторы предлагают дополнить основные характеристики обеспечения информационной безопасности информационных систем, включая сложные сетевые структуры, категорией достоверности, как ее важной составляющей.

Ключевые слова: достоверность, информационная безопасность, доверие, уровень достоверности, нечеткая логика

В настоящее время в России поставлена задача широкого внедрения цифровых технологий в различных областях экономики [1,2], включая, в том числе, разработку и внедрение систем с искусственным интеллектом.

Федеральная программа «Цифровая экономика Российской Федерации» определяет, что для решения всего комплекса поставленных задач и достижения указанных целей необходимо развитие и совершенствование основных инфраструктурных элементов цифровой экономики (информационная инфраструктура, информационная безопасность).

Нормативные документы в области информационной безопасности (ГОСТы, РД и др.) направлены на защиту информации от несанкционированного доступа, модификации или потери возможности ее использования. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите

информации» кроме вышеназванных типов нарушения указывает на необходимость обеспечения достоверности в информационных системах. При этом за нарушения принципа достоверности в государственных информационных ресурсах предусмотрена ответственность, вплоть до уголовной.

Так что такое достоверность, как она обеспечивается и как может влиять на результаты функционирования цифровой экономики?

Достоверность информации – свойство информации, характеризуемое степенью соответствия реальных информационных единиц их истинному значению [3]. Также можно определить, что достоверность информации – это характеристика ее неискаженности. Достоверность информации сильно зависит от ее адекватности, объективности, полноты и полезности.

Полезность информации обеспечивается за счет применения фундаментальных качественных характеристик – уместности, правдивого представления и существенности, и повышается за счет таких качественных характеристик, как сопоставимость, своевременность, проверяемость и понятность [4]. Правдивое (достоверное) представление информации в свою очередь характеризуется полнотой, нейтральностью и отсутствием существенных ошибок.

Как известно, даже в бухгалтерской отчетности нет 100% достоверности, и параллельно может существовать «белая» и «черная» бухгалтерии. Также возможно использование недостоверного (например, похищенного) аккаунта в различных сетевых ресурсах.

Но если недостоверную информацию предоставить для выработки управленческих решений, то результат может быть плачевный. Не говоря о важности достоверных разведданных при проведении военных операций, можно привести следующие повседневные примеры.

Сейчас многие пользуются услугами различных навигаторов: недостоверная информация о дорожной ситуации, ДТП, о поломках городского транспорта может привести к выбору неверного маршрута и потери времени.

В период пандемии важно достоверно знать эпидемиологическую ситуацию в разных регионах: недостоверная

информация может способствовать вспышке заболеваемости или к неоправданно жестким ограничительным мерам.

Особенно важной категория достоверности становится в случаях с искусственным интеллектом – недостоверная информация может привести к невыполнению поставленных задач, а если это связано с системами жизнедеятельности, то и к трагическим последствиям.

Таким образом, достоверность должна являться элементом информационной безопасности.

Что влияет на достоверность информации и как ее повысить?

Для оценки достоверности в информационных системах необходимо проследить всю цепочку от сбора, передачи, обработки, хранения и использования данных, лежащих в основе информационных систем и на основе которых функционирует или будет функционировать цифровая экономика.

1. Сбор данных, какие данные собирает ИС.

Булевы переменные обладают практически 100% достоверностью, так как могут принимать всего два значения, т.е. характеризовать произошло или нет некоторое событие, подлежащее учету. Такие переменные можно еще назвать – транзакционными, т.к. они могут быть сформированы после завершения некой транзакции.

Количественные переменные. Достоверность количественных переменных зависит от метода их измерения и точности используемого оборудования. Если при этом полученные значения будут суммироваться (например, статистика по регионам), то возможная ошибка будет накапливаться с каждым суммированием.

Качественные переменные являются наиболее субъективными и наименее достоверными.

2. Источник информации и метод сбора. Транзакционный, например, кассовый аппарат в магазине, или сбор статистической или бухгалтерской отчетности по определенным формам за определенный период.

Источник с разным уровнем доверия. При этом низкий уровень доверия может быть компенсирован большим объемом выборки. В этом случае статистическая погрешность уменьшается.

Необходимо учитывать, что «излишняя доверчивость» может привести к отрицательному результату, так как через доверенный источник может также поступать дезинформация (чем часто пользуются мошенники). Доверяй, но проверяй.

3. Метод (способ) передачи информации. Информация может поступать в информационную систему непосредственно по каналам электросвязи и автоматически вводиться в БД системы, а может поступать по каналам электронной почты или почтовой связи. В этом случае ввод информации будет осуществляться вручную или в автоматизированном режиме. Чем меньше людей будет задействовано на этом участке, тем меньше влияние субъективных факторов и выше достоверность.

4. Метод обработки данных, включая алгоритмы обработки. Методы обработки могут зависеть от поставленной задачи. В этом случае, при достоверных данных, если применяются неверные (неправильно была поставлена задача) или ошибочные (человеческий фактор) алгоритмы, то могут быть получены неверные (недостоверные) результаты.

5. Своевременная актуализация данных. Чем выше частота обновления данных, тем более достоверная информация находится в информационной системе.

6. Форма и метод использования данных. Например, на объектах критической информационной инфраструктуры требования к обеспечению достоверности должны быть существенно выше.

Для получения достоверной информации необходимо использовать несколько источников, в том числе и с разным уровнем доверия. Чем выше репрезентативность при получении данных, тем выше достоверность информации в ИС.

Основываясь на вышесказанном, достоверность можно представить, как некую функцию, зависящую от перечисленных параметров.

$$D = D\{TD, \Delta i, Ki, MT, MP, A(t), U\} \quad (1)$$

где TD – параметр, определяющий тип данных; Δi – ошибка измерения; Ki – параметр, характеризующий источник информации, включая репрезентативность выборки; MT – характеристика метода сбора и передачи информации; MP – характеристика метода

обработки данных; A(t) – частота обновления (актуализации) информации; U – характер (цель) использования данных.

Оценка достоверности

Так как категория достоверности является элементом безопасности информационных технологий, то возникает необходимость оценивать уровень достоверности и риски, связанные с обеспечением достоверности.

В приведенной выше формуле многие параметры трудно представить количественно, а их взаимное влияние находится в области неопределенности. Поэтому предлагается оценку уровня достоверности в информационных системах проводить с использованием метода нечеткой логики аналогично оценке риска информационной безопасности, изложенной в работе [5].

Представив достоверность как лингвистическую переменную и, например, определив экспертным путем границы терма (таблица 1), то можно определять уровень достоверности как качественно, так и количественно.

Таблица 1 – Уровни достоверности

№ п/п	Уровень достоверности	Границы терма «Достоверность»
1	Абсолютно ненадежный	0-0,4
2	Ненадежный	0,4-0,6
3	Довольно надежный	0,6-0,9
4	Полностью надежный	0,9-1,00

Выводы

Достоверность информации в информационных системах различного уровня является важным элементом обеспечения безопасности функционирования цифровой экономики. Для ее обеспечения рекомендуется:

– минимизировать использование качественных показателей в информационных ресурсах;

– максимально использовать транзакционный метод сбора данных, постепенно отказываясь от периодической отчетности;

– минимизировать влияние субъективных факторов (участие человека) на подготовку и передачу данных;

– обеспечивать репрезентативность, дублировать поступающую информацию из разных источников;

– по возможности увеличить частоту обновления (актуализации) данных.

Литература:

1. Указ Президента Российской Федерации от 7 мая 2018 года № 204 «в редакции 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2024 года». – URL: http://publication.pravo.gov.ru/Document/View/0001201805070038 (дата обращения 11.10.2021).

2. Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года». – URL: http://publication.pravo.gov.ru/Document/View/0001202007210012?index=3&rangeSize=1 (дата обращения 11.10.2021).

3. Бизнес ПРОСТ, Что такое достоверность информации? Описание и определение понятия. – URL: https://biznes-prost.ru/dostovernost-informacii.html (дата обращения 30.09.2021).

4. *Арбатская Т.Г.* К вопросу о сущности категории «достоверность» // Международный бухгалтерский учет. – 2015. – № 8. – С. 17-32.

5. *Козлов А.Д., Нога Н.Л.* Риски информационной безопасности корпоративных информационных систем при использовании облачных технологий // Управление риском. – 2019. – № 3. – С. 31-46.

Сомов С.К.

Проблема оптимизации схемы восстановления разрушенного оперативного резерва данных в распределенных системах

Аннотация: В работе рассмотрена проблема восстановления разрушенных оперативных данных, используемых в распределенной системе, с помощью специального восстановительного резерва. Предложены различные схемы организации процесса восстановления

разрушенных данных. Предложена формальная модель восстановления данных, на основе которой поставлена задача поиска схемы восстановления разрушенных данных, оптимальной по различным критериям оптимальности решения задачи.

Ключевые слова: распределенные системы, оперативное резервирование, восстановительное резервирование, схема восстановления разрушенного резерва

Для обеспечения высокой степени сохранности информации, используемой в распределенных информационных системах, широко используется метод информационной избыточности. А именно – создание и размещение в узлах компьютерной сети, на основе которой работает РСОД, оперативного резерва, состоящего из некоторого количества копий и/или предысторий массивов данных [1]. Такой подход сильно снижает величину вероятности потери или искажения данных, но не исключает полностью возможность искажения или потери данных, используемых в распределенной системе и распределенных в нескольких узлах системы. Данная проблема может быть эффективно устранена путем использования двух методов восстановительного резервирования [2]:

1) Первый метод заключается в том, что для восстановления разрушенных в узле системы оперативных данных используется восстановительный резерв (ВР), в качестве которого используется неразрушенный оперативный резерв, расположенный в узле системы, ближайшем к узлу с разрушенными данными.

2) Согласно второму методу для восстановления разрушенных в некоем узле системы данных используется специальный резерв из копий и/или предысторий массивов данных – архив магнитных носителей (АМН). Данный архив используется только для восстановления разрушенных данных. Данный метод заключается в том, что в узле с АМН создаются копии массивов данных, которые затем пересылаются в узел с разрушенными данными.

Для восстановления разрушенных данных используется одна из двух стратегий восстановления: В-1 или В-2 [2]. При использовании стратегии В-1 в узле с ВР последовательно, одна за другой, на основе данных ВР создается необходимое количество копий

массива данных ОР, который необходимо восстановить. Восстановленные копии затем пересылаются в узел с разрушенным ОР. Восстановление разрушенного ОР согласно стратегии В-2 происходит аналогично стратегии В-1 за одним исключением: при создании очередной копии массива данных используется не только ВР, но и все восстановленные на данный момент массивы данных.

С учетом того, что РСОД состоит из множества узлов, соединенных между собой каналами связи, для восстановления разрушенных данных в некотором узле системы возможно использование различных схем восстановления.

Предположим, что в некотором i-м узле системы использовался оперативный резерв из m копий массива данных, которые в силу некоторых причин были разрушены. Предположим, что в узле j, ближайшем к узлу i с разрушенным резервом, размещен восстановительный резерв, содержащий копии разрушенных в узле i массивов данных. Тогда восстановительный резерв в узле j можно использовать следующим образом. Восстановить с помощью ВР j-го узла y $(1 \leq y \leq m)$ копий разрушенного массива. Затем по каналам связи переслать в i-й узел y восстановленных копий. Остальные $(m - y)$ копий разрушенного массива восстанавливаются простым копированием в самом узле j. В итоге возникает задача определения такого количества y восстанавливаемых в узле с ВР копий массива, чтобы достигалось оптимальное значение критерия оптимальности задачи.

На примере стратегии В-1 сформулируем задачу поиска оптимальной схемы восстановления разрушенных данных. В качестве критериев оптимизации можно использовать следующие три варианта:

– минимум средних затрат *Z(y)* системы на восстановление разрушенного ОР;

– минимум среднего времени *E(y)* затраченного на восстановление разрушенного ОР;

– максимум вероятности *P(y)* восстановления разрушенного оперативного резерва.

Предположим, что в узле с ВР копии массивов данных восстанавливаются последовательно и пересылаются в узел с разрушенным ОР также последовательно. В этом случае на восстановление разрушенного резерва будет затрачено время,

величина которого будет состоять из трех компонент: время, затраченное в узле с ВР на получение *y* копий массива данных, затраты времени на передачу полученных копий в узел с разрушенным ОР по каналам связи и время, затраченное в узле с ОР на создание в нем остальных *(m-y)* копий массива.

Предположим, что на восстановление одной копии массива в узле с ВР затрачивается *T* единиц времени. Обозначим через *t* среднее время передачи по каналам связи одной копии массива данных. Тогда для оценки среднего времени *E(y)* восстановления *y* копий массива данных требуется рассмотреть следующие варианты соотношений времени *t* и времени *T*, представленные на рисунке 1.

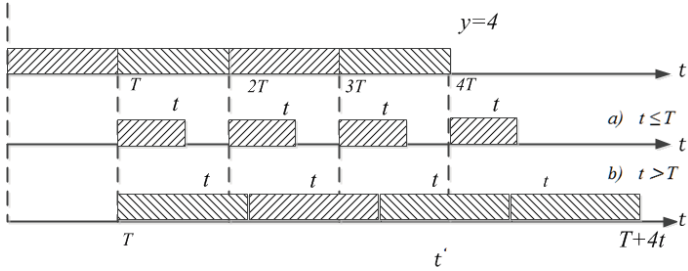


Рисунок 1 – Соотношения между значениями времен *T* и *t*

a) $t \leq T$ – ситуация при которой среднее время t передачи по каналам связи между двумя узлами одной копии массива данных не превышает среднего времени создания копии такого же массива данных в узле с ВР.

b) $t > T$ – в этой ситуации среднее время *t* передачи по каналам связи одной копии массива больше, чем время ее создания в узле с восстановительным резервом.

С учетом представленных выше вариантов среднее время *E(y)* восстановления оперативного резерва, разрушенного в узле системы, будет равно:

$$E(y) = \begin{cases} yT + t + (m-y)\tau & при\ t \leq T \\ yt + T + (m-y)\tau & при\ t > T \end{cases} \quad (1)$$

В формуле (1) τ это величина среднего времени создания в узле с ОР одной копии массива данных.

Разрушенный в узле системы оперативный резерв будет успешно восстановлен с вероятностью:

$$P(y) = \beta^m(\rho r \beta^{-1}) \quad (2)$$

В формуле (2):

– ρ – это вероятность, с которой в узле с ВР создается копия массива данных, необходимая для восстановления разрушенного ОР;

– r – это вероятность успешной передачи восстановленной в узле с ВР копии массива данных в узел, в котором необходимо восстановить разрушенный ОР;

– β – это вероятность, с которой в узле с ОР создается копия массива данных, необходимая для полного восстановления разрушенного ОР.

На восстановление разрушенного ОР в узле системы в среднем тратятся ресурсы *Z(y),* которые равны:

$$Z(y) = y(D + d^* - H) + H * m \quad (3)$$

Здесь: H – затраты ресурсов системы на создание одной копии массива в узле с ОР, d^* – стоимость использования каналов связи для передачи между двумя узлами одной копии восстанавливаемого массива, D – затраты ресурсов системы на восстановления одной копии массива в узле с ВР.

Предположим, что выполняется соотношение: $M \le y \le N\ (1 \le M, N \le m)$ и выполним анализ значений для *E(y).* В соответствии с формулой (1) получаем, что *E(y).*<0 при $t \le T, T < \tau$ и $t > T, t < \tau$. Из этого утверждения следует, что:

$$\begin{aligned} &\textit{при } t \le T \quad \min E(y) = \begin{cases} m\tau + t + N(T - \tau) \textit{ при } T < \tau \\ m\tau + t + M(T - \tau) \textit{ при } T \gg \tau \end{cases} \\ &\textit{при } t > T \quad \min E(y) = \begin{cases} m\tau + T + N(t - \tau) \textit{ при } t < \tau \\ m\tau + T + M(t - \tau) \textit{ при } t \gg \tau \end{cases} \end{aligned} \quad (4)$$

Для *P(y) и Z(y)* получим следующие выражения:

$$\begin{aligned} \max P(y) &= \begin{cases} P(N) \quad \textit{при } \rho r > \beta \\ P(M) \textit{ при } \rho r \le \beta \end{cases} \\ \max Z(y) &= \begin{cases} Z(N) \textit{ при } (D + d^*) < H \\ Z(M) \textit{при } (D + d^*) \ge H \end{cases} \end{aligned} \quad (5)$$

С учетом полученных результатов задача определения оптимальной схемы восстановления разрушенного ОР с

использованием в качестве критерия минимума затрат системы будет иметь следующую формулировку:

$$Z(y) \to \min \quad (6)$$

при следующих ограничениях: $P(y) \geq \bar{P};\ E(y) \leq \bar{E}; y \in \{1,2,\dots,m\}$.

Здесь $\bar{P}$ и $\bar{E}$ это ограничения на минимальную вероятность успешного восстановления и на максимальные затраты системы на восстановление разрушенного ОР, соответственно.

Аналогичным путем формулируются задачи поиска наилучшей схемы восстановления оперативного резерва, разрушенного в некотором узле системы, с помощью восстановительного резерва с использованием в качестве критерия оптимальности задачи минимума среднего времени восстановления разрушенного ОР и максимума вероятности восстановления разрушенного ОР.

Заключение

В работе предложена формальная модель возможных схем восстановления разрушенного оперативного резерва в распределенной системе. На ее основе предложены формулировки задач оптимизации схемы восстановления разрушенных данных с использованием нескольких критериев оптимальности решения данных задач.

Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011

Литература:

1. *Сомов С.К.* Сохранность информации в распределенных системах обработки данных. – М.: ИПУ РАН, 2019. – 254 с.

2. *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.

Сомов С.К.

Анализ целесообразности использования архивов магнитных носителей в распределенных системах в качестве восстановительного резерва

Аннотация: В работе рассмотрена проблема оценки эффективности использования архивов магнитных носителей и неразрушенного оперативного резерва для восстановления разрушенных оперативных данных распределенной системы. Получены условия, определяющие целесообразность использования в распределенных системах неразрушенного ОР или АМН в качестве восстановительного резерва.

Ключевые слова: распределенные системы, оперативное резервирование, восстановительное резервирование, схема восстановления разрушенного резерва

Для обеспечения высокой степени сохранности информации, используемой в распределенных информационных системах, широко используется метод информационной избыточности. А именно – создание и размещение в узлах компьютерной сети, на основе которой работает РСОД, оперативного резерва (ОР), состоящего из некоторого количества копий и/или предысторий массивов данных [1]. Такой подход сильно снижает вероятность потери массивов данных, используемых в распределенной системе. Однако он не исключает полностью возможность искажения или потери данных. Данная проблема эффективно решается за счет использования одного из двух методов восстановительного резервирования (ВР) [2]. В первом методе для восстановления ОР, поврежденного в некотором узле системы используется работоспособный ОР, размещенный в другом узле, ближайшем к узлу с поврежденным ОР. Во втором методе для восстановления поврежденного резерва данных используются специальные архивы магнитных носителей, размещенные в одном или нескольких узлах системы. В отличие от первого метода АМН обрабатывает только запросы на восстановление разрушенного ОР.

Получим условие, определяющее то, при каких условиях будет целесообразно (с точки зрения времени восстановления

разрушенных данных оперативного резерва) использовать АМН в качестве ВР вместо неразрушенного ОР, расположенного в ближайшем узле системы.

Рассмотрим РСОД, работающую на базе однородной вычислительной сети, в которой возможно использование обоих методов восстановительного резервирования. Предположим, что процесс обработки запросов на восстановление в узлах системы с АМН и ОР описывается в терминах системы массового обслуживания типа M/M/I [3]. На вход такой системы поступает пуассоновский поток запросов на восстановление данных (с интенсивностью λ для узла с ОР и μ для узла с АМН), а время их обслуживания распределено по показательному закону. Будем считать, что время передачи информации по каналам связи (запроса на восстановление и восстановленных копий массивов данных в узел с разрушенным ОР), одинаково для обоих рассматриваемых вариантов метода восстановления ОР. Согласно [3], при сделанных предположениях среднее время T_A восстановления данных при помощи АМН и среднее время T_P восстановления данных при помощи неразрушенного ОР определяются по следующим формулам:

$$T_A = T_n + E_A + w_A = T_n + E_A(1 - \mu E_A)^{-1} \quad (1)$$

$$T_P = T_n + E_P + w_P = T_n + E_P(1 - \lambda E_P)^{-1} \quad (2)$$

В формулах использованы обозначения: T_n – среднее время передачи информации по каналам связи; E_A – среднее время обработки запроса на восстановление данных в узле с АМН; w_A – среднее время ожидания запроса в очереди на обработку в узле с АМН; E_P и w_P – среднее время обработки и ожидания в очереди на обработку запроса в узле с ОР; μ – интенсивность запросов на восстановление, поступающих в узел сети с АМН; λ – интенсивность всех запросов, поступающих в узел сети с неразрушенным ОР.

Очевидно, что с точки зрения величины среднего времени восстановления разрушенного оперативного резерва использование для этой цели АМН нецелесообразно, если $T_P < T_A$, или с учетом (1) и (2):

$$\lambda < \mu + (E_A - E_P)(E_A E_P)^{-1} \quad (3)$$

Таким образом, если справедливо неравенство (3), то, с точки зрения величины среднего времени восстановления разрушенного оперативного резерва в узле системы, целесообразно использовать в качестве восстановительного резерва неразрушенный ОР ближайшего узла вместо АМН.

Рассмотрим несколько примеров использования приведенных выше результатов. Допустим, что РСОД функционирует на базе однородной полносвязной компьютерной сети из *N* узлов. В узлах системы размещен оперативный резерв, созданный в соответствии со стратегией 1 оперативного резервирования из m копий массивов [1]. В каждый из узлов поступают запросы к массивам данных с интенсивностью λ запросов в единицу времени. Вероятность разрушения одной копии массива данных при обработке одного поступившего запроса к данным равна q.

Определим целесообразность создания в одном из узлов системы архива магнитных носителей объемом m копий массива. Целесообразность создания АМН будем оценивать по оценке величины среднего времени восстановления оперативного резерва.

Так как по условиям примера объемы ОР каждого узла системы совпадают с объемом АМН, то в силу однородности сети получим, что $E_A = E_P$ и условие (3) будет иметь вид:

$$\lambda < \mu \tag{4}$$

Интенсивность μ возникновения в одном узле системы запросов на восстановление разрушенного оперативного резерва из m копий будет равна:

$$\mu = \sum_{n=1}^{N} \lambda q^m = N\,\lambda q^m \tag{5}$$

Тогда условие (4) будет эквивалентно следующему неравенству:

$$1 < N q^m \tag{6}$$

Пример 1. Допустим, что m=3 и N=4.

В этом случае создание АМН нецелесообразно с точки зрения величины среднего времени восстановления ОР при $q > 0.69$.

Однако в реальных системах обработки данных, работающих в установившемся режиме $q < 0.5$. Следовательно, в данном случае создание АМН в системе целесообразно.

Пример 2. Допустим, что m=3 и N=4.

Определим число узлов системы с ОР, при котором использование только одного узла с АМН для их восстановления будет нецелесообразно, т.е. время ожидания запроса на восстановление данных в очереди на обслуживание в узле с АМН будет больше, чем время ожидания в ближайшем узле с неразрушенным ОР.

Из неравенства (6) при заданных параметрах следует, что

$$N > q^{-3} \tag{7}$$

Тогда при $q = 0.5$ создание только АМН только в одном узле системы будет нецелесообразно для $N \geq 8$, а при $q = 0.1$ для $N \geq 1\,000$.

Пример 3. Рассмотрим случай, когда в системе используется не один, а несколько узлов с АМН. Будем считать, что все возникающие запросы на восстановление разрушенных в узлах ОР распределяются между узлами с АМН равномерно. Обозначим через *K* число узлов системы с АМН.

Определим то, какое число узлов с АМН должно быть в сети, чтобы среднее время восстановления разрушенного ОР с помощью АМН было меньше, чем с помощью неразрушенного ОР. Из (4) следует, что для этого необходимо не меньше μ/λ узлов с АМН.

Тогда, используя (6), получим, что при условии:

$$5) \quad K \geq Nq^m \tag{8}$$

обработка запросов в узлах с АМН запросов на восстановление разрушенного оперативного резерва будет выполняться за время, меньшее времени обработки в узлах с неразрушенном оперативным резервом.

Пример 4. Пусть *N*=30, *m*=2, *q*=0.2. В этом случае из неравенства (8) следует, что при заданных параметрах в системе необходимо разместить два АМН объемом 2 копии в *K*=2 узлах системы.

Заключение

В работе выполнен анализ условий, при которых целесообразно использование в распределенных системах одного из двух вариантов восстановительного резерва: неразрушенного оперативного резерва или специального архива магнитных

носителей. Получены условия, определяющие целесообразность с точки зрения величины среднего времени восстановления разрушенных данных использования в распределенных системах неразрушенного ОР или АМН в качестве восстановительного резерва.

Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011

Литература:

1. *Сомов С.К.* Сохранность информации в распределенных системах обработки данных. – М.: ИПУ РАН, 2019. – 254 с.

2. *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.

3. *Клейнрок Л.* Вычислительные системы с очередями. – М.: Мир, 1979. – 600 с.

Правиков Д.И.

Концепция информационной безопасности «роя» киберфизических систем

Аннотация: На основании анализа существующих подходов сделан вывод о необходимости разработки для комплексов киберфизических систем новых подходов к обеспечению их информационной безопасности. Показано, что комплекс киберфизических систем может быть описан как множество взаимодействующих прикладных программ. Для обеспечсения свойства незамкнутости комплекса киберфизических систем предложено управление безопасностью перенести в распределенный реестр, а определение санкционированности действий осуществлять на основании алгоритма консенсуса.

Ключевые слова: киберфизическая система, информационная безопасность, распределенный реестр, алгоритм консенсуса

Существующие теории информационной безопасности в основном построены на замкнутости защищаемых систем. При этом в основе наиболее распространенных методов обеспечения безопасности (моделей разграничения доступа) лежит субъекто-объектная теория, описанная, например, в [1]. Указанный подход очень хорошо подходит для обеспечения безопасности в автоматизированных информационных системах, предназначенных для хранения и обработки данных, но, как показывает практика, не вполне применим для киберфизических систем, где основной задачей является техническое управление.

В настоящее время обеспечение информационной безопасности киберфизических систем (как комплексов кибефизических устройств), являются предметом изучения и рассмотрения различных научных коллективов [2]. При этом современные тенденции, идущие от практики, показали появление таких подходов, как архитектура «с нулевым доверием», описанная в NIST Special Publication 800-207 Zero Trust Architecture, для которой существуют описанные подходы к обеспечению безопасности, но они не имеют соответствующего теоретического обоснования.

Возможное решение, основанного на использовании существующих теоретических разработо, было положено в основу изобретения [3], в соответствии с которым в «одноранговых коммуникационных сетях киберфизических устройств, включающем управление настройками маршрутизации, дополнительно вводят блок осуществления политики безопасности, в котором формируют правила политики безопасности в виде матрицы доступа между киберфизическими устройствами, получают запросы на сетевой доступ между киберфизическими устройствами, формируют и пересылают киберфизическим устройствам управляющие команды, внося изменения в их таблицы маршрутизации и тем самым определяя разрешенные правилами политики безопасности маршруты пересылки пакетов от одного устройства к другому».

Вместе с тем, предложенное изобретение, на наш взгляд, имеет ряд существенных ограничений. Попытки преодолеть недостатки

были предприняты, например, в [4], где предложена графовая модель функционирования промышленной системы (ПС), которую можно рассматривать как один из вариантов представления комплекса киберфизических устройств. Данная модель описывает сетевую инфраструктуру ПС в виде ориентированного графа G, множество вершин $V = \{v_1, \dots, v_N\}$ которого характеризует все компоненты ПС, способные к сетевому взаимодействию. Множество дуг $E = \{e_1, \dots, e_M\}$ графа отражает все возможные межкомпонентные связи, проявляющиеся как обмен данными между устройствами. Каждый компонент ПС, моделируемый вершиной v_i, характеризуется набором функций, которые он способен реализовывать.

Упомянутая работа [4] интересна тем, что компьютерные атаки описаны в виде преобразований графа G. Они разделяются на структурные, представляющие собой унарные операции над G, и функциональные, заключающиеся в изменении параметров вершин и дуг.

Полное перечисление возможных видов атак на промышленную систему представлено в работе [5], в которой все возможные атаки сведены к набору элементарных действий.

Таким образом, проведенный обзор литературы показывает, возможность описания комплекса киберфизических устройств в виде набора взаимодействующих прикладных программ.

Тогда, пусть у нас существует комплекс киберфизических устройств, работу которого мы считаем безопасной. Для него справедливы следующие постулаты.

Постулат 1. В созданном комплексе киберфизических устройств набор прикладных программ является взаимоувязанным, что подразумевает, что выход одной прикладной программы является входом для другой. Если прикладная программа получает данные извне, то эти данные являются входными для всего комплекса. Если у данных, генерируемых программой нет потребителя, то эти данные являются выходом всего комплекса.

Постулат 2. Любая прикладная программа, находящаяся на одном из киберфизических устройств, объединенных в комплекс, не может иметь входного потока данных, кроме как входного потока для всей системы или от другой прикладной программы, зарегистрированной в комплексе.

Постулат 3. Любая прикладная программа направляет свои данные для другой прикладной программы, зарегистрированной в комплексе, либо на выход всего комплекса, описанный и заданный извне.

Исходя из описанных постулатов можно утверждать, что изменение комплекса киберфизических устройств, приводящее к нарушению 1, 2 или или 3, нарушает безопасность всего комплекса.

Вместе с тем, перечисленный в работе [5] перечень элементарных действий характерен и для штатной модернизации системы. В результате, если руководствоваться только тремя постулатами, будут выявляться воздействия на систему, обнаруживаемые, условно говоря, на уровне противоаварийной защиты. Более сложным случаем является, например, атака MiM, сходная в плане своей реализации со штатной модернизацией системы. Таким образом, задача выявления атак сводится к задаче различения администрирования от несанкционированного воздействия, при условии того, что объект, реализующий положения упомянутой Аксиомы 2 должен находиться за пределами отдельного киберфизического устройства.

Решение данной задачи предлагается осуществлять на основании подхода, определяющего санкционированность или несанкционированность совершаемых действий. Действие, в том числе элементарное, считается санкционированным, если запрос на его реализацию подтверждается всеми сторонами. Применительно к рассматриваемому случаю это будет означать, что совершенное действие получило подтверждение от администратора (в роли которого может выступать автоматическая система администрирования или искусственный интеллект), а также от других киберфизических устройств, перестраивающих свой информационный обмен. В результате запрос на изменение потока данных должен получить подтверждение, выработанное на основании некоего алгоритма консенсуса. Это, в свою очередь (пока теоретически) приводит к тому, что потенциальный злоумышленник при реализации атаки MiM должен инициировать получение подтверждений уже от нескольких источников, что существенно усложняет саму атаку.

В этом случае подключение нового устройства к уже существующему комплексу планируется проводить по следующему алгоритму.

Шаг 1. Перед подключением киберфизическое устройство инициализируется – запускается особый режим операционной системы, который опрашивает каждую загруженную в устройство прикладную программу на предмет ожидаемых входов и выходов. Определим данный файл как дескриптор прикладной среды. В указанном файле для каждой программы должно быть указано, от программ с какими идентификаторами ожидаются данные и программам с какими идентификаторами данные будут передаваться.

Шаг 2. Операционная система запрашивает и получает адрес распределенного реестра (идеальный вариант – каждое устройство имеет свою копию распределенного реестра), в котором уже содержаться загруженные в него ранее дескрипторы киберфизических устройств, описывающие наборы прикладных программ. Дескриптор прикладной среды выгружается в формате отдельных записей, каждая из которых описывает отдельную прикладную программу.

Шаг 3. Каждое из киберфизических устройств на основании размещения дескриптора нового устройства принимает решение о переключении информационных потоков.

Необходимо отметить, что приведенные три шага не означают реализации управления информационными потоками на технологии распределенного реестра. Исходя из попыток, описанных, в частности, в [6], создание полноценного распределенного реестра с механизмами, ориентированными на обработку криптовалют нецелесообразно. Вместе с тем, возможно использование отдельных элементов, таких как связанное хранение данных, когда структура данных и алгоритмы контроля целостности не допускают изменения содержания данных и их последовательности и алгоритмы обеспечения консенсуса.

Можно предложить алгоритм, который обеспечивает информационную безопасность «роя» киберфизических устройств за счет:

– сведения вопросов информационной безопасности к вопросам безопасного взаимодействия и модификации набора

прикладного программного обеспечения, функционирующего в комплексе киберфизических устройств (аналога субъектно-объектной модели);

– вынесения описания прав и порядка взаимодействия прикладного программного обеспечения (аналога таблицы разграничения прав доступа) в распределенный реестр.

– администрирования распределенного реестра на основании алгоритма консенсуса (фактически децентрализованное администрирование и управление безопасностью).

Таким образом, обеспечение информационной безопасности набора киберфизических устройств, функционирующих в условиях отсутствия «защищенного периметра», является актуальной научной и практической задачей. Решение указанной задачи возможно наделением киберфизических устройств функциями формирования «интеллектуального роя», обладающего распределенными механизмами обеспечения информационной безопасности. Предложено реализовать указанные механизмы на уровне операционной систем, осуществляющей управление отдельным киберфизическим устройством.

Литература.

1. *Щербаков А.Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009 – 352 с.

2. *Колосок И.Н., Коркина Е.С.* Анализ кибербезопасности цифровой подстанции с позиций киберфизической системы // Информационные и математические технологии в науке и управлении. – 2019. – № 3 (15). – С. 121-131.

3. *Калинин М.О.* Способ осуществления правил политики безопасности в одноранговых коммуникационных сетях киберфизических устройств. Российский патент 2020 года по МПК H04L12/721 G06F21/60. RU2714217C1.

4. *Лаврова Д.С.* Методология предотвращения компьютерных атак на промышленные системы на основе адаптивного прогнозирования и саморегуляции. – Автореферат диссертации на соискание ученой степени доктора технических наук. – СПбТУ, 2019. – 37 с.

5. *Лаврова Д.С., Зегжда Д.П., Зайцева Е.А.* Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. – 2019. – № 2 (30). – С. 13-20.

6. *Афанасьев М. Я., Федосов Ю. В., Крылова А. А., Шорохов С. А.* Организация киберфизических производственных систем с использованием технологий блокчейн и смарт-контрактов // Известия высших учебных заведений. Приборостроение. – 2019. – Т. 62. № 3. – С. 226-234.

Изотова И.А., Мысак М.Ю., Фейзов В.Р.

Технология кибербразведки как инструмент выстраивания проактивной защиты

Аннотация: Работа посвящена актуальной на сегодняшний день проблеме низкого уровня осведомленности организаций о технологии кибербразведки и вопросам применения данных о киберугрозах при выстраивании системы обеспечения кибербезопасности. В работе проанализированы методы применения данных кибербразведки в целях повышения уровня защищенности организации путем выстраивания проактивной защиты. Вопросы, изучаемые в работе, заинтересуют руководителей служб информационной безопасности (ИБ), а также центров мониторинга и реагирования организаций кредитно-финансового сектора.

Ключевые слова: кибербразведка, данные о киберугрозах, кибербезопасность, повышение уровня защищенности, кредитно-финансовый сектор

Современный мир невозможно представить без информационных технологий, и финансовая сфера не стала исключением. Пандемия лишь ускорила процесс цифровизации в кредитно-финансовом секторе, что сместило приоритеты в сторону дистанционного обслуживания клиентов и организации удаленных рабочих мест для сотрудников. Это было бы невозможно без достижений в области информационных технологий, которые стали неотъемлемой частью финансовых услуг. Распространение сфер

применения цифровых сервисов влечет необходимость пересмотра и усиления мер обеспечения кибербезопасности.

Только по информации Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) в 2020 году через Автоматизированную систему обработки инцидентов ФинЦЕРТ от участников информационного обмена в процессе информирования о компьютерных атаках было получено 968 сообщений о фактах распространения вредоносного программного обеспечения (ВПО), содержавших 1300 образцов ВПО [1]. Большинство случаев – распространение различного ВПО с использованием электронной почты. Сравнение структуры исследованного объема ВПО с данными 2019 года позволяет выделять смещение векторов применяемого ВПО. Своевременное выявление и реагирование на большое количество сложных направленных атак невозможно без глубокого изучения особенностей атаки и принятия соответствующих превентивных защитных мер. Проблема низкой осведомленности об актуальных угрозах распространена как внутри отдельных компаний, так и внутри всей отрасли. Несмотря на общий высокий уровень защищенности организаций финансового сектора, обмен и применение данных о киберугрозах развивается медленнее остальных направлений кибербезопасности.

К финансовым организациям Банком России предъявляется ряд требований, включая требования к содержанию базового состава мер защиты информации в соответствии со стандартом ГОСТ Р 57580.1-2017 «Защита информации финансовых организаций» [2]. Одной из целей указанного нормативного документа является достижение адекватности состава и содержания мер защиты информации, применяемых финансовыми организациями, актуальным угрозам безопасности информации и уровню принятого финансовой организацией операционного риска (риск-аппетиту). В целях выполнения указанных требований организации вынуждены обратить особое внимание на применяемые процессы мониторинга и реагирования на компьютерные атаки.

Стоит отметить, что в процессе реагирования на кибератаки, организации часто сталкиваются с проблемой повышенной нагрузки на работников, вызванной разбором инцидентов, созданных на основании некачественных и несвоевременно

поступивших данных. Кроме того, приходится тратить много времени на поиск и обогащение данных из инцидента дополнительным контекстом. Все это приводит к увеличению времени реагирования и снижению качества разбора инцидентов, являющихся реальными угрозами, увеличению числа ошибок первого и второго рода при принятии решения об актуальности угрозы, увеличению наносимого ущерба или даже к нарушению требований и сроков оповещения внешних регуляторов. Применение технологии кибербразведки позволяет применять знания об угрозах в целях автоматизации мониторинга и выстраивания проактивной защиты от целенаправленных атак, что снижает нагрузку на работников центра мониторинга и реагирования, облегчает процесс разбора инцидентов и минимизирует возможный ущерб.

Существуют три основных типа данных кибербразведки: стратегические, тактические и операционные. Все они важны при построении кибербезопасности и их грамотное применение помогает минимизировать затраты на реализацию системы обеспечения кибербезопасности при повышении общего уровня защищенности. Стратегические данные включают информацию о текущих тенденциях, целях и мотивации злоумышленников. Потребителями данной информации чаще являются руководство и топ-менеджмент организации. Тактические включают более подробную информацию о конкретных готовящихся или проводимых атаках, техники, тактики и процедуры атакующих. Потребителями тактических данных чаще являются Руководители служб ИБ, центров мониторинга и реагирования, работники ИТ-подразделений. Операционные включают в себя индикаторы компрометации и индикаторы конкретных атак. Потребителями такой информации являются работники центра мониторинга и реагирования.

Примерами собираемых данных кибербразведки служит следующая информация: индикаторы, включая хэш-суммы вредоносных файлов, IP адреса, домены, URL-адреса, артефакты, правила, инструменты, данные утечек, информация о злоумышленниках из новостей, отчетов и других доступных источников. Источниками получения данных могут являться:

- бюллетени внешних регуляторов;

- открытые сообщества обмена данными об угрозах;
- коммерческие потоки данных об угрозах;
- интернет, включая социальные сети;
- СМИ;
- внутренний трафик;
- собственные средства защиты информации;
- результаты разбора внутренних инцидентов.

Важно, чтобы данные о киберугрозах, поступающие от внешних источников, были актуальные, своевременные, точные и, желательно, обогащенные контекстом. При выборе источников стоит руководствоваться репутацией поставщика, анализировать его возможности по своевременному сбору и поддержанию актуальности данных кибербразведки, релевантности предоставляемых им данных к конкретной инфраструктуре и не стоит гнаться за количеством подключаемых источников и собранных данных. Хранение данных кибербразведки лучше реализовывать совместно с соответствующими контекстными данными. Данные, которые записываются об угрозах, в основном можно разделить на пять групп.

1. Информация об индикаторе:
   - тип;
   - значение;
   - дата добавления;
   - дата последнего обновления;
   - вес.
2. Счетчик срабатываний:
   - количество подтвержденных выявлений в инфраструктуре;
   - количество ложных срабатываний;
   - даты первого и последнего срабатывания.
3. Данные источника:
   - название источника;
   - название поставщика;
   - тип;
   - достоверность;
   - дата добавления;

– дата последнего обновления.

4. Контекст угрозы:

– название;

– категория;

– уровень критичности;

– даты первого и последнего упоминания об угрозе.

5. Дополнительная информация.

Отдельной сложной математической задачей является скоринг данных кибербразведки, зависящий от множества меняющихся во времени параметров, относящихся как к самой информации, так и к источнику, контексту угрозы: дата получения данных, достоверность источника, дата последнего обновления данных от источника, рейтинг, релевантность угрозы и т.д. Например, параметры индикаторов, являющихся хэш-суммой вредоносного файла (значение хэш-суммы файла со временем не изменяется), будут с течением времени изменяться иначе, нежели IP-адреса контрольно-командных серверов, которые злоумышленники склонны менять.

Для эффективного выстраивания проактивной защиты процесс кибербразведки необходимо имплементировать в действующие процессы обеспечения кибербезопасности, такие как управление уязвимостями, поиск угроз, мониторинг и реагирования на инциденты. Без должного уровня зрелости в организации перечисленных процессов внедрение технологии кибербразведки может быть неоправданным и не принести должного положительного эффекта.

В свою очередь, процесс кибербразведки является композицией следующих основных этапов [3]:

- этап планирования, включающий определение целей и требований к собираемым данным об угрозах;
- этап сбора актуальных данных, удовлетворяющих целям и требованиям, структурирования и нормализации данных;
- этап обработки, включая унификацию;
- этап подготовки данных;
- этап распространения.

После разбора составляющих процесса кибербразведки встает вопрос о механизмах автоматизации обработки данных об угрозах.

Неспециализированные инструменты обмена данными об угрозах, такие как электронные таблицы, почта и др. не могут обеспечить требуемого уровня гибкости. Threat Intelligence Platform (TIP) или платформа кибербразведки позволяет собирать, нормализовать, коррелировать и анализировать данные об угрозах, полученные из различных источников. В статьях [4,5] выполнен сравнительный анализ основных платформ обмена данными о киберугрозах. При выборе платформы необходимо руководствоваться требованиями и потребностями конкретной организации. В случае наличия большого числа потребностей, не закрывающихся продуктами, представленными на рынке, стоит рассмотреть возможность разработки собственной платформы кибербразведки.

Внедрение платформы кибербразведки даст следующие основные преимущества:

- обеспечение единой точки управления данными кибербразведки всех типов;
- использование данных об угрозах в процессе мониторинга;
- повышение эффективности работы средств защиты за счет предоставления актуальных данных;
- обогащение контекстом, ведущее к облегчению принятия решения относительно реакции на угрозу или потенциальную угрозу;
- раннее выявление подозрительной сетевой и хостовой активности.

Таким образам, знания об актуальных угрозах, методах и инструментах злоумышленников позволяют выстраивать систему обеспечения кибербезопасности с учетом оценки релевантности угроз для конкретной отрасли и региона, приоритизировать риски и выстроить проактивную защиту от актуальных угроз. Выявление кибератак на ранних стадиях поможет значительно снизить, а то и вовсе предотвратить нанесение ущерба организации.

Литература:

1. Банк России. Основные типы компьютерных атак в кредитно-финансовом секторе в 2019-2020 годах. – URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения 10.10.2021).

2. Стандарт Банка России ГОСТ Р 57580.1-2017 «Защита информации финансовых организаций». – URL: https://docs.cntd.ru/document/1200146534 (дата обращения 11.10.2021).

3. *Туманов Д., Абрамов Е.* Разработка системы анализа и верификации индикаторов компрометации (IoC) / Материалы 12-й Международной научной конференции «Безопасность информации и компьютерных сетей» (SIN 2019). – Сочи: Сочинский государственный университет, 2019. – С. 54-57.

4. Краткий анализ рынка Threat Intelligence Platforms . – URL: http://www.volgablob.ru/blog/?p=1842 (дата обращения 08.10.2021).

5. *Вульфин А.* Система управления данными киберразведки // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. №(1). – С. 1-18.

Фейзов В.Р.

Цветные революции и безопасность коммуникаций и данных в условиях существования современных олигополий

Аннотация: Интенсивный процесс перехода человечества к цифровому обществу позволил реализовать множество возможностей, одновременно с положительным эффектом возникли как новые этические вопросы, так и угрозы политического характера. В работе рассматриваются некоторые аспекты потенциально возможного деструктивного воздействия транснациональных корпораций на граждан и политическую систему отдельных стран. Рассмотренные в работе вопросы могут заинтересовать специалистов по защите информации и информационной безопасности.

Ключевые слова: цветные революции, безопасность данных, средства массовой информации, социальные сети, рекомендательные системы

В настоящее время проводится большое количество исследований посвященных анализу проблем, связанных с демонтажом политических режимов в современных государствах и ролью в этом процессе технологий цветных революций. Еще не так

давно инструментами подобного демонтажа выступали в основном вооруженные перевороты, локальные вооруженные конфликты, гражданские войны и т.п. В настоящее время на смену технологиям вооруженных переворотов приходят более тонкие технологии цветных революций, которые умело маскируются под истинные общественные движения и ориентированы на извлечение и использование больших данных, а также на широкое применение современных информационных технологий.

Джин Шарп – американский ученый, идеолог цветных революций, посвятивший свою жизнь изучению вопросов связанных со сменой политических режимов при помощи методов ненасильственной борьбы («мягкой силы»). Его идеи остаются актуальными и активно используются во многих странах при массовых протестах. Ненасильственные движения часто перетекают в открытые столкновения на улицах городов с реальными жертвами среди населения. Вот некоторые из известных прецедентов, которые начались с «мирных» протестов на улицах:

- бульдозерная революция (Югославия, 2000 г.);
- революция роз (Грузия, 2003 г.);
- оранжевая революция (Украина, 2004-2005 г.);
- тюльпановая революция (Киргизия, 2005 г.);
- финиковая революция (Тунис, 2010-2011 г.);
- бархатная революция (Армения, 2018 г.).

Наиболее известная работа автора – «От диктатуры к демократии» (1993) переведена более чем на 44 языка. Шесть из 198 предложенных методов ненасильственных действий относятся к взаимодействию с широкой аудиторией [1].

В своей работе Джин Шарп подчеркивал важность информационного воздействия на население участниками ненасильственного демократического движения, таким образом, важным вопросом становится выбор средств коммуникации между участниками сопротивления и различными социальными группами (как с целью пропаганды, так и для координации дальнейших действий). В годы, когда труды были опубликованы, широко использовались такие средства коммуникации как телефоны и средства массовой информации (СМИ) как газеты, радио, телевиденье. Благодаря развитию технологий многие средства коммуникации подверглись значительным изменениям. Основными

драйверами изменений являются процесс мировой глобализации и развитие информационно-коммуникационных технологий. Благодаря развитию, появилась возможность за считанные секунды распространить почти любые материалы по всему миру. Появление социальных сетей и мессенджеров позволило любому пользователю (агенту) опробовать себя в роли источника и дистрибьютера новостей, достаточно просто транслировать мысли и идеи на своих страницах, каналах, группах. Концепция распространения контента в социальных сетях отличается от СМИ. Контент в социальных сетях распространяется, в основном, через связи между агентами и рекомендательные системы. На данный момент известно несколько моделей [2], которыми можно описать распространения информации в социальных сетях:

- модель SIR (susceptible – infected – removed);
- модель Далея-Кендалла;
- клеточный автомат;
- марковская модель влияния.

97 миллионов пользователей социальной сети ВКонтакте, 2.7 миллиарда активный пользователей в месяц Facebook, 1.3 миллиарда аккаунтов Twitter, с каждым днем количество пользователей лишь растет, контроль этих сервисов и контента внутри сетей дает большие возможности корпорациям. К 2021 году половина населения планеты имеет как минимум один смартфон. Исследователи Strategy Analytics прогнозируют дальнейший рост на 19% до 2026 года (рисунок 1) [3]. Газеты, радио, и даже телевиденье постепенно пропадают или переходят на цифровые аналоги в сеть Интернет.

Социальные сети, мобильные устройства, браузеры, а также множество других устройств собирают информацию о своих пользователях абсолютно легальным способом. Пользователи сами дают разрешение на сбор, а иногда и передачу данных третьим лицам в момент подписания пользовательского соглашения. Данные, собранные таким образом, помогают корпорациям и разработчикам таких решений предоставлять более качественные услуги. Банковский скоринг, таргетированная реклама, рекомендательный контент – везде используются собранные о пользователях данные. [4] Существуют общие модели известных рекомендательных систем [5], но точные алгоритмы остаются

скрытыми, так как такая информация является коммерческой тайной корпораций.

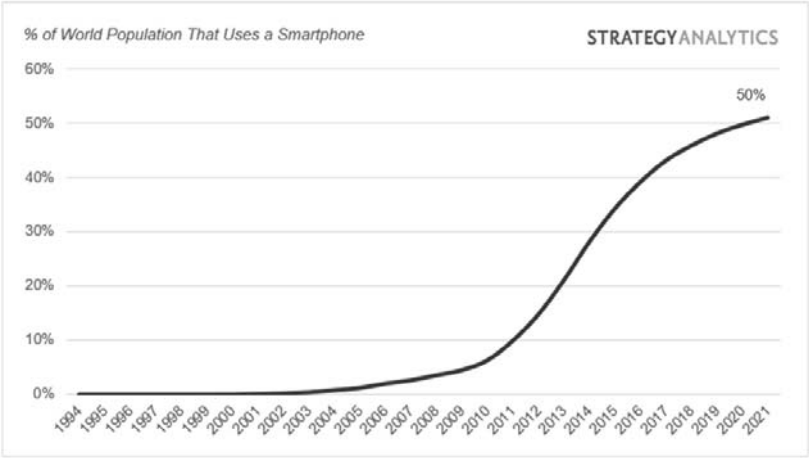


Рисунок 1 – Процент мирового населения, использующего смартфоны

Статистические модели (построенные на основе данных о больших социальных группах) вместе с управляемыми алгоритмами рекомендаций могут создать угрозу безопасности устойчивости государства в отдельно взятых регионах. Таким образом, контроль как сервисов, так и самих транснациональный корпораций государством является необходимым процессом. В первую очередь необходимо реализовать качественную систему защиты данных пользователей, прозрачность фильтров и рекомендаций контента, а также здоровую рыночную конкуренцию в технологической отрасли.

Репрезентативным примером политического вмешательства крупных транснациональных корпораций, является ситуация, которая сложилась с 45-ым президентом США Дональдом Трампом и его электоратом в 2021 году [6]. Аккаунты сторонников президента, самого президента и магазин его политической компании были заблокированы в большей части социальных сетей и сервисов. Facebook, Twitter, Reddit, Snapchat, Amazon (сервис

Twitch), Shopify, Google (сервис YouTube) заблокировали аккаунты связанные с Трампом в результате захвата Капитолия США. Apple и Google удалили из своих магазинов социальную сеть Parler, где общались сторонники президента, которые протестовали против фальсификации выборов. Если рассматривать этот прецедент отдельно от протестов и столкновений, то можно отметить, что без каких-либо судебных решений компании могут своевольно блокировать как аккаунты действующего президента, так и большую часть политического движения.

Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011

Литература:

1. *Шарп Д.* От диктатуры к демократии. Концептуальные основы освобождения. – М.: Ультра. Культура, 2005. – 224 с.

2. *Горковенко Д.К.* Обзор моделей распространения информации в социальных сетях // Молодой ученый. – 2017. – № 8 (142). – С. 23-28.

3. Four Billion People Use a Smartphone. – URL: https://www.strategyanalytics.com/strategy-analytics/blogs/devices/smartphones/smart-phones/2021/06/24/four-billion-people-use-a-smartphone (дата обращения 10.10.2021).

4. *Фейзов В.Р.* Цифровой портрет человека в сети / Материалы XXVIII Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС-2020) (16 декабря 2020 г. Москва). – М: ИПУ РАН, 2020. – С. 147-151.

5. Анатомия рекомендательных систем. Часть первая. – URL: https://habr.com/ru/company/lanit/blog/420499 (дата обращения 11.10. 2021).

6. Blocked: how the internet turned on Donald Trump. – URL: https://www.theguardian.com/us-news/2021/jan/12/blocked-how-the-internet-turned-on-donald-trump (дата обращения 11.10.2021).

Бугайский К.А.

Определение успешности действий нарушителя в однородной среде

Аннотация: В работе представлена модель элемента информационной системы, позволяющая оценивать возможности реализации угроз нарушителем на основе расчета расхождения между текущими и эталонными параметрами.

Ключевые слова: доля восприимчивых элементов, вероятность единичного заражения, вероятность захвата элемента, вероятность продолжения атаки, модель элемента, оценка нарушителя

Построение современных ИС на основе облачных, туманных технологий и технологии «инфраструктура как код» приобретает все большую популярность. Решения Правительства РФ о создании государственной единой облачной платформы, позволяет рассматривать данные технологии как основное направление развития информационных систем (далее – ИС). Неизбежным следствием функционирования ИС на основе таких технологий является размывание границ ИС, что, в свою очередь, приводит к необходимости рассматривать любой отдельный элемент ИС как возможный источник угроз. В работе [1] предложена дискретная модель заражения ИС, дающая возможность оценить вероятность реализации угрозы (успешных действия нарушителя) в:

$$p_s = K_{ss}\frac{p_{SE}(s)p_{EI}(s)p_I(s)(1-L_2)}{1-L_1-L_2-L_3-L_4} \quad (1)$$

где:

– значения переменных L_1-L_4 определяются характеристиками средств защиты информации используемых в элементе ИС;

– K_{ss} – доля восприимчивых элементов;

– $p_{SE}(s)$ – вероятность единичного заражения;

– $p_{EI}(s)$ – вероятность того, что нарушитель захватит элемент;

– $p_I(s)$ – вероятность продолжения атаки на соседние элементы.

Далее будет рассмотрен один из возможных путей определения значений: K_{ss}, $p_{SE}(s)$, $p_{EI}(s)$ и $p_I(s)$ на основе модели элемента ИС.

Модель элемента ИС

Пусть дана ИС, состоящая из конечного множества элементов $E = \{e_1, \dots e_i, \dots e_n\}$, $i \in N = \{1, \dots, n\}$. Традиционно все элементы $e_i \in E$, $i \in N$ ИС описываются кортежем $e =< S, O, R >$, где: S – множество субъектов доступа, O – множество объектов доступа, R – множество прав доступа. В современных ИС в качестве множества субъектов доступа целесообразно рассматривать исполняемые файлы, работающие в пространстве данного пользователя элемента. Можно утверждать (см., например, [2]), что исполняемые файлы непосредственно являются носителями уязвимостей и реализуют ошибки при выполнении правил распределения доступа. Тогда элементы ИС можно описать кортежем: $e =< V, R, A >$, где: V – множество уязвимостей, A – множество исполняемых файлов приложений, которые осуществляют доступ и обработку данных по требованию субъекта, R – множество прав доступа файлов к данным. В каждый конкретный момент времени элемент ИС может быть описан перечнем исполняемых файлов (процессов) или набором состояний $e = \{s_1, \dots, s_i, \dots, s_n\}$, $i \in N = \{1, \dots, n\}$ представленных выборками V известных уязвимостей и R прав доступа. Тогда элемент ИС: $e = \{(v_1, r_1), \dots, (v_i, r_i), \dots, (v_n, r_n)\}$, $i \in N = \{1, \dots, n\}$.

Каждому v_i и r_i может быть поставлена в соответствие оценка по В-бальной шкале – v_i^g и r_i^g соответственно и сформированы функции распределения оценок $P^v(v^g)$ и $P^r(r^g)$. Тогда элемент ИС: $e = \{P^v(v^g), P^r(r^g)\}$. Как правило, v_i^g и r_i^g формируются на основе экспертных заключений, а кроме того, для разных элементов ИС размеры выборок V и R будут различаться, что даст смещение оценок возможности реализации угроз в ИС. Но для каждой выборки V и R можно определить наихудший вариант распределения оценок v_i^g и r_i^g – когда все сопутствующие угрозе оценки имеют максимальное значение, что, в свою очередь, даст эталонные функции (равномерного) распределения $Q^v(\max v^g)$ и $Q^r(\max r^g)$ для $P^v(v^g)$ и $P^r(r^g)$.

Реальное распределение оценок для каждого из β диапазонов B-бальной шкалы будет отличаться от наихудшего (эталонного) варианта. Положим, что чем больше отклонение распределения $P^v(v^g)$ и $P^r(r^g)$ от наихудшего (эталонного) варианта $Q^v(\max v^g)$ и $Q^r(\max r^g)$, тем меньше возможность реализации угроз нарушителем. В ходе исследования будем осуществлять расчет расхождения текущего и эталонного распределений D^* на основе расхождения Реньи и последующей нормализации для шкалы B от 1 до 3 (с учетом качественных оценок «низкий», «средний», «высокий»). Тогда элемент ИС $e = (D^v, D^r)$, где D^v – оценка различия между текущим распределением уязвимостей и наихудшим из возможных, а D^r – оценка различия между текущим распределением прав доступа и наихудшим из возможных.

Расчет D^r основан на функциях отображения $r = a(o)$ и $r = b(s)$, где r, s, o – элементы соответствующих множеств. Функции отображения b, a дают 1, если для данного объекта доступа применим данное право доступа или 0 в противном случае. Тогда получаем множества $E^A(a) = \{r \in R | \exists\, o \in O, r = a(o)\}$, $E^B(b) = \{r \in R | \exists s \in S, r = b(s)\}$, $E^A, E^B = \{0,1\}$. Поскольку E^A и E^B транзитивны относительно R, то можно построить шкалу оценки реализации прав доступа на основании распределения как числа объектов доступа, так и числа субъектов доступа. Учитывая, что число субъектов доступа меньше числа объектов, то будем рассчитывать оценку для каждого субъекта доступа по числу доступных ему прав доступа одновременно с нормированием результатов для диапазона значений шкалы от 1 до 10 по формуле: $\forall s_i \in S: p_i^r = \frac{(k_i - r_{min})(b-c)}{r_{max} - r_{min}} + c$, где: k_i – число прав доступа (элементов множества R) доступных для субъекта s_i, r_{min} – минимальное число элементов множества R ($r_{min} = 1$), r_{max} – максимальное число элементов множества R, b – максимальное значение шкалы ($b = 10$), c – минимальное значение шкалы ($c = 1$). Далее, с использованием расхождения Реньи и приведения к шкале $B = [1, 3]$, получаем значение D^r для элемента ИС.

В настоящее время, разработан алгоритм (подробнее см. [3]) по выборке оценок уязвимостей на основе баз данных MITRE.ORG (далее – MITRE) учитывающего взаимосвязи между сущностями: CAPEC, CWE, CVE. Алгоритм формирует список уязвимостей,

каждому элементу которого сопоставлен вектор из (как минимум) трех экспертных оценок CVE: $L_i^v = \{v_1, \dots, v_i, \dots v_n\}$, $v_i = (v^b, v^e, v^c)$, $i \in N$, где: v^b – базовая оценка CVE, v^e – оценка эксплуатируемости, v^c – оценка влияния на конфиденциальность, целостность и доступность. Расчет D^v предлагается проводить по выборке базовых оценок уязвимостей v^b (как текущего распределения $P^v(v^g)$).

Если учесть, что коэффициенты D^v и D^r рассчитываются единообразно, то тогда можно рассматривать пространство $\Phi = D^v \times D^r$ как пространство состояний элементов ИС. В этом случае любое изменение состава ПО элементов ИС или правил доступа будет приводить к изменению координат точек пространства. Расчет центроида множества по точкам пространства даст интегральную оценку ИС с точки зрения возможности реализации угроз.

Введем метрику $\rho(x, y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$ и определим особые точки $x^0 = (3, 3)$ и $y^0 = (0, 0)$ на плоскости, что даст $\varphi_i = \frac{p(x_i, y_i)}{p(x^0, y^0)}$. Величину $1 - \varphi$ можно рассматривать как вероятность того, что данный элемент ИС $e = (D^v, D^r)$ будет использован нарушителем для реализации угроз при заданных распределениях уязвимостей и прав доступа, тогда $p_{SE}(s) = 1 - \varphi$.

Потенциал нарушителя как правило включает в себя возможности по эксплуатации существующих уязвимостей и возможные последствия при их успешной эксплуатации для элементов ИС. С этой точки зрения MITRE – кроме D^v и D^r – позволяет рассчитать оценки: сложности эксплуатации уязвимостей – D^e и их влияния на конфиденциальность, целостность и доступность – D^c. Таким образом, оценки D^* дают полное описание потенциала нарушителя. Пусть имеем множество оценок D, его среднее значение μ^d и среднее квадратичное отклонение σ^d. Определим границы разбиения на подмножества: $y^{min} = infD + \sigma^d$ и $y^{max} = supD - \sigma^d$. Произведем разбиение множества: $d_i \in D^{min}\ \forall d_i: infD \le d_i \le y^{min}$, $d_i \in D^{aver}\ \forall d_i: y^{min} < d_i < y^{max}$, $d_i \in D^{max}\ \forall d_i: y^{max} \le d_i \le supD$. Введем отношения $\frac{|D^{min}|}{|D|}$, $\frac{|D^{aver}|}{|D|}$, $\frac{|D^{max}|}{|D|}$. Тогда для различных оценок D^*получим интегральные

оценки потенциала нарушителя: I^e_{min}, I^e_{aver}, I^e_{max} – на основании оценок эксплуатируемости уязвимостей; I^c_{min}, I^c_{aver}, I^c_{max} – на основании оценок влияния уязвимостей на конфиденциальность, целостность и доступность; I^r_{min}, I^r_{aver}, I^r_{max} – возможности реализации угроз на основании оценок распределения прав доступа.

Тогда *потенциал нарушителя*, как вероятность того, что он захватит элемент ИС: $p_{EI}(s) = (1 - I^e_{min}),\ (1 - I^c_{min}),\ (1 - I^r_{min})$. Соответственно *доля восприимчивых элементов* $K_{ss} = I^e_{max} + I^e_{aver}$.

Полагаем, что вероятность продолжения атаки на соседние элементы $p_I(s)$ тем выше, чем больше сходство элементов ИС. Сходство элементов целесообразно проводить по критерию различия составов слабостей (CWE) и пользователей. MITRE дает возможность получить лексикографически упорядоченный список CWE для отдельного элемента ИС $L^w = \{w_1, \dots, w_i, \dots w_n\},\ i \in N$. Строится лексикографически упорядоченный список $L^u = \{s_1, \dots, s_i, \dots s_n\},\ i \in N$ пользователей для отдельного элемента ИС. Тогда вероятность продолжения атаки рассчитывается [4] по формуле: $p_I(s) = \sqrt{\left(1 - \frac{c}{a}\right)\left(1 - \frac{c}{b}\right)}$, где: a – число L^w или L^u одного элемента, b – число L^w или L^u другого элемента, c – число L^w или L^u общих для сравниваемых элементов.

Представляет интерес проведение исследований по оценке состояния ИС, то есть траекториям движения ее элементов в трехмерном пространстве $\Phi = D^c \times D^e \times D^r$ при различных условиях эксплуатации и различных вариантах атак. Это позволит определять численные значения функции распределения риска необходимую для механизмов анализа и управления рисками в различных ИС предложенных и исследованных в [5,6] с учетом конкретных параметров и условий функционирования ИС.

Заключение

В работе рассмотрена задача расчета исходных данных для оценки вероятности реализации угрозы (успешных действия нарушителя) в дискретной модели заражения ИС. Разработанная модель элемента ИС, позволяет в условиях неопределенности, присущей процессам формирования и оценке угроз и нарушителя в ИС, проводить расчеты доли восприимчивых элементов, вероятности единичного заражения, вероятности захвата элемента

нарушителем, вероятности продолжения атаки на соседние элементы. Также модель позволяет рассматривать вопросы защиты информации ИС в пространстве состояний ее элементов с учетом динамики изменений состава элементов ИС и правил доступа.

Показана возможность применения результатов для оценки рисков, реализации угроз, потенциала нарушителя, а также для определения актуальных угроз безопасности информации.

Литература:

1. *Остапенко А.Г., Радько Н.М., Калашников А.О. Остапенко О.А., Бабаджанов Р.К.* Эпидемии в телекоммуникационных сетях. – М: Горячая линия – Телеком, 2018. – С. 123-149 .

2. Банк данных угроз безопасности информации. Термины // FSTEC.RU: ФСТЭК России. – URL: https://bdu.fstec.ru (дата обращения 27.09.2021).

3. *Калашников А.О., Бугайский К.А.* Методика оценки возможности реализации информационных угроз // Информация и безопасность. – 2020. – Т. 23. № 2(4). – С. 163-178.

4. *Костина Н.В.* Применение индексов сходства и различия для районирования территорий на основе локальных флор // Известия Самарского научного центра Российской академии наук. – 2013. – Т.15. № 3 (7). – С. 2160-2168.

5. *Калашников А.О.* Модели и методы организационного управления информационными рисками корпораций. – М.: Эгвес, 2011. – 311 с.

6. *Новиков Д.А., Остапенко А.Г., Калашников А.О., Остапенко Д.Г., Соколова Е.С., Уразов М.Ю.* Информационные риски и эпистойкость безмасштабных сетей // Информация и безопасность. – 2015. – Том 18. № 1. – С. 5-18.

Муромцев В.В., Муромцева А.В.

Цифровизация – угрозы и риски

Аннотация: Рассматриваются процессы, происходящие в современном информационном пространстве, которые в условиях глобализации цифровых информационных потоков ставят перед современным обществом целый ряд серьезных проблем и прежде всего в сфере безопасности.

Ключевые слова: цифровизация, технология Веб 2.0, глобализированное информационное сообщество, виртуальное пространство, психоинформационная безопасность

В Доктрине информационной безопасности РФ в разделе «Стратегические цели и основные направления обеспечения информационной безопасности» отмечено, что одним из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности являются: «обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности».

Наверное, это важнейший тезис в области психоинформационной безопасности населения потому, что касается каждого человека, всего общества особенно в период реализации процесса цифровизации.

Цифровизация – это процесс, о котором сегодня не говорит только ленивый. Предполагается, что он замечательным образом преобразует к лучшему все вокруг, включая производственную и социальную сферы. Однако необходимо понять, насколько безоблачно будущее.

Прежде всего, настораживает та настойчивость и безаппеляционность, с которой формируется цифровое общество и агрессивность действий, с которой реализуется этот процесс, а если обратиться к уже реальному опыту Китая, то возникают определенные сомнения в полезности этих преобразований.

Отметим также, что формирование цифрового общества реализуется в соответствии с определенными решениями давосского клуба и в рамках концепции «Индустрия 4.0», которая была сформулирована в 2011 г. президентом Всемирного экономического форума в Давосе Клаусом Швабом.

Отметим, что информатизация представляла собой процесс создания и добровольного использования информационной инфраструктуры, поддерживающий формирование информационного общества.

Цифровизация – это процесс, поддерживающий становление цифрового общества, в рамках которого реализуется

принудительное использование, созданной информационной инфраструктуры. Такое положение заставляет обратить особое внимание на обеспечение защищенности граждан от информационных угроз.

Без знания цифровых технологий, т.е. без определенной информационной культуры, существование человека в цифровом обществе станет невозможным или весьма некомфортным. Процессы, происходящие в современном информационном пространстве, определяют сегодня тенденции изменения всей мировой информационной культуры.

Глобализация информационных потоков, ставшая следствием тотальной цифровизации информации, ставит перед современным обществом целый ряд серьезных проблем и прежде всего в сфере безопасности.

Переход компьютерных коммуникаций на технологии Веб 2.0 изменил всю технологию коммуникаций в рамках Сети. На первом этапе функционирования Глобальной Сети пользователю предоставлялась возможность только «чтения и редактирования» информации в сети Интернет. Главной особенностью технологий Веб 2.0 стали программные решения, обеспечивающие ничем не ограниченный личностный обмен информацией при формировании глобального информационного пространства. Технологии SST (Social Software Technologies), предоставляют каждому пользователю Сети постоянную возможность ничем не ограниченного участия в создании информационного сообщения, его распространения (обнародования), изменения и продвижения (навязывания). Возникшие в результате появления Веб 2.0 простые возможности самореализации в результате действия эффекта «больших данных» (‘big data’) оказались способны изменить всю информационную структуру общества и потребовали существенной трансформации всех способов управления информационными потоками в социуме [1]. Сегодня на первый план выходит изучение и понимание того, как формируются и развиваются информационные системы, которые состоят из комбинации технических и социальных компонентов – «социотехнические системы». Таким образом, при создании любых технических решений и программных разработок социальные аспекты необходимо рассматривать и учитывать наряду с техническими. В

противном случае исключительно технократически ориентированные концепции делают технические решения не только неэффективными, неточными, но иногда и опасно ошибочными, если они встраиваются в социальный контекст, окружающий системы принятия решений.

Знание теории и практики функционирования социотехнических систем приобретает в современном обществе, которое вступило в эпоху т.н. «пост-цифрового вызова» (postdigital challenge), особую актуальность. Необходимо фундаментальное понимание того, как люди на самом деле работают и живут в группах, организациях, сообществах и других формах коллективной жизни, реализуемых в цифровом информационном пространстве [2]. Без теоретического осмысления этой проблемы и выработки практических рекомендаций по формированию сбалансированной эффективной политики управления современным глобализированным информационным сообществом мы обречены на обострение внутренних противоречий между разными общественными слоями и группами, которые будут усугублять цифровое информационное неравенство (digital divide) всех видов [3]. И здесь полезно обратиться к истории возникновения технологии цифрового социального взаимодействия, которая получила название Веб 2.0. Сегодня можно утверждать, что многие исходные теоретические предположения о социальных последствиях перехода современного информационного общества на этап Веб 2.0 реализовались в той или иной мере и превратились в настоящие вызовы для безопасного функционирования человеческого сообщества. Так, стало очевидным, что социальные сетевые взаимодействия участников коммуникации активно способствуют формированию новых ментальных и поведенческих стереотипов, а также беспрецедентно быстрому их распространению с охватом многомиллионной аудитории. В последнее время и теоретики, и практики информационных технологий все чаще говорят об опасности проявления в социальных сетях феномена группового «коллективного разума» (‘collective intelligence’), проявляющегося через т.н. эффект «мудрой толпы» (‘wisdom of crowd’). Этот эффект основан на презумпции истинности коллективного мнения в противовес мнению индивидуальному, что ведет к распространению и усиленному

навязыванию мнения некоторой референтной группы как единственного источника правильного знания. Можно заметить, что сегодня этот феномен повсеместно активно вторгается в сферу управления информационными потоками, способствуя тем самым плохо контролируемой трансформации информационного состояния общества в целом. В то же время хорошо известно, что реализация информационных связей по сценарной модели «мудрость толпы» приводит к тому, что большинство веб-ссылок в Интернете (семантических связей) формируется не на основе профессиональных знаний, а по принципу «овечьей тропы в горах», т.е. путей, которые «сформировались с течением времени, когда многие животные и люди просто случайно воспользовались ими» [4].

Одним из главных уроков новой информационной революции, начатой с появлением Веб 2.0, как отмечает O'Reilly, стало также то, что «сетевой эффект от личного вклада каждого пользователя становится ключом к доминированию на рынке в эпоху Веб 2.0» [1]. Личный вклад пользователя таким образом превращает самого пользователя в своеобразное «средство массовой информации», что, как показывает клинический опыт, имеет серьезные психологические последствия для личности, действия которой начинают определяться принципом «быть замеченным – это все» ("getting noticed is everything") [5].

Еще одним серьезным психологическим следствием всеобъемлющего вмешательства в жизнь каждого индивида технологий Веб 2.0 стало явление, отмеченное психологами очень рано, – когнитивная перегрузка современного человека, которая привела к изменению самой формы восприятия информационного потока, в котором он вынужден существовать, – наиболее часто в этой связи упоминается «клиповое мышление», управляющее всеми когнитивными процессами у т.н. поколения Z. Это явление признано особенно опасным в образовательной сфере, поскольку провоцирует серьезные изменения когнитивных способностей, проявляющиеся в нарушении концентрации внимания, ухудшении процесса запоминания информации, трудности ее анализа и рефлексии [6].

Таким образом, результаты глобальной сетевой социализации информационных процессов оказались довольно противоречивыми.

С одной стороны, масштабное вовлечение широких слоев населения в креативную информационную активность способствует обогащению и расширению глобального информационного пространства (примером может служить несомненный успех многих проектов, реализованных с использованием Вики-технологий), однако оборотной стороной информационной сетевой активности стало сегодня то, что в условиях нарождающегося цифрового общества недопонимание, искажения информации, подмена понятий, ложная интерпретация приводят к весьма печальным последствиям в социальной сфере.

В настоящее время разработаны и активно применяются различные технологии информационного управления. Информационное воздействие на объект управления, с целью формирования заданного поведения, возможно сегодня как под контролем объекта управления, так и без его контроля, непосредственно на его подсознание [7]. Использование технологий информационного управления в социотехнических системах является еще одной угрозой информационной безопасности граждан.

Следует отметить, что процессы в глобальном информационном пространстве во многом не являются спонтанными. Они реализуются, во многом целенаправленно, в соответствии с указаниями Давосского клуба и западного цифрового лобби, основной задачей которых является достижение цифрового доминирования и осуществление глобального информационного управления.

Цифровизация привела к возрастанию влияния действий в виртуальном пространстве на события в реальной жизни, причем не только в сфере социально-психологической, но и технической и технологической. В социальной сфере потоки ложной, неадекватной и откровенно враждебной информации приносят обществу большой вред. Кроме формирования негативных настроений, это отрицательно влияет на формирование понятийной базы общественных и специальных коммуникаций.

Еще одно явление характерное для современного информационного пространства это cancel culture — современная форма судов инквизиции, при которой человек или определенная группа лишаются поддержки и подвергаются осуждению в

социальных или профессиональных сообществах, как в онлайн-среде и в социальных медиа, так и в реальном мире.

Несомненную и весьма существенную опасность представляет практика цифровой диктатуры, которая реализуется не только в рамках коммуникации, но и путем ее ликвидации. Цифровые монополисты позволяют себе удалять из сети аккаунты по своему желанию, практически бесконтрольно. Это прямой путь к цифровой диктатуре, ее реализации во всех формах. Осуществление цифрового давления на социум во всех его проявлениях представляет собой новый этап в формировании современного информационного пространства, в котором сочетаются формы психоинформационного давления с психологией толпы и прямым технологическим терроризмом. Сегодня в условиях нарождающегося цифрового общества недопонимание, искажения информации, подмена понятий, ложная интерпретация и, наконец, цифровая диктатура могут привести к весьма печальным последствиям.

Таким образом, тезис Доктрины «обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности» требует выполнения не только за счет усилий государства, но и общество в целом должно знать и быть готовым парировать возникающие информационные угрозы.

Литература:

1. *O'Reilly T.* What is Web 2.0. Design patterns and business models for the next generation of software by Tim O'Reilly 09/30/2005. – URL: https://www.oreilly.com/pub/a/web2/archive/what-is-web20.html (дата обращения 11.04.2021).

2. *Ackerman M.S.* The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility // Human–Computer Interaction. – 2000. – Volume 15. Issue 2-3. – P. 179-203

3. *Eubanks V.* Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. – New York: St Martin's Press, 2017. – 272 p.

4. *Surowiecki J.* The wisdom of crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies,

societies and nations. – New York: Random House, Doubleday Books, 2004. – 336 p.

5. *Andersen P.* What is Web 2.0?: ideas, technologies and implications for education. – Bristol: JISC, 2007. – Vol. 1. – P. 1-64.

6. *Гурьянов Н.Ю., Коротаева Т.В.* Девиации когнитивных способностей человека под воздействием информационных технологий // Вестник МГОУ. Серия: Философские науки. – 2021. – №1. – С. 111-118.

7. *Муромцев В.В., Немцова С.Р.* Проблемы психоинформационной безопасности в современном информационном пространстве // Информационные войны. – 2014. – №2. – С. 73-80.

IV. Кибербезопасность. Особенности обеспечения безопасности в социальных сетях

Промыслов В.Г., Семенков К.В.

Управление риском кибербезопасности на этапе проектирования для промышленных систем

Аннотация: В работе рассматривается процедура оценки риска кибербезопасности для этапа разработки в промышленных системах. Предлагается двухэтапная процедура. Первый этап включает общую для системы оценку риска, не использующую детальных данных о системе, что позволяет преодолеть неопределенность входных данных на начальном этапе жизненного цикла. Второй (опциональный) этап включает детальную оценку риска, что позволяет учитывать особенности архитектуры системы и специфичную для системы модель угроз.

Ключевые слова: кибербезопасность, оценка риска, разработка, неопределенность данных

Нет простого рецепта, как обезопасить промышленную систему управления (АСУ ТП) от киберугроз. Однако, есть общее понимание, что работа по обеспечению кибербезопасности, должна начинаться на самых ранних этапах жизненного цикла системы, начиная с первых шагов по ее разработке [1]. Этап разработки характеризуется неопределенностью в понимании деталей реализации системы и частично – в требованиях, предъявляемых к системе. Этап разработки может быть не самым значительным по времени, но является одним из важных этапов, когда закладываются основные технически решения по обеспечению информационной безопасности.

В ситуации, когда нет четко сформулированных моделей явлений или есть неопределенность во входных данных, часто применяют риск-ориентированные подходы. Поэтому обеспечение

кибербезопасности промышленных систем во многом связано с управлением риском. С каждой АСУ ТП у организации связаны разные риски, которые зависят как от внешнего контекста (месторасположение, специфические для отрасли угрозы и вероятности реализации угроз в смысле как она понимается в оценке риска [2]), так и внутреннего контекста (присущие конкретной системе: уязвимости, влияние последствия кибератаки на объект управления и пр.).

В данной работе рассматривается двухэтапный подход к оценке риска кибербезопасности для промышленных критически важных объектов (КВО).

Процедура оценки риска на этапе разработки делится на два этапа. Целью первоначальной оценки рисков кибербезопасности для системы, свойства которой известны только в самом общем виде, является получение базовой оценки риска.

Риск в этом случае обычно оценивается с точки зрения воздействия инцидента кибербезопасности на здоровье, безопасность, окружающую среду, или нарушение производственной деятельности.

Эта оценка помогает установить приоритеты детальной оценки рисков и облегчает разработку архитектуры безопасности КВО, например, в части деления на зоны безопасности или классификации активов. Существенным с точки обеспечения и анализа кибербезопасности системы является то, что система управления обычно строится по иерархическому принципу. Иерархия заложена и в архитектуру системы (наличие подсистем), и в архитектуру кибербезопасности (уровни и зоны кибербезопасности). Для обеспечения эффективной защиты и минимизации набора применяемых мер активы группируют по уровням кибербезопасности. Этот процесс неотделим от задачи категоризации/классификации активов. Объединение активов на уровне архитектуры системы приводит к появлению комплексных активов, которые принадлежат к другому уровню иерархии системы управления.

Процесс управления кибербезопасностью АСУ ТП КВО на первом этапе можно представить в виде последовательности следующих шагов:

– разработчик совместно с собственником КВО, в рамках общей программы информационной безопасности, определяет внешний и внутренний контекст оценки риска [3]. Внешний контекст включает всю доступную информацию об окружении КВО на данный момент, требования регуляторов или применяемых стандартов. Внутренний контекст составляют требования высших политик безопасности, которые действуют в организации-разработчике, известная на данный момент спецификация системы. Принимается неизменный набор мер безопасности, определяемый требованиями регулятора, используемых стандартов или политик безопасности верхнего уровня. Обязательным элементом внутреннего контекста должно стать информация о допустимом уровне риска для организации;

– для анализа риска используются стандартные для данного типа объекта наборы угроз и уязвимостей, без учета деталей реализации системы [3];

– оценку первоначального риска можно выполнять с использованием матрицы рисков, которая устанавливает взаимосвязь между вероятностью, воздействием и риском [4];

– полученный риск сравнивается с допустимым для организации риском.

Если риск для организации приемлем, то оценка риска может быть завершена. По крайне мере, до момента, когда она будет требовать переоценки. Переоценка может быть частью периодической процедуры перерасчета риска по истечении времени, или в связи с завершением этапа разработки или получения новых данных, не учтенных на предыдущем шаге.

Если же риск неприемлем, то необходим детальный анализ риска с целью выявления «точек напряжения» в системе и применения мер защиты для снижения риска до допустимого уровня.

Второй этап оценки риска по структуре повторяет процессный подход первого этапа, однако имеет более детальный характер. К моменту завершения первого этапа оценки риска обычно уже известна архитектура системы, в частности, ее разбиение на подсистемы. Подсистемы определены, по крайней мере, с точностью до ее спецификации, часто известны детали реализации.

Оценка риска на втором этапе проводится для каждой из подсистем.

– Проводится описание внешнего и внутреннего контекстов. Внешний контекст включает список специфичных для подсистемы угроз. Внутренний контекст включает всю доступную информацию о подсистеме на данный момент. Должен быть определен набор уязвимостей для реализации подсистемы.

– Собственник идентифицирует цифровые активы в подсистеме, а также функциональность активов в части обработки, хранения, передачи информации в цифровой форме.

– С использованием информации о специфичных угрозах и уязвимостях формируются сценарии атак на активы подсистемы.

Применяя одну из методик оценки риска [4], получают оценку риска.

Полученные риски сравниваются с допустимым для организации риском.

Для рисков, превышающих допустимый уровень, выбирается одна из стратегий управления риском [3].

Применение двухэтапной процедуры оценки риска имеет несколько преимуществ. Первый этап можно провести еще на самых начальных стадиях разработки, на неполных данных о системе, сразу после появления спецификации системы. Такой подход позволяет избежать критических ошибок в формировании требований на систему, связанных с недооценкой или переоценкой требований по кибербезопасности. Разбиение на этапы в случае необходимости предусматривает детальную оценку риска, но, с другой стороны, позволяет уменьшить выполняемый объем работ, устранив детальную оценку риска для подсистем, если общий риск для системы не превышает допустимый уровень.

Литература:

1. *M. de la Cámara, F.J. Sáenz, J.A. Calvo-Manzano and M. Arcilla*. Security by design factors for developing and evaluating secure software / 10th Iberian Conference on Information Systems and Technologies (CISTI) (17-20 June 2015 Aveiro). – URL: https://ieeexplore.ieee.org/document/7170500 (дата обращения 10.10.2021).

2. IEC 62443-3-2. Security for industrial automation and control systems. Part 3-2: Security risk assessment for system design. – IEC, 2020. – 63 p.

3. ГОСТ Р ИСО/МЭК 27005. Менеджмент рисков информационной безопасности–2010. – Москва: Стандартинформ, 2011. – 48 с.

4. ГОСТ Р ИСО/МЭК 31010. Методы оценки риска–2011. – М.: Стандартинформ, 2012. – 70 с.

Асратян Р.Э.

Использование технологии SSL/TLS для создания защищенных сетевых каналов в распределенных системах

Аннотация: Рассмотрены принципы организации защищенного сетевого взаимодействия на основе использования технологии SSL/TLS для создания защищенных сетевых каналов через общедоступную сеть. В отличие от технологии VPN, описываемый подход предполагает подключение средств информационной защиты на верхнем («транспортном») уровне стека протоколов модели OSI, что позволяет более точно «сфокусироваться» на потребностях конкретного протокола приложения: HTTP/SOAP, т.е. на защите взаимодействий web-клиентов и web-сервисов.

Ключевые слова: распределенные системы, Интернет-технологии, информационная безопасность, SSL/TLS, web-сервисы, разграничение прав доступа

Многие современные распределенные информационные системы включают десятки и даже сотни рабочих станций и серверов, взаимодействующих через общедоступную глобальную сеть. Задача организации безопасных взаимодействий в таких системах уже давно вышла «на первый план» [1-2]. Обычный способ решения этой задачи заключается в использовании технологии VPN (Virtual Private Network), позволяющей реализовать защищенный «туннель» через общедоступную сеть [3]. Так как средства криптозащиты подключаются в VPN на нижнем уровне иерархии протоколов OSI (как правило, не выше

«сетевого»), эта технология отличается высокой универсальностью и способна обеспечить безопасное взаимодействие для любого из протоколов уровня «приложения» (HTTP, SMTP, POP3 и т.п.) [4].

Однако разработчики распределенных систем до сих пор сталкиваются с серьезными сложностями в области информационной безопасности. Это во многом связано с дефицитом готовых технических решений для таких задач, как разграничение прав доступа к информационным ресурсам, аутентификация информационных запросов и проверка подлинности серверов. Это приводит к появлению многих «частных решений» этих задач, приспособленных к особенностям конкретных проектов, что увеличивает трудозатраты и риск появления «брешей» в информационной защите.

В данной работе рассматривается новый подход к организации безопасных взаимодействий в распределенных системах, основанный на построении защищенных сетевых каналов с помощью технологии SSL/TLS [5]. В отличие от VPN, данный подход строго ориентирован на поддержку систем, опирающихся на технологию web-сервисов [6] для обслуживания информационных запросов. Подход основан на предположении, что технологии, более точно «сфокусированные» потребностях распределенных систем имеют больше возможностей в продвижении в сторону готовых технических решений, чем технологии, претендующие на универсальность.

Описываемый подход опирается на соединение двух сетевых технологий: SSL/TLS и технологии прокси-серверов. Структура защищенного канала проиллюстрирована на рисунке 1. Как видно из рисунка, канал включает две компоненты: клиентский шлюз и серверный шлюз.

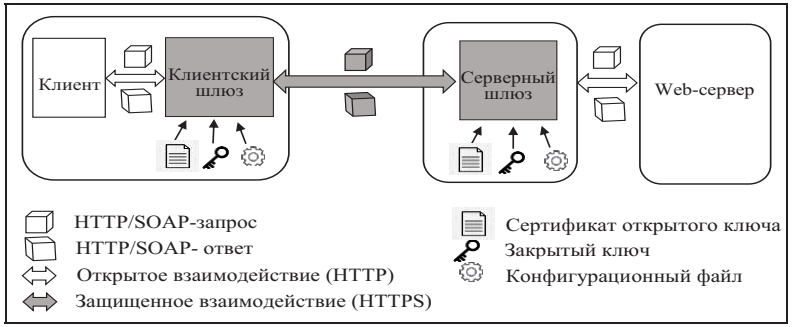


Рисунок 1 – Структура защищенного канала

Основное назначение клиентского шлюза заключается в решении следующих задач:

- «перехват» исходящих от клиента HTTP/SOAP-запросов в режиме прокси-сервера,
- анализ заголовков запросов,
- установка защищенного соединения с серверным шлюзом с применением технологии SSL/TLS и проверка подлинности серверного шлюза на основе сертификата открытого ключа,
- передача запроса серверному шлюзу и получение HTTP/SOAP-ответа по защищенному соединению,
- передача HTTP/SOAP-ответа клиенту.

Основное назначение серверного шлюза включает решение следующих задач:

- установление защищенного соединения с клиентским шлюзом по его запросу с применением технологии SSL/TLS,
- получение HTTP/SOAP-запроса от клиентского шлюза по защищенному соединению,
- 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 HTTP/SOAP-запроса,
- получение HTTP/SOAP-ответа от web-сервиса по открытому соединению и передача его клиентскому шлюзу по защищенному соединению.

Разграничение 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. Например, если в конфигурационном файле указано, что вызывать функцию MyFunction сервиса MyService имеют право только клиенты с реквизитами

C=Russia, L=Moscow, O=Titan, OU=dir*,

то доступ к этой функции будет разрешен только служащим московской организации Titan, сотрудником подразделения с названием, начинающимся на «dir» (directorate, direkciya и т.п.).

Описанный защищенный канал был реализован в среде операционной системы Linux на языке C++ с использованием библиотек поддержки SSL/TLS: libssl и libcrypt. И клиентский и серверный шлюзы приспособлены к работе в режиме фоновых программ («демонов»). Во время работы каждый из шлюзов занимает всего около 1 мегабайта оперативной памяти. Область наиболее эффективного применения канала включает распределенные системы, построенные на основе сетевой архитектуры ".NET" [7] в среде Linux (например, в интегрированной среде разработки MonoDevelop).

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 (20 января 2021 г. Пенза). – 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. *Baka P, Schatten J.* SSL/TLS under lock and key: a guide to understanding SSL/TLS cryptography. – Keyko books, 2020. – 132 p.

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.

Саломатин А.А.

Методы противодействия отслеживанию браузерных отпечатков пользователей

Аннотация: Рассматриваются методы противодействия отслеживанию браузерных отпечатков пользователей. Проанализированы различные группы мер, позволяющие препятствовать корректному отслеживанию браузерных атрибутов и изменять их значения таким образом, что сформированный отпечаток браузера не сможет верно идентифицировать пользователя. Приведены примеры способов осуществления мер в каждой группе. Отдельное внимание уделено оценке эффективности применения данных методов на сущности, полученные с помощью инструмента «fingerprint3.js». На основе проведенного исследования становится возможным осуществление практического эксперимента по идентификации пользователя с учетом применения методов, препятствующих получению полного и верного идентификатора пользователя. Развитие методов противодействия отслеживания браузерных отпечатков особенно важно для сложных систем, обслуживающих большое количество субъектов доступа.

Ключевые слова: кибербезопасность, браузерный отпечаток, идентификатор, информационная безопасность, браузерные атрибуты

В эпоху информационных технологий все большее внимание приобретает проблема кибербезопасности. Пользователи интернет-сетей, не только обычные люди, но и критически важные государственные инфраструктуры, подвергают себя рискам потери конфиденциальности, связанной с тем, что большинство веб-серверов в наше время собирает информацию о пользователях, которые с ними взаимодействуют. В таком случае, несмотря на положительный аспект, связанный с тем, что обеспечивается безопасность самого веб-сервера, безопасность посетителей ставится под угрозу.

Нередко собираемая информация о пользователях преподносится в виде их цифрового следа, который представляет собой набор данных о статических и динамических поведенческих признаках пользователя в сети [1,2]. Более того, получение цифрового следа не всегда требует длительного периода времени. Такая ситуация происходит, например, если формируется браузерный отпечаток пользователя, который содержит сведения о браузерных атрибутах пользователя (версии браузера, операционной системе, языке и т.д.) [3].

Снятие отпечатков браузера происходит в два этапа [4,5]. Первый этап – получение пользовательских данных о признаках по различным каналам (например, с помощью JavaScript или плагинов). Второй этап – объединение всех значений признаков в одну строку и затем вычисление идентификатора – цифрового следа пользователя.

Рассмотрим, какие существуют меры противодействия сбору информации, необходимой для выполнения этой цели, и проведем классификацию используемых методов по группам с примерами для каждой из групп:

1) *Блокировка доступа к данным пользователя*. Ее можно осуществить с помощью отключения JavaScript, который является основным механизмом получения атрибутов пользователя в наше время. Многие веб-сайты запрещают доступ, если браузер не поддерживает JavaScript [6]. Таким образом, остановка JavaScript может быть неприемлемой для значительной части пользователей

Другим вариантом является использование Do Not Track HTTP заголовка, который принимает значение, указывающее на предпочтение пользователя в отслеживании и отправляемое с сообщением запроса. Однако, и этот метод порой тяжело реализовать, потому что большинство серверов игнорируют такие запросы на запрет, либо теряют функциональность при отключении отслеживания.

2) *Создание идентичных признаков*. Подразумевается, что пользователи будут иметь одинаковые значения браузерных атрибутов, что затруднит различие пользователей между собой. В качестве примера можно привести Tor браузер, концепция которого заключается в изменении и ограничении многих атрибутов (например, списка шрифтов, списка плагинов, User-Agent и т.д.).

3) *Снижение уникальности идентификатора без надстроек.* Оно происходит за счет изменения числа некоторых атрибутов. Например, за счет уменьшения числа используемых плагинов или увеличения числа используемых браузеров.

4) *Снижение уникальности идентификатора с помощью надстроек.* С одной стороны, возможно скрывать значимые атрибуты, оказывающие наибольшее влияние на идентификацию пользователя. В данном случае, например, возможно применить Privaricator, который генерирует случайным образом значимые признаки (например, списки плагинов и шрифтов) с помощью добавления случайного шума в значения атрибутов. Другой пример – User Agent Switcher, который может управлять HTTP-заголовком User-Agent [7]. Изменение лишь значимых атрибутов не всегда может быть достаточно, поэтому более эффективным может быть использование надстроек, влияющих на получение и других признаков. Например, RubberGlove может находить объекты навигатора и экрана внутри веб-страницы, а затем заменять их значения на нулевые. Объект навигатора содержит информацию о названии и версии браузера, поддерживаемых типах MIME и плагинах, платформе, на которой был скомпилирован браузер, поддерживаемом языке и операционной системе, в которой браузер запущен. Объект экрана, в свою очередь, хранит информацию об экране пользователя, например, информацию о разрешении (высоте и ширине) экрана, а также глубины цветов. Имеются также расширения, блокирующие Canvas, которые ограничивает веб-

сайты от получения данных о canvas параметре пользователя, получаемого с помощью JavaScript.

Для того, чтобы лучше понять, как влияет применение мер противодействия на формирование браузерного отпечатка, предлагается обратиться к эксперименту, в котором будут вычислены браузерные атрибуты без применения надстроек и вместе с ними.

Для вычисления браузерных отпечатков пользователей можно задействовать уже готовые ресурсы. С одной стороны, возможно использование специализирующихся сайтов. С другой стороны, можно применить методы самостоятельно, при этом создав свой сервер. Такой подход можно осуществить с помощью библиотеки «fingerprint3.js». Ее преимуществом является частое обновление и оптимизация кода с целью увеличения числа получаемых браузерных атрибутов и улучшения параметров работы самой программы.

Было выявлено, что всего для полученных 32 атрибутов с помощью надстроек, примеров для группы мер под номером 4, является возможным изменение таких параметров, как userAgent, fonts, screenFrame, screenResolution, colorDepth, languages, osCpu, plugins, platform, canvas, cpuClass, contrast. Изменение других браузерных атрибутов также может иметь место, но зависит от используемой надстройки в эксперименте.

Таким образом, в ходе выполнения данного исследования были рассмотрены четыре группы методов противодействия идентификации пользователей на основе браузерных отпечатков. В каждой были приведены примеры с описанием функциональности конкретных методов. Создались условия для проведения будущего эксперимента по применению надстроек с целью скрытия подлинного отпечатка пользователя и спрогнозировать часть его результатов. Эксперимент может проводиться для любого пользователя, поэтому его результаты могут оказаться эффективны в задаче обеспечения конфиденциальности информации о пользователях в сложных системах.

Исследование выполнено при частичной финансовой поддержке гранта Президента Российской Федерации в рамках научного проекта МК-3172.2021.1.6

Литература:

1. *Агафонов Ю.М.* Деанонимизация пользователей на основе цифровых отпечатков браузера / Безопасность информационного пространства – 2017: XVI Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых (12 декабря 2017 г. Екатеринбург). – Екатеринбург: Изд-во Урал. ун-та, 2018. – С. 3-5.

2. *Feher K.* Digital Identity and The Online-Self: Footprint Strategies – An Exploratory and Comparative Research Study // Journal of Information Science. – 2021. – Volume 47. Issue 2. – P. 192-205.

3. *Nair K., RoseLalson E.* The Unique Id's You Can't Delete: Browser Fingerprints / International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR) (11-13 July 2018 Ernakulam, India). – Ernakulam, 2018. – P. 1-5. – URL: https://ieeexplore.ieee.org/document/8529040 (дата обращения 10.10.2021).

4. *Bujlow T., Carela-Español V., Solé-Pareta J. and Barlet-Ros P.* A Survey on Web Tracking: Mechanisms, Implications, and Defenses // Proceedings of the IEEE. – 2017. – Vol. 105. № 8. – P. 1476-1510.

5. *Luangmaneerote S., Zaluska E., Carr L.* Inhibiting Browser Fingerprinting and Tracking / IEEE 3rd International Conference on Big Data Security on Cloud (26-28 May 2017 Beijing, China). – Beijing, 2017. – P. 63-68. – URL: https://ieeexplore.ieee.org/document/7980318 (дата обращения 10.10.2021).

6. *ElBanna A., Abdelbaki N.* Browsers Fingerprinting Motives, Methods, and Countermeasures / International Conference on Computer, Information and Telecommunication Systems (CITS) (11-13 July 2018 Alsace, Colmar, France). – Colmar, 2018. – P. 1-5. – URL: https://ieeexplore.ieee.org/document/8440163 (дата обращения 10.10.2021).

7. *Fiore U., Castiglione A., De Santis A. and Palmieri F.* Countering Browser Fingerprinting Techniques: Constructing a Fake Profile with Google Chrome / 17th International Conference on Network-Based Information Systems (NBiS 2014) (10-12 September Salerno, Italy). – Salerno, 2014. – P. 355-360. – URL: https://ieeexplore.ieee.org/document/7023976 (дата обращения 10.10.2021).

Смирнов А.М., Исхаков А.Ю.

Алгоритм двухфакторной аутентификации как инструмент снижения FRR для проактивного фильтра выявления атак

Аннотация: В исследовании предлагается подход к снижению ложноотрицательных заключений проактивного фильтра веб-ориентированной платформы за счет применения двухфакторной аутентификации. Предлагаемый алгоритм в случае подозрения на инцидент информационной безопасности осуществляет дополнительные проверки субъекта доступа, тем самым позволяя избежать блокировки легитимных посетителей. Данная проблема особенно актуальна для сложных систем, характеризующихся динамичностью параметров окружения профилей субъектов доступа.

Ключевые слова: информационная безопасность, аутентификация субъектов доступа, фактор аутентификации, система управления контентом машинное обучение

Введение

Задача разработки адаптивных или риск-ориентированных алгоритмов аутентификации неразрывно связана с применением интеллектуального анализа данных. Современные возможности злоумышленников – подходы и программные средства для автоматизации – зачастую с легкостью позволяют обходить статичные алгоритмы проверки легитимности и механизмы защиты от брутфорс-атак.

В данном исследовании рассматривается алгоритм двухфакторной аутентификации, основанный на дополнительной проверке параметров веб-окружения, фиксируемых системой управления контентом.

Состояние исследований

Разработка эффективного алгоритма двухфакторной аутентификации для веб-ориентированных платформ является актуальной научно-технической задачей, сочетающей комплекс взаимосвязанных работ по применению методов машинного обучения с учетом совокупности структур данных, программно-

аппаратной инфраструктуры, архитектуры фреймворков, протоколов прикладного уровня и т.д. При этом, в литературе достаточно полно рассматриваются аспекты применения различных методов интеллектуального анализа данных в задаче адаптивной аутентификации. Так, согласно [1,2], одним из эффективных механизмов является Байесовская сеть. Кроме того, метод Байесовской сети может быть применен для автоматической генерации правил корреляции при анализе ранее наблюдаемых предупреждений, что позволяет применять подобные сети и для изучения стратегий вторжения. В работах [3-5] отражены исследования различных алгоритмов выявления аномалий и взаимосвязанных процедур идентификации и аутентификации пользователей.

В работе [6] с целью повышения надежности механизма аутентификации пользователей рассматривается технология, сочетающая в себе проверку пароля, биометрических данных и OTP. Стремление специалистов по информационной безопасности сделать многофакторные технологии проверки более доступными и массовыми также находит свое подтверждение в виде научных работ. В частности, в статье [7] рассматриваются результаты проекта по внедрению многофакторной аутентификации с использованием карты «My Number Card», предоставляемой публичной службой идентификации личности, и WebUSB (находится в стадии стандартизации)

Постановка задачи

В качестве исходного объекта был использован действующий веб-портал, построенный на базе популярной сертифицированной ФСТЭК системы управления контентом (CMS). С целью повышения эффективности работы встроенного проактивного фильтра было принято решение разработать алгоритм двухфакторной аутентификации, позволяющий в случае детектирования подозрения на инцидент информационной безопасности осуществлять адаптивный подбор транспортного механизма для отправки одноразовых верификационных кодов в зависимости от источника атаки. В таблице 1 представлен пример запросов, помеченных проактивным фильтром как вредоносные.

Пример регистрации событий, отмеченных как инцидент информационной безопасности приведен в таблице 1.

Таблица 1 – Примеры детектирования инцидентов

Объект	Событие	IP	User Agent	URL	Комментарий
$_SERVER["REQUEST_URI"]	Попытка внедрения PHP	XXX.40.250.124	python-requests/2.26.0	/remote/fgt_lang?lang=/../../../..////////dev/cmdb/sslvpn_websession/../../../..////////dev/cmdb/sslvpn_websession	Корректное определение вредоносной сигнатуры запроса
$_POST['FEEDBACK_TEXT_FID1']	Попытка внедрения SQL	XXX.92.178.86	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.72 Safari/537.36	/support/	Корректное определение вредоносной сигнатуры запроса
123751	Попытка авторизации	XXX.211.197.12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36	/auth/	Ошибочное определение в связи с нехарактерной геопозицией субъекта

Представленные данные свидетельствуют о наличии ошибок 1 рода, связанных с преобладанием сигнатурных методов выявления атак и статических моделей субъектов доступа.

Предложенный алгоритм

На рисунке 1 представлена блок-схема предложенного алгоритма двухфакторной аутентификации, позволяющей снизить количество ошибок работы встроенного проактивного фильтра веб-ориентированной платформы, при этом обеспчивая надлежащий уровень доверия к процедурам проверки легитимности за счет применения дополнительного фактора аутентификации.

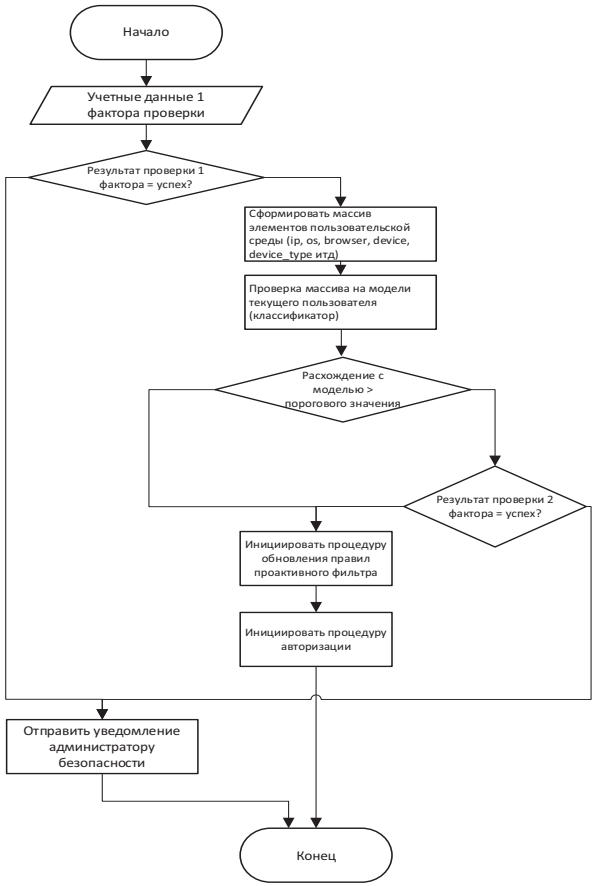


Рисунок 1 – Блок-схема работы алгоритма адаптивной аутентификации

Эксперимент

Реализация классификатора субъектов доступа осуществлена на языке программирования Python. Выходным признаком был выбран параметр event из журнала аудита CMS. Для обучения классификаторов использовался стандартные журналы аудита объемом 20000 записей. Программная реализация классификации данных была внедрена в обработчик процесса аутентификации и синхронизирована с проактивным фильтром обнаружения атак. Оценка алгоритмов осуществлялась с применением метода K-Fold Cross-validation с параметром K = 8. В результате проведения EDA анализ и последующей оценки информативности входных признаков, наибольшее влияние на результат оказывают IP-адрес и отдельные компоненты UserAgent.

Результаты апробирования алгоритмов представлены в таблице 2.

Таблица 2 – Результаты внедрения алгоритма

Механизм	FRR
Однофакторная аутентификация, проактивный фильтр CMS	0,0045%
Двухфакторная аутентификация, проверка окружения с помощью алгоритма KNN (Евклидово расстояние)	0,0031%
Двухфакторная аутентификация, проверка окружения с помощью алгоритма KNN (Косинусная метрика)	0,0033%
Двухфакторная аутентификация, проверка окружения с помощью алгоритма SVM (Линейная разделяющая функция)	0,0034%
Двухфакторная аутентификация, проверка окружения с помощью алгоритма SVM (Радиальная базисная функция)	0,0023%

Экспериментальная проверка доказывает эффективность предложенного алгоритма с использованием классификатора набора данных по входным признакам. Наилучший результат классификации показало применение алгоритма двухфакторной

аутентификации, с применением проверки окружения с помощью алгоритма SVM с радиальной базисной функцией.

Исследование выполнено при частичной финансовой поддержке гранта Президента Российской Федерации в рамках научного проекта № МК-2421.2020.9

Литература:

1. *Chantan C., Sinthupinyo S., Rungkasiri T.* Improving Accuracy of Authentication Process via Short Free Text using Bayesian Network // International Journal of Computer Science Issues. – 2012. – Vol. 9. Issue 2, № 3. – P. 10-16.

2. *Kavousi F., Akbari B.* A Bayesian network-based approach for learning attack strategies from intrusion alerts // Security Comm. Networks. – 2014. – Vol. 7. – P. 833-853.

3. *Srilakshmi V., Dhamodharan P.* Improved Privacy over Authentication of K-Nearest Neighbor Query on Spatial Network. IJSRM. – 2015. – Vol. 3. Issue 2. – P. 2196-2203.

4. *Калинин М.О., Штеренберг С.И.* Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // Интеллектуальные технологии на транспорте. – 2018. – №3 (15). – С. 47-54.

5. *Попова И.А.* Обнаружение аномалий в наборе данных с помощью алгоритмов машинного обучения без учителя Isolation Forest и Local Outlier Factor // StudNet. – 2020. – Т.3. № 12. – С. 1460-1470.

6. *Hassan M.A., Shukur Z.* A Secure Multi Factor User Authentication Framework for Electronic Payment System / 3rd International Cyber Resilience Conference (CRC) (29-31 Jan. 2021 Langkawi Island, Malaysia). – URL: https://ieeexplore.ieee.org/document/9392564 (дата обращения 10.10.2021).

7. *Fujita Y., Inomata A., Kashiwazaki H.* Implementation and Evaluation of a Multi-Factor Web Authentication System with Individual Number Card and WebUSB / 20th Asia-Pacific Network Operations and Management Symposium (APNOMS) (18-20 Sept. 2019 Matsue, Japan). – Matsue, 2019. – P. 1-4. – URL: https://ieeexplore.ieee.org/document/8893134 (дата обращения 10.10.2021).

Жарко Е.Ф.

Некоторые вопросы процесса верификации и валидации управления кибербезопасностью

Аннотация: В работе рассматриваются процессы обеспечения качества программного обеспечения для средств управления кибербезопасностью. В связи с тем, что системы управления могут быть модифицированы, то для обеспечения выполнения функций безопасности, необходимых для управления кибербезопасностью предложено использовать расширенный жизненный цикл разработки ПО. Также в работе предложена качественная модель процесса верификации и валидации управления кибербезопасностью.

Ключевые слова: программное обеспечение, верификация, валидация, кибербезопасность, критическая информационная инфраструктура

Цифровизация систем управления объектов критической информационной инфраструктуры (КИИ) обратила внимание на новую задачу – обеспечение их кибербезопасности. В первую очередь это связано с тем, что объекты КИИ в виду своей инерционности в части внедрения цифровых технологий в настоящее время находятся на ранней стадии решения задачи обеспечения кибербезопасности [1]. До последнего времени уделялось мало внимания задачам кибербезопасности по сравнению с другими вопросами безопасности, и одновременно стоит отметить закрытость информации по инцидентам и аварийным ситуациям [2]. Для обеспечения предоставления необходимой информации о имеющихся проблемах кибербезопасности были разработаны нормативные документы, руководства и стандарты, в том числе в части оценки и выбора средств управления кибербезопасностью. Управление кибербезопасностью в первую очередь – это меры безопасности или контрмеры, которые позволяют избегать, обнаруживать, минимизировать риски кибербезопасности для физического имущества, информации, компьютерных систем и других активов.

Необходимо учитывать, что сложная структура объектов КИИ и большое количество средств управления кибербезопасностью

затрудняют верификацию и применение средств управления кибербезопасностью на всех этапах жизненного цикла от проектирования до эксплуатации. В связи с этим для усилия направлены на разработку методологии оценки и выбора средств управления кибербезопасностью. Данный подход применяется при разработке систем верхнего уровня объектов КИИ.

Однако применение мер безопасности в системах управления объектов КИИ является не только проблемой защищенности, но и проблемой безопасности системы в целом. Это связано с тем, что функции безопасности и защищенности могут влиять друг на друга и вызывать проблемы безопасности. Поэтому особую важность приобретает безопасное управление конфигурацией при интеграции, при этом производительность и надежность систем управления объектов КИИ не должны ухудшаться средствами управления кибербезопасностью. Стоит отметить, что в существующих руководствах по кибербезопасности подчеркивается, что некоторые средства контроля защищенности, которые могут оказать негативное влияние на функции обеспечения безопасности и защиты, должны быть верифицированы для подтверждения отсутствия неблагоприятного влияния.

В связи с внедрением новых технологий (таких как искусственный интеллект и кибербезопасность), разработчиков программного обеспечения (ПО) для систем управления объектов КИИ внимание привлекли новые типы программных сбоев и неисправностей. Однако из-за присущих характеристик и практических ограничений программного обеспечения систем управления объектов КИИ подходы количественного измерения надежности программного обеспечения имеют некоторые ограничения в демонстрации требуемого уровня надежности. Одним из наиболее перспективных альтернативных подходов является использование информации о качестве разработки программного обеспечения. С этой точки зрения предложен метод оценки надежности программного обеспечения на основе процесса верификации и валидации [3], позволяющий моделировать процесс внесения и устранения ошибок на каждом этапе разработки.

Разработка программного обеспечения обычно адаптируется к одному из классических жизненных циклов ПО [4]. В классическом жизненном цикле процесс разработки ПО можно рассматривать как

эволюцию ПО, которая проходит через упорядоченную последовательность переходов от одной фазы к другой в порядке очередности. Ошибки ПО вносятся и устраняются в ходе переходного процесса на каждом этапе разработки, и количество внесенных в процессе разработки ошибок сильно зависит от качества процесса разработки ПО. Ошибки, внесенные разработчиками или средствами разработки ПО, устраняются проведением верификации и валидации. На рисунке 1 представлена упрощенная модель внесения и устранения ошибок на этапе разработки. Используя байесовскую сеть доверия, число оставшихся отказов может быть оценено с учетом факторов, имеющих отношение к надежности, таких как качество управления процессом разработки, сложность процесса и т.д.

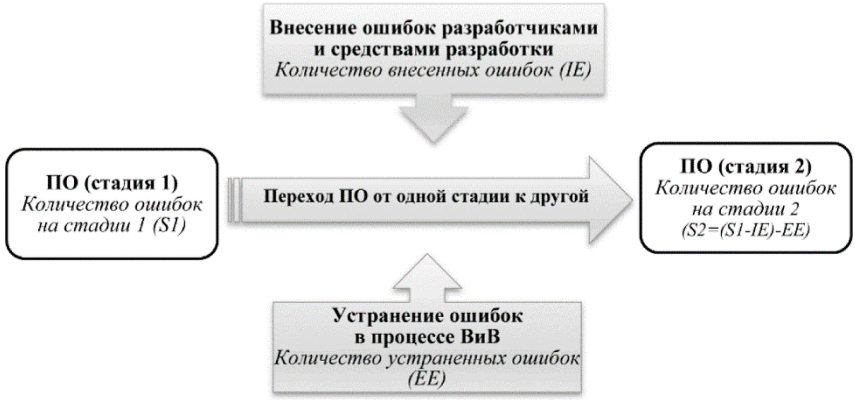


Рисунок 1 – Схема внесения/устранения ошибок на каждом этапе разработки ПО

В перспективе системы управления объектов КИИ будут защищены мерами кибербезопасности, применяемых регулирующими органами, которые будут включать подсистемы безопасности, такие как система обнаружения вторжений, система наблюдения, система контроля доступа и т.д. Системы управления могут быть модифицированы с целью обеспечения выполнения функций безопасности, необходимых для управления кибербезопасностью, на основе расширенного жизненного цикла

разработки ПО (рисунок 2) [1]. Применение мер управления кибербезопасностью повышает уровень связности системы, а также уровень ее безопасности. Уровень связности является активно используемой мерой, которая фиксирует зависимости, существующие между каждым компонентом ПО и каждой системой [5]. По мере увеличения уровня связности, частота программных сбоев имеет тенденцию к увеличению. Поэтому чрезмерные модификации при применении средств управления кибербезопасностью могут привести к увеличению размера и сложности ПО систем, а также увеличить риск программного сбоя. Кроме того, применение средств управления кибербезопасностью без тщательной проверки качества может усложнить не только структуру системы, но также процессы разработки и интеграции программного обеспечения, что в свою очередь увеличит вероятность сбоев программного обеспечения. Сбои в работе ПО и оставшиеся ошибки, вызванные применением мер безопасности, рассматриваются как серьезная проблема, влияющая на безопасность.

Рисунок 2 – Расширенная V-образная модель жизненного цикла программного обеспечения для обеспечения качества программного обеспечения

Для надежного управления процессом применения средств управления кибербезопасностью, необходимо обеспечивать качество ПО, используя различные методы проверки и тестирования. В области разработки систем управления могут потребоваться дополнительные мероприятия по обеспечению качества средств управления кибербезопасностью.

На рисунке 3 приведена качественная модель процесса верификации и валидации управления кибербезопасностью.

Рисунок 3 – Процесс оценки вероятности сбоя ПО

Первым этапом является разработка процесса применения средств управления кибербезопасностью на основе соответствующих цифровых устройств и функций безопасности, необходимых для каждого элемента управления безопасностью. На втором этапе оценивается отказоустойчивость каждого элемента управления безопасностью, и на основе оценки выявляются и расставляются приоритеты для элементов управления кибербезопасностью. На третьем этапе проверочные тесты

проводятся после определения соответствующего объема и уровня проверки в зависимости от предполагаемой отказоустойчивости каждого элемента управления безопасностью. На четвертом этапе в соответствии с результатами проверочного теста происходит принятие каждого элемента управления безопасностью. Только средства управления безопасностью, прошедшие верификационные тесты, могут применяться к цифровым системам и далее подвергаться постоянному мониторингу. Средства управления кибербезопасностью, которые еще не прошли верификационные тесты, должны быть перепроверены и/или пересмотрены.

Литература:

1. *Жарко Е.Ф., Промыслов В.Г., Исхаков А.Ю., Мещеряков Р.В., Семенков К.В., Абдулова Е.А., Байбулатов А.А., Исхаков С.Ю.* Кибербезопасность беспилотных транспортных средств. Архитектура. Методы проектирования. – М.: Радиотехника, 2021. – 160 с.

2. *Baylon C., Brunt R., Livingstone D.* Cyber security at civil nuclear facilities: understanding the risks. – Chatham House, 2016. – 56 p.

3. *Eom H.S., Park G.Y., Jang S.C., Son H.S., Kang H.G.* V&V-based remaining fault estimation model for safety-critical software of a nuclear power plant // Annals of Nuclear Energy. – 2013. – Vol. 51. – P. 38-49.

4. *Жарко Е.Ф.* Сравнение моделей качества программного обеспечения: аналитический подход // Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). – М.: ИПУ РАН, 2014. – С. 4585-4594.

5. *Жарко Е.Ф.* Формализация функций безопасности и обеспечение качества программного обеспечения систем, важных для безопасности АЭС / Материалы 12-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2019) (1-3 октября 2019 г. Москва). – М.: ИПУ РАН, 2019. – С. 844-847.

Орлов В.Л., Курако Е.А.

Сервис-браузер и атаки типа Man in the middle

Аннотация: Рассматривается устойчивость информационной системы использующей технологию сервис-браузера к атакам Man in the middle. Сервис-браузерная технология сравнивается с веб-браузерной технологией для данного типа атак. Анализируются предпринимаемые меры безопасности.

Ключевые слова: сервис-браузер, атаки, безопасность, информационная система, сеть

В современном мире к информационным системам предъявляются все более строгие требования по устойчивости и безопасности работы. Исследованиям различных угроз в данной области посвящено множество работ. Одной из наиболее значимой угроз, являются атаки типа «человек посредине» (Man in the middle – MITM), которую также называют атакой посредника [1].

Атаки данного типа осуществляются при передаче данных от одного узла другому и, как правило, не зависят от самих узлов. Следует отметить, что эти угрозы можно разделить на активные и пассивные. Активные – это такие атаки, при которых злоумышленник вмешивается в передачу пакетов данных, удаляя или подменяя их. При пассивных атаках ведется только прослушивание каналов связи. Заметим, что в основном, предварительно происходит прослушивание сетевого трафика, а уже после анализа злоумышленник переходит к активным действиям.

Главная опасность заключается в том, что на стадии пассивных очень трудно обнаружить. Трудности обуславливаются тем, что все вредоносная активность происходит вне наблюдаемых узлов. Необходимо проводить постоянный анализ сетевой активности. Существуют и другие методы определения, например, по временным задержкам [2]. Но все равно существующие методы не позволяют достоверно выявлять производимые атаки.

Технология сервис-браузера [3] по сути является распределенной, то есть обеспечивает функционирование на разных узлах, объединенных в сеть. В силу этого она может подвергаться

рассматриваемому типу атак. Условно схему работы данного браузера можно представить, так, как это изображено на рисунке 1. При этом сервис-браузер через публичную сеть взаимодействует с сервером приложений, который, в свою очередь, общается с сервером баз данных.

Таким образом, сеть разделена на два фрагмента. Первый фрагмент предназначен для общения клиентских рабочих мест и сервера приложений посредством сервис-браузера. Он является общедоступным, например, может работать через глобальную сеть Интернет. Второй фрагмент – это внутренняя закрытая сеть информационной системы, где сервера взаимодействуют между собой. Она является частной, и никто, кроме серверов, не имеют в нее доступ.

Таким образом, при рассмотрении атак типа MITM следует рассмотреть два направления защиты.

Рисунок 1 – Схема работы сервис-браузера

Для участка публичной сети обеспечить безопасность необходимо криптографическими средствами. Наиболее прост и распространен способ замены открытого протокола HTTP на зашифрованный протокол HTTPS. К сожалению, простое использование функций шифрования канала, не гарантирует полноценной защиты [4]. В работе рекомендуется использовать пользовательские браузеры, обеспечивающих возможность своего списка доверенных сертификатов. Сервис-браузер, в отличие от стандартного веб-браузера, создавался для ограниченного круга

пользователей, обязательно проходящих аутентификацию и авторизацию. При реализации сервис-браузерной технологии была заложена возможность заранее определять список доверенных сертификатов или список доверенных корневых центров. В результате сервис-браузер прикрывает достаточно слабое место протокола HTTPS – взаимную аутентификацию.

При этом важно понимать, что использование пользователем беспроводных сетей, подключение к общественной сети в непроверенных местах может значительно облегчить злоумышленнику пассивный сбор информации.

Для фрагмента, образующего внутреннюю сеть, часть реализуемой защиты можно обеспечить административными мерами. То есть обеспечить функционирование серверов в закрытом периметре, чтобы доступ к ним имел ограниченный круг пользователей. При этом также, как и в случае публичной сети, необходимо обеспечить шифрование трафика между узлами.

Литература:

1. *Арзуманян Э.А., Чумаков А.А.* МИТМ-атака. Угроза информационной безопасности в РФ // Znanstvena Misel. – 2019. – № 8-1(33). – С. 37-40.

2. *B. Aziz; G. Hamilton* Detecting Man-in-the-Middle Attacks by Precise Timing / Third International Conference on Emerging Security Information, Systems and Technologies (18-23 June 2009 Athens, Greece). – Athens, 2009. – P. 81-86 – URL: https://ieeexplore.ieee.org/abstract/document/5211025 (дата обращения 06.10.2021).

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

4. *Акулов А.А.* Подмена SSL-сертификатов как средство перехвата зашифрованного трафика // Символ науки: международный научный журнал. – 2018. – № 1-2. – С. 19-21.

Жуковская Л.В.

Особенности применяемого математического инструментария для построения систем обеспечения безопасности в социальных сетях

Аннотация: В «эпоху постправды» оценка и прогнозирование информационных угроз, возникающих и распространяющихся посредством социальных сетей, приобретает принципиальное значение для обеспечения безопасности национального информационного пространства. В этой связи, осуществление регулятором «информационной гигиены» национальной медиасферы является одной из приоритетных задач государства. Указанная задача решается посредством построения и использования систем поддержки принятия решений (ИСППР), при разработке которых используется разнообразный математический инструментарий для описания текущего состояния инфосферы и ее прогнозирования. Такой подход определяет возможность использования формальных математических моделей изменения мнений для обнаружения и мониторинга источников потенциальных информационных угроз, возникающих в социальных сетях.

Ключевые слова: индивид, пользователь, изменение мнений, поляризация мнений, социальные сети, информационное пространство, информационные угрозы

На современном этапе активно осуществляются попытки моделирования динамики мнений эпохи «постправды». С одной стороны, это обусловлено изменением сбора данных, что позволяет отслеживать мнения отдельных лиц и социальных групп на гораздо более детальном уровне, с другой стороны, возрастает роль инструментов конструирования социальной реальности. Большая часть влияний, формирующих общественное и индивидуальное мнение по различным вопросам, определяется фальшивыми новостями, манипуляциями и формированием различных форм человеческих предубеждений и пр. Одним из компонентов рассматриваемых моделей является механизм взаимодействия,

описывающий влияние одного или группы пользователей на остальных. Например, «модель избирателя», «модель ограниченной уверенности» или «модель группы влияния», где соответствующим образом усредненное мнение группы «окружающей» пользователя повлияло на его мнение, например, «модели социального воздействия» [1]. Среди наиболее широко используемых моделей используются модели «ограниченной уверенности», которые предполагают, что мнения двух взаимодействующих пользователей могут стать ближе друг к другу только в том случае, если начальная разница была достаточно небольшой, ниже порога толерантности. Группы моделей «ограниченного доверия» разработаны, чтобы охватить множество вариантов, некоторые из которых включают в себя «отталкивание» достаточно разных мнений, рассмотрение многомерного пространства мнений, присутствие групп меньшинств, твердо придерживающихся своего мнения, и многие другие. Другая концепция, способствующая потенциальному отсутствию консенсуса в обществе, заключается в рассмотрении взаимосвязи индивидуальных изменений мнений с развитием сети социальных контактов. Результатом этого процесса является разделение сообщества на несвязанные части, которые сравнивают с социологическими понятиями фокус-групп и избирательных предпочтений [2].

Необходимо отметить, что модели изменения мнений содержат ряд проблем, некоторые из которых не решены до сих пор. Например, выбор начальных условий: предположение, что социальные системы можно «подготовить» полностью рандомизированным образом нереалистично. Второй пример – это отображение временных параметров модели на существующие реальности. В некоторых случаях, таких как реакция на чрезвычайные события (стихийные бедствия или террористические акты), проблема отслеживается характерными формами социального поведения, например, всплесками количества пожертвований на благотворительность. В других случаях, когда существует предположение о том, что общение осуществляется через инструменты социальных сетей, такие как Twitter или Facebook, или обсуждения в Интернете. Если рассматривать каждое такое сообщение как соответствующее одному событию моделирования, то предположительно можно протестировать

способность модели имитировать глобальную динамику, используя «реалистичное» количество временных интервалов [2].

Следующая группа моделей возникла в результате роста интереса исследователей к реальным социальным системам и их свойствам и включает такие важные явления, как роль лидеров мнений и средств массовой информации; долговременная нестационарность и влияние экстремизма; проявление «принципа доминирования меньшинства над большинством», основанные на мнениях и мировоззрениях и глобальнорастущей поляризации общества. Последняя проблема сформулировала для исследовательского сообщества вопрос, «*каким образом мнения в различных группах населения становятся поляризованными*».

Одним из способов объяснения поляризации общества является предположение о существовании особых классов пользователей – непреклонных, фанатиков или экстремистов [3]. Если пользователи представляют мнения на «крайних концах разрешенного спектра», они могут управлять динамикой мнений и «притягивать» к себе умеренных, создавая сильно поляризованное общество. Фактически делается интуитивное предположение о том, что, «нет необходимости включать в модель какой-либо особый класс «негибких элементов», например, в рамках ограниченной доверительной структуры, все, что требуется, – это условие, чтобы мнения, близкие к крайним концам пространства мнений, были связаны с уменьшением допусков» [3]. В такой ситуации большинство пользователей не только могут придерживаться крайних взглядов, но и сами становятся «негибкими».

Другие способы достижения «поляризованного конечному состояния», это например, «рассмотрение нескольких тем, некоторые из которых могут быть более «важными» для пользователей, и при этом разногласия по более важному мнению могут вызвать поляризацию в менее важной» [3]. Рассматриваемые модели могут быть довольно сложными через объединение «внутренних» измерений, характеризующих пользователей (уровень образования и социально-экономическое положение) и тематических измерений (относительно финансовых и социальных вопросов)» [4-6]. Общение между пользователями, на которых они обсуждают свое мнение, часто связаны с приводимыми ими аргументами, используемыми в поддержку индивидуальных

мнений. Когда два индивида «разделяют схожие взгляды», они могут «усилить» свое мнение, предлагая друг другу новые способы поддержки и результат становится более радикальным. Этот подход, получивший название «теории убедительных аргументов», использовался в нескольких поляризационных моделях [4-6]. Еще один подход – «использовать отталкивающие реакции на мнения, сходные с вашим собственным», через нонконформизм и противоречивость [7].

Существуют также модели, подчеркивающие так называемые «эффекты несходства», в которых пользователи не только не сближают свои мнения друг с другом, если их мнения относительно схожи, но и еще больше расходятся, если исходная разница превышает определенный порог. Такие модели «силы отталкивания или отторжения» имеют обоснование с точки зрения психологии, в частности, в исследованиях так называемого «обратного эффекта». Столкнувшись с информацией, противоречащей текущим убеждениям, вместо того, чтобы изменить свое мнение в сторону некоторого усредненного значения, пользователи могут «двигаться в противоположных направлениях». В то же время, в исследованиях «обратного эффекта» и его вклада в продолжающуюся поляризацию общества, следует принимать во внимание такие психологические аспекты как, так называемое «избирательное внимание» и «предвзятость подтверждения», которые могут ограничить частоту и возможность встреч лиц с противоположными взглядами. Если индивид будет избегать контактов с другими пользователями или средствами массовой информации, выражающими противоположные взгляды так называемый «эффект отталкивания или неприятия» уменьшится, вследствие отсутствия информационного воздействия. Такие эффекты моделировались в сетевых моделях, предполагающих динамический характер социальных связей, например в [6].

Таким образом, поляризация, понимается как «разделение общества на отдельные группы, придерживающиеся непересекающихся мнений» [7] и может быть объяснена вышеуказанными описанными формальными механизмами. Обзор достижений в динамике общественного мнения [8] перечисляет несколько «важных» расширений классических моделей: человеческое упрямство, наличие предвзятости, манипулирование

мнением, наличие отталкивающего поведения, взаимосвязь между несколькими темами и разница между выраженным и частным мнением.

Еще одно направление развития моделей изменения мнений было вызвано их объединением с исследованиями настроений или эмоций в межличностном общении, особенно проводимых с помощью электронных средств. Было обнаружено, что эмоции не только «сопровождают» обмен мнениями, но также во многих случаях определяют результаты такого обмена и формируют процессы коммуникации. Исходя из этих наблюдений, модели, включающие в себя эмоции в качестве параметров, позволили воспроизвести широкий спектр характерных черт общения по широкому кругу тем [5,6]. Например, в модели эмоции / информации / мнения (EIO) [4] использована нелинейная динамика взаимодействия между эмоциями и полученной информацией для формирования индивидуальных мнений. Абстрактная модель позволила предсказать результаты польских парламентских выборов 2015 г. с точностью 3% [5].

Несмотря на достижения, предлагаемые современным математическим инструментарием, например, способность имитировать не только консенсус, но также конфликты и разногласия, все еще существует огромный разрыв между богатством реального человеческого поведения и ограниченным набором действий и характеристик, включенных в формальные модели. Например, информация, передаваемая при личных контактах или полученная из средств массовой информации или наблюдений, может быть неточной, подтасованной или ложной. Причина разницы между переданными ценностями и истинным состоянием, например, истинное мнение человека, с которым мы разговариваем, или точное описание вопроса, связанного с СМИ, может быть преднамеренным или нет. Сознательная ложь может быть вызвана стремлением достичь определенных целей, защитить или сохранить свое положение в группе или обществе. Но ложная информация также может быть результатом самообмана или обмана. Более того, намеренное искажение информации не обязательно является «злом» – манипулирование информацией используется во многих ситуациях «на благо всех заинтересованных», включая получателя, который

затем будет принимать «правильные» решения на основе ошибочных данных. Включение искажений и манипуляций в структуру моделирования чрезвычайно сложно и зависит от субъективной способности определять цели и мотивацию пользователей. Также недостаточно сведений о статистическом распределении таких характеристик, поэтому создание разумных начальных условий, особенно для крупномасштабного моделирования, было бы практически невозможно. Более того, влияние коммуникации на мнение конкретного человека может быть и, часто зависит, от одного или нескольких когнитивных предубеждений, вызванных содержанием, формой коммуникации или даже внешними обстоятельствами. В психологии распознают более ста различных типов «смещений», в результате воздействия таких факторов, как информационная перегрузка, отсутствие смысла, необходимости действовать быстро, и обработку информации и селективности запоминания. При этом важным вопросом, остается «какие именно, предубеждения доминируют для конкретного индивида в данной ситуации, далеко не очевидно и может зависеть от его личной истории или от обстоятельств, которые обычно отсутствуют в рамках моделирования».

Вывод

Эволюция математического инструментария, используемого при построении ИСПРР за достаточно короткий промежуток времени прошла путь от простых решетчатых структур до формализации динамики изменения сложных социальных сетей, включая сети, которые меняются динамически параллельно с изменением мнений и многие формальные модели учитывают различия в топологиях межличностного общения. При этом поиск динамики (изменения) мнений в вышеуказанных моделях определяется представляющими перспективный научный интерес несколькими доминирующими факторами и механизмами, которые могут позволить «распутать» связи между различными методологиями естественных и гуманитарных наук.

В завершении необходимо отметить, что нормативная правовая база, используемая для обеспечения регулятором «информационной гигиены» (Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности

Российской Федерации») носит рамочный и общий характер, что не позволяет четко сформировать группы показателей, которые можно использовать при построении аналитических конструкций. Для решения указанной проблемы требуется разработать и принять в меры правового воздействия (предотвращения) на появление не только внешних, но и внутренних информационных угроз. В данном случае необходимо действовать на опережение, так как меры правового воздействия на появление различного рода информационных угроз, как и весь комплекс их реализации и последствий, в той или иной степени нормативно не урегулирован.

Литература:

1. *Galam S.* Sociophysics: a physicist's modeling of psycho-political phenomena. – Berlin, Germany: Springer, 2012. – 439 p.

2. *Sobkowicz P.* Social simulation models at the ethical crossroads // *Science and Engineering Ethics.* – 2019. – Volume 25. Issue 1. – P. 143-157. doi:10.1007/s11948-017-9993-0

3. *Sobkowicz P.* Extremism without extremists: deffuant model with emotions // *Front Phys.* – March 2015. – Volume 3. – Article 17. doi:10.3389/fphy.2015.00017

4. *Sobkowicz P.* Discrete model of opinion changes using knowledge and emotions as control variables // *PloS One.* – 2012. – Volume 7 (9). –e44489. doi:10.1371/journal.pone.0044489

5. *Sobkowicz P.* Quantitative agent based model of opinion dynamics: polish elections of 2015 // *PloS One.* – 2016. – 11(5):e0155098. doi:10.1371/journal.pone.0155098

6. *Sobkowicz P.* Studies of opinion stability for small dynamic networks with opportunistic agents // *Int J Mod Phys C.* – 2009. – Vol. 20. – №10. – P. 1645-1662. doi:10.1142/S0129183109014655

7. *Sobkowicz P.* Whither Now, Opinion Modelers? // *Front. Phys.* – 2020. – Vol. 8. – Article 587009. doi: 10.3389/fphy.2020.587009

8. *Noorazar H.* Recent advances in opinion propagation dynamics: a 2020 survey // *Eur Phys J Plus*. – 2020. – Volume 135. Issue 6. – Article 521. doi:10.31140/epjp/s13360-020-00541-2

Авдеева З.К., Коврига С.В.

Систематизация психологических факторов влияния на изменение убеждений и аттитюдов в результате коммуникативных воздействий в виде модели причинно-следственных влияний

Аннотация: На основе анализа современных психологических исследований проведена систематизация психологических факторов, характеризующих убеждающие воздействия при коммуникации, и построена модель причинно-следственных влияний этих факторов на эффективность убеждающего воздействия, нацеленного на изменение аттитюдов, представлений и убеждений. Данная модель является основой для исследования возможных постановок задач анализа устойчивости и согласованности убеждений и аттитюдов по оцениваемому явлению (ситуации) посредством методов анализа и моделирования на основе когнитивных карт.

Ключевые слова: информационно-психологические процессы, коммуникация, убеждающее воздействие, аттитюд, убеждение, когнитивная карта ситуации

Одним из актуальных направлений обеспечения безопасности личности, общества и государства является обеспечение информационно-психологической безопасности, которое связано со сферой растущего многообразия информационно-психологических и когнитивных процедур, угроз, операций [1].

В условиях глобальной информатизации, бурного роста информационных и телекоммуникационных технологий и медиатизации общества информационно-коммуникативные процессы занимают все более значимое место в сфере социально-политического управления в обществе. Любая поступающая к человеку информация оказывает то или иное влияние на его поведение, суждения, установки (аттитюды), чувства [2]. Тем самым убеждающая коммуникация всегда предполагает воздействие, под влиянием которого у объекта воздействия (личности, группы) могут возникать потребности как конструктивного, так и деструктивного характера, что

существенным образом влияет на развитие информационно-психологических конфликтов в обществе, на социально-политическую ситуацию в отдельно взятой стране и в мировом пространстве в целом.

В широком смысле под убеждением (persuasion) понимаются любые попытки воздействия (как правило, речевого), цель которых – изменение установок, убеждений (beliefs) и представлений человека. Чаще всего в качестве цели убеждения рассматривается изменение установок – аттитюдов (attitudes) [2]. В современной социальной психологии аттитюд определяется как относительно общая и продолжительная оценка объекта по валентному измерению, варьирующемуся от негативного до позитивного. Эти оценки могут быть привязаны практически ко всему, включая людей, социальные группы, физические объекты, поведение и абстрактные концепции [3].

Основными элементами коммуникативной ситуации являются коммуникатор – субъект воздействия, сообщение – средство воздействия, реципиент (или аудитория) – объект воздействия, каждый из которых характеризуется группой факторов, определяющих эффективность убеждающего воздействия [3-4]. При этом максимальная эффективность убеждающего сообщения достигается за счет оптимального сочетания разных факторов.

Опираясь на современные психологические исследования в области коммуникативного воздействия ([2-4] и др.), мы провели систематизацию психологических факторов, характеризующих убеждающие воздействия при коммуникации, и на ее основе построили M_{Inf} – модель причинно-следственных влияний этих факторов на эффективность убеждающего воздействия, нацеленного на изменение представлений, аттитюдов и убеждений (рисунок 1). Разработанная модель M_{Inf} предназначена для исследования возможных постановок задач анализа устойчивости и согласованности аттитюдов и убеждений в информационно-психологических, социально-политических процессах посредством методов анализа и моделирования на основе когнитивных карт (КК).

КК – это формализованная модель о причинно-следственных связях между значимыми факторами ситуации, построенная на основе суждений, убеждений отдельного или коллективного субъекта коммуникации.

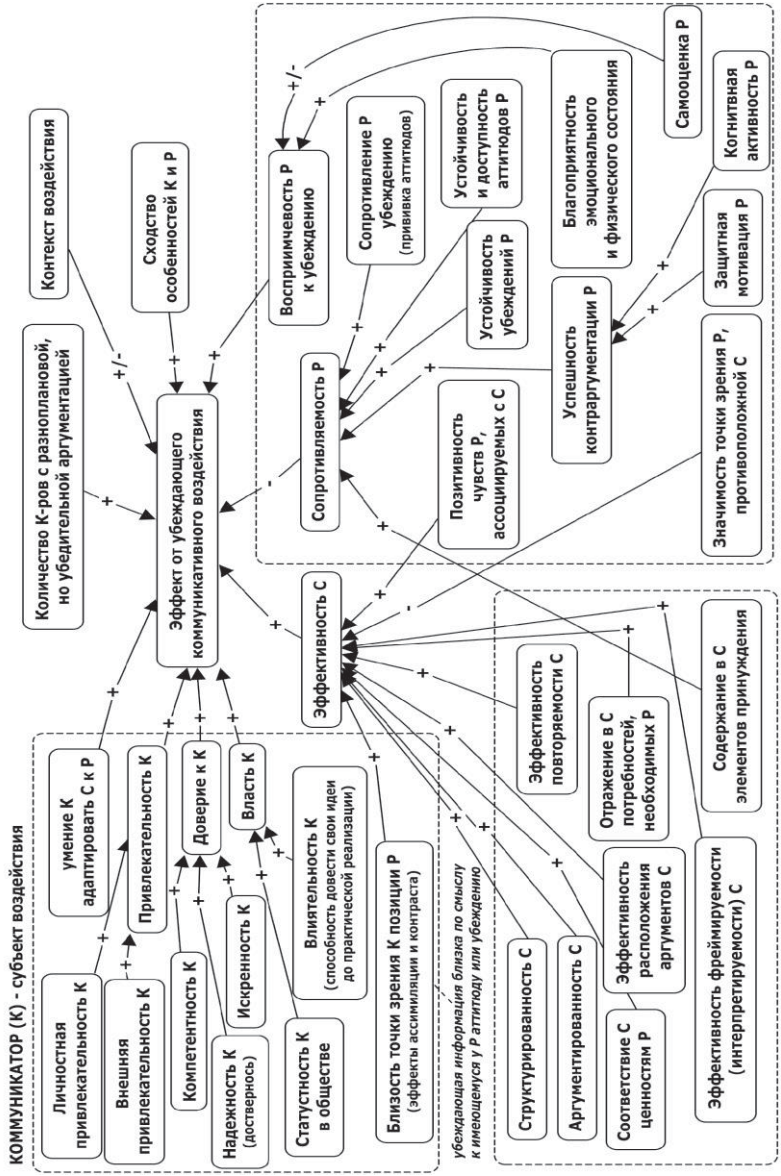


Рисунок 1 – Модель причинно-следственных влияний факторов коммуникативного воздействия на убеждения и аттитюды

Особенность КК состоит в возможности вербализации ментальных моделей, убеждений и представлений причастных сторон по некоторой проблеме или теме. Как следствие, КК позволяет (1) делать убеждения и представления субъекта явными и проверяемыми, и (2) формировать целостное представление о ситуации с учетом разного видения нескольких субъектов. Диапазон приложений КК простирается от концептуального моделирования, направленного на улучшение структурирования и понимания проблем, до решения практического моделирования анализа и моделирования динамики ситуации.

В таких сферах как политика, геополитика, международные отношения, безопасность окружающей среды, где коммуникация различных причастных сторон в ситуации играет существенную роль в принятии решений, а сами субъекты по-разному воспринимают ситуацию и интерпретируют поступающую информацию о ней, КК и методы на ее основе находят все большее применение как инструменты (1) исследования аргументации участников коммуникации с целью анализа устойчивости их взглядов, выявления противоречий в представлениях и интересах; (2) формирования коллективного целостного и согласованного представления о ситуации; (3) формирования возможных сценариев развития ситуации в условиях консенсуса мнений или под воздействием убеждений одной из конфликтных сторон [5-7].

Принимая во внимание перечисленные возможности КК и с учетом выделенных факторов коммуникативного воздействия (модель M_{Inf}), мы планируем исследовать постановки задач, связанные с устойчивостью и непротиворечивостью системы убеждений и аттитюдов субъекта по некоторой ситуации, явлению (P) в условиях коммуникативных воздействий других субъектов ситуации или в условиях массовой коммуникации посредством различных медиа-средств.

Для исследования указанных задач базовая модель представления системы убеждений субъекта об оцениваемой ситуации P (объект аттитюда) в виде КК ситуации $K(X, A, f)$ включает: X – множество факторов (каждый из которых представлен понятием – концептом) в системе убеждений субъекта S о P, включая факторы его интересов (целевые факторы); A – множество отношений между X, которое может быть представлено квадратной матрицей $A = [a_{ij}]$

причинно-следственных влияний, где a_{ij} – вес влияния фактора x_i на x_j, характеризующий степень уверенности субъекта в наличии влияния $x_i \rightarrow x_j$ на шкале в интервале от -1 до 1 (число градаций может варьироваться); f – функцию агрегирования (активации) любого зависимого фактора от факторов, влияющих на него. Каждый фактор из X, связанный с субъектом S, может позитивно или негативно оцениваться им в контексте P; для этого вводится оценка фактора субъектом на простой шкале 1, 0, -1 («полезно-нейтрально-вредно» / «хорошо-нейтрально-плохо» и т.п.) или шкале с большим числом градаций в интервале от -1 до 1 (для более детального оценивания).

В качестве задела по методам для решения задач, связанных с устойчивостью и непротиворечивостью системы убеждений и аттитюдов субъекта по некоторой ситуации, явлению (P) в условиях коммуникативных воздействий, мы рассматриваем методы анализа на основе различных структурных показателей сетей и КК [8, 9] и собственные методы построения и анализа КК [10, 11].

Важно отметить, что состав параметров базовой модели и методы ее анализа в рамках исследования обозначенных постановок задач могут быть расширены. В частности, $K(X, A, f)$ субъекта S, отражающая его внутренние представления о P, может быть расширена внешними факторами (вместе с их взаимосвязями между собой и факторами из $K(X, A, f)$), отражающими представление объекта аттитюда P в «общем» коммуникативном пространстве.

На основе построения $K(X, A, f)$ (с или без внешних факторов) и последующей ее коррекции и анализа в разные периоды времени, можно рассмотреть задачу прослеживания траектории изменения системы убеждений и аттитюдов субъекта S о ситуации P (с учетом изменений и самой P), ранжировать значимость влияния факторов на эти изменения. Кроме того, объединение нескольких карт субъектов $\{S_i\}$ по оцениваемой ситуации (явлению) P для выявления противоречий в убеждениях, путей снятия или нейтрализации этих противоречий позволяет рассмотреть задачу формирования консенсуса, согласованного представления (в том числе проследить и траекторию его изменения со временем).

Работа выполнена при финансовой поддержке РФФИ – грант 19-29-07525

Литература:

1. Информационно-психологическая и когнитивная безопасность. Коллективная монография / Под ред. И.Ф. Кефели, Р.М. Юсупова. – СПб: ИД «Петрополис», 2017. – 300 с.

2. *Латынов В.В.* Психология коммуникативного воздействия. – М: Институт психологии РАН, 2013. – 368 с.

3. The Handbook of Attitudes. Volume 1: Basic Principles / Ed. D. Albarracnn and B.T. Johnson. – New York-London: Taylor & Francis, 2019. – 678 p.

4. *Гулевич О.А., Сариева И.Р.* Социальная психология. – М.: Юрайт, 2015. – 452 с.

5. Аналитические доклады. Новое пространство мировой политики: взгляд из США. Выпуск 6 (30) / Под общ. ред. В.М. Сергеева и Е.С. Алексеенковой. – М.: МГИМО – Университет, 2011. – 136 с.

6. *Горелова Г.В., Рябцев В.Н.* Моделирование архитектуры и динамики геополитических регионов современного мира: когнитивный подход (зона «Черноморье-Кавказ-Каспий»). – Ростов-на-Дону: Изд-во ЮФУ, 2014. – 374 с.

7. *Papageorgiou K.* and other. Fuzzy cognitive map-based sustainable socio-economic development planning for rural communities // Sustainability. – 2020. – 12(1). – URL: https://www.mdpi.com/2071-1050/12/1/305 (дата обращения 14.10.2021).

8. *Gray S.A., Zanre E. and Gray S.* Fuzzy cognitive maps as representations of mental models and group beliefs: theoretical and technical issues / Fuzzy cognitive maps for applied sciences and engineering. E. Papageorgiou (Ed). – Springer, 2014. – P. 29-48.

9. *Yoon B.S., Jetter A.J.* Comparative Analysis for Fuzzy Cognitive Mapping // Engineering and Technology Management Faculty Publications and Presentations. – 2016. – 112. – URL: https://pdxscholar.library.pdx.edu/etm_fac/112 (дата обращения 14.10.2021).

10. *Avdeeva Z.K.., Kovriga S.V.* On situation control problem settings with multiple stakeholders using cognitive maps // Automation and remote control. – 2020. – Vol. 81(Iss.1). – P. 139-152.

11. *Avdeeva Z.K., Kovriga S.V.* Analytical and instrumental framework for the analysis and resolution of stakeholder interest conflict using cognitive maps // Journal of Physics: Conference Series. – 2021. – Vol. 1828. – URL: https://iopscience.iop.org/article/10.1088/1742-6596/1828/1/012108/pdf (дата обращения 14.10.2021).

Мамченко М.В., Рей А.С.

Оценка рисков распространения деструктивного контента в социальных сетях

Аннотация: В работе представлен обобщенный подход к оценке рисков в задаче выявления и блокирования деструктивного контента в социальных сетях, позволяющий вводить дополнительные метрики для оценки значений параметров, связанных с передаваемым сообщением. Представлены структура типовой системы выявления и блокирования деструктивного контента в социальных сетях, место в ней системы оценки рисков и обобщенный алгоритм ее работы. Задействование системы оценки рисков теоретически позволяет сократить количество обращений к модератору, используя значения показателей доверия для отправителя, осуществлять стратификацию и агрегацию категорий деструктивного контента в зависимости от уровня его угрозы, а также контролировать возраст целевой аудитории, являющейся адресатом направляемого сообщения.

Ключевые слова: социальные сети, оценка риска, критерии риска, социо-киберфизическая система, деструктивный контент

В настоящее время сеть Интернет уже возможно рассматривать в качестве социо-киберфизической системы (СКФС), которая оказывает сильное влияние на поведение и способы коммуникации людей. Использование ресурсов Интернета предоставляет большие возможности, но также несет большие риски, связанные с влиянием деструктивного контента на индивидуальное и групповое сознание пользователей. Среди всех пользователей Интернета несовершеннолетние дети и подростки считаются наиболее уязвимой группой риска, так как, будучи одной из наиболее

активных групп в сети Интернет, они начинают взаимодействовать с киберпространством еще с дошкольного возраста. В целом деструктивный контент в сети Интернет и других СКФС является одним из основных негативных факторов воздействия на пользователей (особенно – на молодое поколение), и задача выявления и блокирования подобного контента является актуальной [1]. Социальные сети предпринимают самостоятельные меры по выявлению и блокировке запрещенного контента. В частности, реализуются и совершенствуются алгоритмы фильтрации сообщений и потоковых трансляций пользователей и сообществ в режиме реального времени. Предложено большое количество соответствующих подходов, методов, алгоритмов и архитектур. Например, в работе [2] предложена архитектура мультиагентной системы выявления деструктивного информационного воздействия в социальных сетях, включающая в себя множество агентов, а в статье [1] представлена независимая и федеративная реализации архитектуры отдельной СКФС для выявления разнородного негативного контента в сети Интернет. Недостатком подобных систем является необходимость полной проверки всех сообщений вне зависимости от уровней доверия и охвата его отправителя (источника) и характеристик целевой аудитории, отсутствие разделения деструктивного контента в зависимости от степени его опасности, а также невозможности снижения уровня доверия источника сообщения при попытке передать в нем деструктивный контент. Таким образом, целью настоящей работы является разработка подхода к комплексной оценке риска распространения сообщения в контуре системы выявления и блокировки деструктивного контента.

В соответствии с [3], проведем детализацию задач системы комплексного оценивания риска распространения сообщений в виде дерева критериев. Комплексным показателем (критерием) будет «уровень риска распространения сообщения» (К1), который будет определяться «состоянием угрозы источника» (К21), «возрастным показателем целевой аудитории» (К22) и «уровнем деструктивности контента» (К23). В свою очередь, показатель «состояние источника» будет определяться «уровнем доверия источника» (К211) и «уровнем популярности источника» (К212) (рисунок 1).

Рисунок 1 – Дерево критериев

Введем дискретную шкалу с агрегированными оценками для каждого критерия, где значения уровня риска возрастают от 1 до 4. На основании сформированных критериев и их дискретных оценок сформируем матрицы свертки. Свертка оценок критериев К211 и К212 позволит сформировать оценки критерия К21. Затем возникает необходимость осуществить операцию свертки для оценок трех критериев (К21, К22, К23), чтобы получить значения интегрального критерия К1. В этом случае возможны три комбинации критериев, в результате которых получаются три матрицы свертки, среди которых выбирается матрица с наивысшими выходными значениями уровня риска. Следует отметить, что конкретные значения в матрицах свертки для сопоставления оценок критериев выбираются ответственными должностными лицами или экспертами [3]. Графическое описание формирования матриц свертки для оценок всех критериев представлено на рисунке 2.

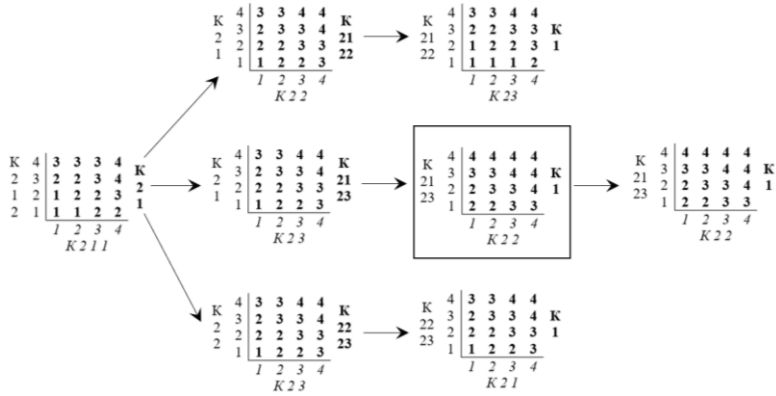


Рисунок 2 – Матрицы свертки для значений оценок критериев

Рассмотрим архитектуру СКФС обнаружения негативного контента в социальных сетях, представленную в [1]. Система состоит отдельно из парсера контента, модуля анализа, базы данных (БД) оценок деструктивных свойств контента и модуля принятия решения, с которым взаимодействует оператор (модератор контента).

Систему оценки рисков возможно внедрить в архитектуру данной системы в виде отдельного блока в составе модуля принятия решения. Кроме того, необходимо внедрение дополнительной БД, содержащей оценки надежности отправителей сообщений. Алгоритм функционирования блока системы оценки рисков (БСОР) включает в себя следующие шаги (действия):

На вход БСОР подаются сведения об отправителе и адресате контента, а также само сообщение и результат работы модуля анализа с оценкой критерия «уровень деструктивности контента» (К23).

Осуществляется обращение к БД, содержащей оценки надежности отправителей сообщений, соответствующие значениям критериев «уровень доверия источника» (К211) и «уровень охвата источника» (К212). Если значения для конкретного отправителя в БД отсутствуют, значения критериев получают наивысшее значение риска (К211 = 4; К212 = 4).

С помощью заданной матрицы свертки из значений критериев К211 и К212 получается оценка критерия К21.

Для формирования оценки критерия «возрастной показатель целевой аудитории» (К22) БСОР проверяет возраст получателей. В случае если получателей несколько (например, при публикации поста в сообществе), формируется массив возрастов получателей. Значение каждого элемента массива сравнивается с диапазонами критерия К22, сопоставляя им определенное значение риска.

Из значений оценок критериев К21, К22 и К23 с помощью трех матриц свертки формируется три значения интегрального критерия, из которых выбирается показатель с максимальным значением риска.

Далее БСОР по заранее установленному правилу принимает одно из следующих решений: переслать сообщение на дополнительную (усиленную) проверку на наличие деструктивного контента; разрешить отправку сообщения потребителям; заблокировать отправку сообщения; или направить сообщение модератору на дополнительную проверку. На усиленную проверку сообщения могут направляться, например, при наличии повышенного (но не максимального) уровня интегрального риска (например, К1 = 3). Если усиленная проверка не выявит деструктивного контента, а новое значение К1 не станет ниже предыдущего, сообщение может быть направлено на проверку модератору. Если отправка сообщения блокируется из-за наличия негативного контента, отправителю присваивается повышенное значение критерия «уровень риска» К211 (вплоть до К211 = 4 – не заслуживающий доверия источник).

Таким образом, оценка рисков в задаче выявления и блокирования деструктивного контента в социальных сетях позволяет вводить дополнительные метрики для оценки значений параметров, связанных с передаваемым сообщением (как между двумя лицами, так и в адрес неограниченного круга пользователей). Внедрение блока системы оценки рисков, алгоритм работы которого описан в настоящей статье, в состав типовой системы обнаружения деструктивного контента теоретически позволяет сократить количество обращений к модератору, используя значения показателей доверия для отправителя (в виде отдельной БД), осуществлять стратификацию и агрегацию категорий деструктивного контента в зависимости от уровня его угрозы, а также осуществлять контроль возраста целевой аудитории.

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 18-29-22104

Литература:

1. *Kulagina I., Iskhakov A.* Problems of Automation of the Aggression Analysis in Socio-Cyberphysical Environment / Proceedings of the 8th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2020). – Advances in Intelligent Systems Research. – 2020. – Volume 174. – P. 35-40.

2. *Охапкин В.П., Охапкина Е.П., Исхакова А.О., Исхаков А.Ю.* Деструктивное информационно-психологическое воздействие в социальных сетях // Моделирование, оптимизация и информационные технологии. – 2020. – №8(1). – С. 1-14.

3. *Новиков Д.А.* Теория управления организационными системами. – М.: Издательство физико-математической литературы, 2012. – 604 с.

Боресков Г.К.

Этические аспекты применения инструментов искусственного интеллекта для обеспечения пространства доверия в электронных СМИ

Аннотация: В работе рассматриваются специфические риски этического характера, связанные с применением инструментов искусственного интеллекта для обеспечения безопасного коммуникационного пространства доверия на площадках электронных СМИ.

Ключевые слова: социальные сети, электронные СМИ, инструменты искусственного интеллекта, безопасность, доверие

За последнее десятилетие рынок телевизионного вещания в Российской Федерации претерпел значительные изменения. Телевизионные информационные программы теряют привлекательность для современной аудитории, в то же время существенно возрастает популярность разного рода интернет-сервисов. Эту тенденцию отражают, например, результаты

исследования фонда Общественное мнение «Допускает ли ТВ-аудитория переключение на другие источники информации?» [1].

В ситуации стремительного развития социальных сетей, миграции аудитории от телевидения в сторону онлайн потребления контента «по запросу» и технического проникновения широкополосного интернета во многие отдаленные регионы страны одним из наиболее перспективных направлений развития вещания становится формирование трансмедийных суперплатформ (далее – ТМСП), способных охватить как все доступные среды современной медиакоммуникации, так и большинство социально-демографических слоев населения и доставить контент до пользователя, где бы он не предпочитал получать его в эпоху гибридного телесмотрения. Эффективность такого подхода подчеркивается в работе Дженкинса, Форда и Грина «Spreadable media: Creating value and meaning in a networked culture» [2].

В силу высокой конкуренции поставщиков контента как в сфере телевидения, так и в сферах социальных сетей и мобильных платформ, вещание ТМСП должно максимально соответствовать явным и неявным запросам и предпочтениям аудитории, не только оперативно адаптироваться к возникающим информационным трендам, но и целенаправленно порождать их, не искать свою зрительскую нишу, а постоянно расширять ее, одновременно привлекая новых зрителей и удерживая имеющихся.

Обеспечить это возможно с использованием модулей искусственного интеллекта, функционал которых предусматривает:

- выявление нарождающихся информационных трендов, подготовку рекомендаций по формированию контента, направленного на расширение аудитории на волне тренда;
- анализ представительства аудитории в социальных сетях, сегментирование и кластеризацию, выявление лидеров мнений и горизонтальных связей;
- выявление факторов, определяющих реакцию аудитории на демонстрируемый контент, дающее возможность существенно повысить востребованность контента, проектируя его в соответствии с этими факторами, отражающими предпочтения аудитории;

- выявление связей между характеристиками просматриваемого контента и динамикой мнений и предпочтений зрителей.

При этом адресное донесение до пользователя ТМСП востребованного им информационного контента будет эффективным только при условии доверия пользователя к этой платформе, обеспечение которого является еще одним важным направлением применения инструментов искусственного интеллекта в сфере трансмедийного вещания. Традиционно используемые для этого инструменты, основанные на объединении технологий модерации и краудсорсинга исследуются в книге Тарлтона Гиллеспи «Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media» [3]. Эти инструменты имеют ряд существенных ограничений, включая:

- риски предвзятых, либо тенденциозных действий модераторов, разрушающих доверие участников к коммуникационному пространству – эта тенденция стала основной темой статьи Джоан Донаван «Why social media can't keep moderating content in the shadows» [4];
- высокую сложность идентификации целенаправленно спланированных масштабных манипулятивных информационных воздействий среди множества случайных «вбросов» обычных пользователей без применения специального инструментария, функционирующего на постоянной основе в автоматическом режиме;
- невозможность без такого инструментария определить потенциал распространения и конечный эффект манипулятивных воздействий.

Таким образом, ключевым инструментом обеспечения пространства доверия в информационной среде ТМСП должна стать информационная система, способная в режиме автоматизированного мониторинга средств массовой электронной коммуникации выявлять манипулятивные информационные воздействия, прогнозировать развитие линии распространения информации и определять источники и «слабые точки» таких линий, что создает возможности не только управляемого купирования негативных воздействий, но и своевременного

принятия этичных и не вызывающих отторжения у участников информационной среды превентивных мер.

Эти система должна объединять в себе автоматизированные средства мониторинга соцсетей, анализа больших данных и выявления информационных воздействий на основе алгоритмов искусственного интеллекта, решая задачи:

- многовекторного анализа эмоционального контекста социальных сетей;
- выявления и типизации линий воздействия;
- предотвращения информационных угроз и реагирования на случаи их реализации.

Важно не забывать, что пространство доверия может обеспечиваться не только нивелированием случайных и целенаправленных манипулятивных воздействий, но и путем расширения доступа его участников к достоверной информации, предоставления им инструментов ее структурирования и достижения консенсуса, для чего также могут быть применены инструменты искусственного интеллекта. Этот подход предложен в статье А.Н. Райкова «Accelerating technology for self-organising networked democracy» [5]. При этом соблюдение этических норм, очевидно, становится одним из ключевых факторов для создания среды доверия в медиа-пространстве.

Это ставит ряд задач в сфере этических аспектов применения искусственного интеллекта в медиа-среде, среди которых:

- разработка методик классификации этических рисков при применении инструментов искусственного интеллекта в медиа-среде, их идентификации и предотвращения;
- прогнозирование последствий разработки, внедрения и использования инструментов искусственного интеллекта в сфере электронных средств массовой информации и массовой коммуникации;
- определение базовых ценностей и этических ориентиров для различных акторов искусственного интеллекта в медиа-среде.

В качестве одного из базовых ориентиров для этой работы может быть взято «Предварительное исследование возможности подготовки нормативного акта по вопросам этики применения искусственного интеллекта», подготовленное Рабочей группой КОМЕСТ [6] – всемирная комиссия по этике научных знаний и

технологий КОМЕСТ является консультативным органом и форумом для размышлений, учрежденным ЮНЕСКО в 1998 г. В документе подчеркивается: «Искусственный интеллект играет все более важную роль в обработке, структурировании и предоставлении информации. Автоматизированная журналистика и алгоритмические новостные ленты в социальных сетях – лишь некоторые из примеров этой тенденции, в связи с которой возникают вопросы доступа к информации, дезинформации, дискриминации, свободы выражения мнений, неприкосновенности частной жизни, а также медийной и информационной грамотности».

Мы можем выделить ряд этических рисков, специфических именно для сферы применения инструментов искусственного интеллекта в СМИ:

- усугубление поляризации мнений в результате формирования алгоритмами медиа-среды так называемых «фильтрующих пузырей» и «эхо-камер». Пользователи, попадающие в один и тот же «пузырь», могут не только подвергаться воздействию потока единообразным образом отфильтрованной информации, но также коммуницировать в основном друг с другом. Это приводит к заполнению медиа-среды все более однородными группами сторонников того или иного мнения, занимающими при этом все более полярные и радикальные позиции по отношению друг к другу. В ряде случаев развитие подобных тенденций может привести даже к серьезной дестабилизации общества, например, подорвав доверие к обнародованным результатам выборов у пользователей, необоснованно экстраполировавших предпочтения своих «друзей» в социальных сетях (в большинстве, близких им по политическим взглядам) на всех избирателей. Вопросы политической поляризации, в том числе, как результат взаимодействий в социальных сетях подробно рассматриваются в работе «Political sectarianism in America» [7];
- тенденциозность и предвзятость при модерации пользовательского контента, приоритизации результатов поисковой выдачи и формировании подборок новостей, что может повлечь обвинения в автоматизированной цензуре и неправомерных ограничениях свободы слова;

- превращение алгоритмов, производящих отбор и первичную обработку информационных материалов для редакции современного СМИ, из инструмента, кардинально облегчающего и ускоряющего выполнение рутинных операций, в своего рода фильтр, искажающий реальную картину мира для самих сотрудников редакции. Это можно рассматривать как более радикальный вариант «фильтрующего пузыря»;
- расфокусировка редакционной политики и деградация имиджа СМИ в результате «гиперадаптации» контента к актуальным информационным трендам и предпочтениям аудитории, выявленным с помощью инструментов искусственного интеллекта.

Речь идет о том, что стремление редакции любого СМИ к расширению аудитории может быть существенно усилено рекомендациями алгоритмов искусственного интеллекта.

Литература:

1. Фонд «Общественное мнение». Допускает ли ТВ-аудитория переключение на другие источники информации? 06 Февраля 2021 – URL: https://fom.ru/SMI-i-internet/14536 (дата обращения 15.10.2021).

2. *Jenkins H., Ford S., Green J.* Spreadable media: Creating value and meaning in a networked culture. – N.Y.: New York University Press, 2013. – 352 p.

3. *Tarleton Gillespie.* Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. – New Heaven, CT: Yale University, 2018. – 298 p.

4. *Joan Donovan.* Why social media can't keep moderating content in the shadows // MIT Technology Review. – November 6, 2020.

5. *Raikov A.* Accelerating technology for self-organising networked democracy // Futures. – October 2018. – Volume 103. – P. 17-26. – URL: https://www.sciencedirect.com/science/article/abs/pii/S0016328717302380 (дата обращения 14.10.2021).

6. COMEST Extended Working Group on Ethics of Artificial Intelligence. Preliminary study on the Ethics of Artificial Intelligence (COMEST) (26 February 2019 Paris). – URL: https://unesdoc.unesco.org/ark:/48223/pf0000367823 (дата обращения 15.10.2021).

7. *Eli J. Finkel, Christopher A. Bail, Mina Cikara, Peter H. Ditto, Shanto Iyengar, Samara Klar, Lilliana Mason, Mary C. McGrath, Brendan Nyhan, David G. Rand, Linda J. Skitka, Joshua A. Tucker, Jay J. Van Bavel, Cynthia S. Wang, James N. Druckman.* Political sectarianism in America // Science. – 30 Oct 2020. – Vol. 370. Issue 6516. – P. 533-536.

Охапкина Е.П.

Разработка динамической системы функционирования сообществ социальной сети

Аннотация: Протекающие в сообществе социальной сети процессы показаны в виде системы дифференциальных уравнений первого порядка. Рассмотрена имитационная модель построенной исследованной динамической системы при различных начальных условиях имитации.

Ключевые слова: дифференциальные уравнения, социальные сетевые сервисы, системная динамика, информационно-коммуникационные технологии, имитационное моделирование

Примем, что в рамках моделирования предметной области для системы сообществ социальной сети (далее ССС) определены три обязательных параметра:

1. L – общее количество отметок «нравится» (так называемых «лайков» (‘like’) на внутреннем сленге аудитории сообщества социальной сети) за анализируемый период времени t.
2. P – общее количество подписчиков (постоянных читателей) для ССС за анализируемый период времени t.
3. S – общее количество сообщений в ССС вне зависимости от адресатов и получателей за анализируемый период времени t.

Каждый из приведенных параметров участвует в процессах системы ССС. Таким образом, для каждого параметра может быть определен закон его изменения, который в рамках математической постановки будет представлен характеристическим уравнением.

Пусть l_i – количество отметок типа ‘like’ для одной произвольной записи («поста») сообщества социальной сети. Тогда

параметр L может быть определен как сумма отметок типа «like» для всех записей («постов») ССС, имеющей вид (1).

$$L = \sum_{i=1}^{n} l_i, \tag{1}$$

где n – количество записей в ССС за анализируемый период времени t, i – порядковый номер записи.

Размер постоянной аудитории ССС напрямую зависит от уровня интереса и привлекательности публикаций, поставляемых сообществом. В качестве параметра, определяющего читательский интерес аудитории ССС, предлагается использовать введенный ранее показатель l_i. Пусть l_j количество посетителей, ставших подписчиками целевого ССС после просмотра одной произвольной публикации. В этом случае параметр P может быть определен в виде записи (2).

$$P = \frac{\sum_{i,j=1}^{n,m} l_i p_j}{\gamma}, \tag{2}$$

где m – количество наборов посетителей, ставших подписчиками после просмотра одной произвольной публикации; j – порядковый номер публикации; γ – коэффициент негативного восприятия публикации j аудиторией, который может быть интерпретирован как доля негативных отзывов/комментариев о публикации j, , при этом $\gamma \in [1,...,9]$.

Для описанного набора параметров предполагается зависимость вида (3)

$$\gamma \to 0 \Rightarrow P \to \infty \tag{3}$$

Таким образом, очевидно, что наименьший коэффициент негативного восприятия публикации j аудиторией приводит к увеличению числа посетителей, ставших подписчиками сообщества после прочтения публикации j.

В рамках математического моделирования предметной области предполагается, что в ССС возможность обмена сообщениями доступа руководству и пользователям, которые имеют статус подписчиков сообщества. Пусть s – количество сообщений, инициируемых одним подписчиком сообщества, а r – количество сообщений, инициируемых одним членом руководства сообщества. Далее предположим, что каждый из подписчиков и членов

руководства сообщества может с некоторой вероятностью h начать обмен сообщениями. В этом случае для параметра S следует считать справедливым равенство вида (4).

$$S = \frac{(P_S + R_r)h}{\mu} - \vartheta, \tag{4}$$

где $R \in N$ – количество членов руководства сообщества; μ – технический коэффициент загруженности сети, $\mu \in (1,...,1.8]$; ϑ – доля погрешности или количество сообщений, не дошедших до адресата ввиду проблем на технической стороне сети.

Для всех ранее определенных параметров ССС могут быть установлены взаимозависимости, описываемые дифференциальными уравнениями.

Количество отметок типа ‘like’ в сообществе зависит от качества и характера восприятия аудиторией поставляемых сообществом публикаций. С учетом данного фактора, предлагается описать закон изменения общего количества «лайков» через коэффициенты негативного и положительного восприятия постоянной аудиторией генерируемого сообществом контента. Введение нового коэффициента положительного восприятия публикаций аудиторией позволяет описать закон изменения отметок типа ‘like’ в виде уравнения (5).

$$\frac{dL}{dt} = \omega(L + P + S) - \gamma L, \tag{5}$$

где $\omega = [1,...,9]$ – коэффициент положительного восприятия аудиторией публикаций сообщества.

В данном случае предполагается, что отметки типа «нравится» могут выставлять только участники, являющиеся подписчиками сообщества. В данном случае количество сообщений S следует считать косвенным показателем активности аудитории, ввиду чего в законе изменения количества отметок типа «нравится» значение данного параметра учитывается наравне с количеством подписчиков P.

В рамках моделирования предполагается, что размер постоянной аудитории будет изменяться в зависимости от общего числа отметок типа ‘like’, а общее количество сообщений в сообществе никаким образом не влияет на размер постоянной аудитории, что может быть описано уравнением вида (6).

$$\frac{dP}{dt} = \omega L - 2\gamma P, \tag{6}$$

В данном случае влияние коэффициента негативного восприятия публикаций будет иметь вдвое большее значение, поскольку он является определяющим в решении читателя публикации стать членом постоянной аудитории ССС.

Подразумевается, что в ССС обмен сообщениями могут инициировать только подписчики и члены руководства сообщества. В этом случае закон изменения общего количества сообщений будет описан уравнением вида (7).

$$\frac{dS}{dt} = RP - \frac{\omega L}{\gamma}, \tag{7}$$

Все описанные законы изменения для каждого из целевых параметров дают возможность описать процессы ССС в виде системы дифференциальных уравнений первого порядка, которая выражает баланс между доступными параметрами ССС. Таковая система уравнений записана в виде (8).

$$\begin{cases} \dfrac{dL}{dt} = \omega\left(L + P + S\right) - \gamma L \\ \dfrac{dP}{dt} = \omega L - 2\gamma P \\ \dfrac{dS}{dt} = RP - \dfrac{\omega L}{\gamma} \end{cases} \tag{8}$$

Система (8) может быть представлена в наиболее традиционном представлении, для этой цели предлагается произвести следующие замены:

$L \to x$

$P \to y$

$S \to z$

В этом случае исходная система будет иметь вид (9)

$$\begin{cases} \dfrac{dx}{dt} = \omega\left(x + y + z\right) - \gamma x \\ \dfrac{dy}{dt} = \omega x - 2\gamma y \\ \dfrac{dz}{dt} = Ry - \dfrac{\omega x}{\gamma} \end{cases} \tag{9}$$

Воспользуемся системой имитационного моделирования iThink v.8.0 [1] для оценки динамики развития основных показателей (9) при различных начальных условиях. На рисунке 1 показан ориентированный граф имитационной модели соответствующий динамической системе (9).

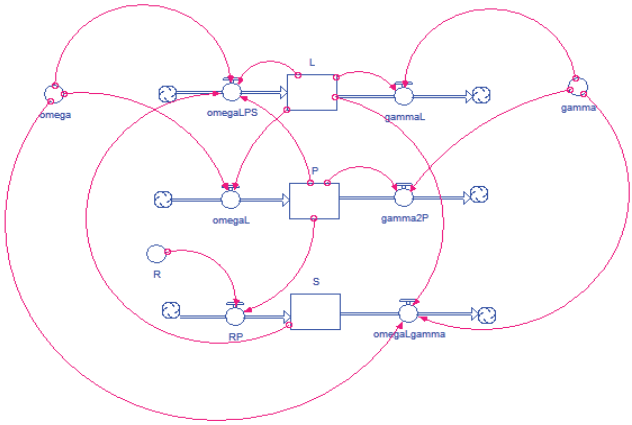


Рисунок 1 – Ориентированный граф динамической системы

Рассмотрим несколько сценариев развития процессов изменения количества отметок «like» (L), подписчиков (P) и сообщений (S). В таблице 1 покажем начальные условия для первого сценария.

Таблица 1 – Начальные условия сценария

Параметр	Значения		
	Первый сценарий	Второй сценарий	Третий сценарий
L	100000	10000	500000
P	10000	1000	1000000
S	20000	2000	500000
ω	1.1	1.1	0.9
γ	2.5	2.5	1.0
R	5	5	1

Для решения в численном виде воспользуемся методом Runge-Kutta 4, наиболее точным методом доступным в iThink. В качестве временной шкалы укажем условные временные единицы. На рисунке 2 можно видеть динамику изменения показателей L, P and S для начальных условий первого сценария.

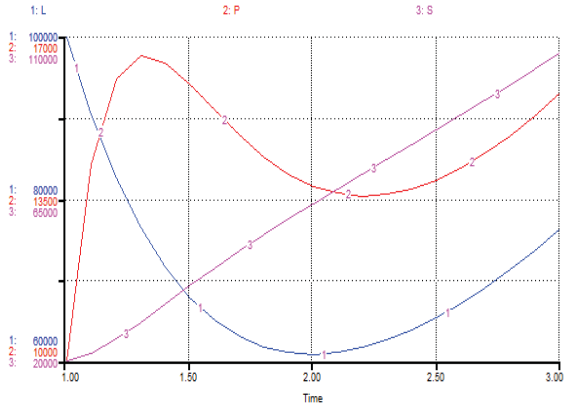


Рисунок 2 – Динамика развития процессов в условном масштабе времени

Наблюдение нестабильных режимов работы динамической системы для рассматриваемого объекта моделирования, с одной стороны, кажется предсказуемым: множество отдельно действующих пользователей. Но, с другой стороны, даже большое

количество пользователей объединяют единые оценки высказываний, что дает повод о том, что формирование мнений на виртуальной площадке возможно. Считаю перспективным также рассмотреть подход, связанный с созданием динамической системы основанной на мультиагентном моделировании. В таком подходе формирование отклика со стороны пользователя подчинено его деятельности в малой группе большого сообщества социальной сети. В этом смысле, малая группа выступает с двух позиций: как агент формирования мнения и его транслирования на общую аудиторию и, в то же время, является агентом сообщества, воспринимающим чужое мнение извне.

Исследование выполнено при финансовой поддержке РФФИ в рамках научно-исследовательского проекта № 18-29-22104 «Разработка социально-киберфизической системы мониторинга разнообразного интернет-контента для противодействия проявлению агрессии, давления и других форм деструктивного воздействия на индивидуальное и групповое сознание пользователей»

Литература:

1. *Якимов И.М., Кирпичников А.П., Устинов Р.Д., Спиридонов Г.В.* Имитационное моделирование в системе структурного и имитационного моделирования "ITHINK" // Вестник Технологического университета. – 2019. – Т. 22. №. 2. – С. 159-164.

V. Экологическая и техногенная безопасность

Мещеряков Р.В.

Подход к защищенному интеллектуальному управлению роботами и их коалициями с использованием интерфейса человек-робот(ы) и робот-робот(ы)

Аннотация: Рассмотрен подход к защите обеспечения каналов управления и формирования коалиции роботов при использовании различных интерфейсов. Предлагается обеспечивать типовые решения за счет введения функций интеллектуализации при принятии решения. Предлагается использование различных интерфейсов для резервирования каналов связи при подаче команд и получения обратной связи от объектов управления.

Ключевые слова: кибербезопасность, защита информации, интерфейсы, коалиция, интернет вещей

Введение

Развитие интеллектуальных робототехнических систем в современном мире оказывает значительное влияние на другие отрасли науки и промышленности. В настоящее время количество роботов, задействованных не только в промышленности, но и в быту, стремительно увеличивается. Современные робототехнические системы зачастую представляют собой распределенные децентрализованные системы, для обеспечения работоспособности которых необходима связь между их отдельными элементами, в том числе беспроводная. Связь между элементами робототехнических систем может быть реализована через межмашинное взаимодействие, в том числе в рамках концепции интернета вещей (Internet of Things, IoT). В настоящее время происходит глубокая интеграция интеллектуальных робототехнических систем и IoT-инфраструктуры. Однако это приводит к появлению проблемы, не имеющей на данный момент полноценного решения. Массовое использование интернета вещей,

как в робототехнике, так и в иных отраслях, затруднено теми проблемами безопасности, которыми обладает данная концепция.

Вмешательство злоумышленников в управление роботами и группами роботов может не только воспрепятствовать выполнению тех задач, для решения которых используются роботы, и в связи с этим привести к финансовым потерям, но и создать угрозы для жизни и здоровья людей. Поэтому крайне актуальной становится проблема формирования защищенных механизмов межмашинного обмена данными при управлении робототехническими системами.

Ситуация осложняется тем, что на сегодняшний день не существует стандартов безопасности для робототехнических систем и типовых систем управления с использованием человеко-машинных интерфейсов. Наследование робототехническими системами уязвимостей, характерных для IoT-инфраструктуры, не позволяет применять традиционные меры обеспечения безопасности, в частности, из-за ограниченной вычислительной мощности и других характерных особенностей исследуемых устройств. В отличие от компьютеров и смартфонов, значительная часть IoT-устройств не способна применять средства защиты от вредоносного программного обеспечения из-за отсутствия инфраструктуры для запуска подобных приложений. С другой стороны, разработка интерфейсов при участии человека требует решения проблем удаленного взаимодействия с реальными и виртуальным робототехническими системами, в частности, ограничения информации по каналу связи устройство-человек. При использовании существующих каналов связи отсутствуют тактильные и ряд звуковых данных, а видео-информация представляется в урезанном виде по сравнению с непосредственным наблюдением как за управляемой системой, так и за другими пользователями, осуществляющими либо управление этой же системой (разделение операторских функций) либо же другими системами в общем пространстве.

Отдельную сложность проблемам безопасности робототехнических систем независимо от используемых технологий связи и методов управления придает увеличение числа одновременно взаимодействующих единиц, обусловленное постоянным технологическим ростом робототехнической отрасли. Это приводит к появлению принципиально новых угроз

безопасности. Для того, чтобы вмешаться в работу коалиции роботов, злоумышленнику достаточно получить возможность управлять отдельными представителями коалиции и за счет этого организовать деструктивное воздействие на систему в целом.

Состояние исследований

Робототехника применяется в различных сферах человеческой деятельности и их количество год от года стремительно увеличивается. Происходит стремительная интеграция роботов в инфраструктуру интернета вещей. Например, в работе [1] предлагается структура, обеспечивающую беспрепятственную связь между интеллектуальными домашними устройствами и роботами.

Большое количество исследований направлено на разработку алгоритмов управления роботами [2-6]. Многие задачи способны эффективно решаться только при групповом взаимодействии роботов. Модели группового поведения, в частности, коалиций роботов, рассмотрены в [7]. Согласно [7], коалиции образуют агенты (роботы), которые могут объединять свои ресурсы для решения сложных задач. В [8] рассмотрена модель координации роботов на основе клеточных автоматов. В [9] с помощью клеточных автоматов моделируется коллективное взаимодействие агентов для совместного преодоления препятствий.

В работе [10] подробно рассмотрены аспекты группового взаимодействия гетерогенной группы роботов, т.е. роботов с различным устройством, алгоритмами управления и задачами, а также наличием централизованного автоматического управления каждой гомогенной подгруппой. Авторы отмечают, что групповое управление должно осуществляться с минимальным участием человека, поэтому необходимо применение механизмов интеллектуального управления.

Вопросы интеллектуального управления рассмотрены в [11]. В данной работе предлагается подход к взаимодействию пользователей и роботов с помощью онтологий для совместного решения задач. Онтологии публикуются в интеллектуальном пространстве, позволяющем пользователям и роботам осуществлять непрямое взаимодействие. Пользователи и роботы формируют и публикуют задачи, роботы определяют задачу, объединяются в

коалицию для ее выполнения и распределяют подзадачи в рамках этой коалиции.

Авторы [12] сфокусированы на работе нескольких агентов с точки зрения интерактивного интеллектуального пространства. В основе архитектуры управления лежит обеспечение локализации и надежного отслеживания.

Обзор большого числа архитектур интеллектуального управления приводится в статье [13]. Среди них иерархическая, поведенческая и другие архитектуры. В работе [14] представлен частный случай архитектуры интеллектуального управления, основанной на взаимодействии человека с роботом для помощи в детской реабилитации.

Постановка задачи и обсуждение

Для выявления наиболее проблемных участков в информационном взаимодействии элементов робототехнических систем, подверженных отказам, была построена классификация возможных отказов и нарушений в воздействии на данные и команды управления, передаваемые в интеллектуальных робототехнических системах, функционирующих с использованием технологии интернета вещей. В частности, было установлено, что уникальные особенности построения группы роботов затрудняют использование существующих механизмов обеспечения информационной безопасности и предоставляют возможность злоумышленникам для воздействия на роевые алгоритмы (адаптивное поведение) [15].

В качестве основных механизмов реализации атак были выделены физические атаки на группы робототехнических устройств; атаки на каналы связи; затруднение идентификации и аутентификации агентов-роботов в системе; внедрение сторонних устройств в коалицию (в том числе перепрограммированные злоумышленником легитимных роботов) [15].

Было установлено, что интерфейсы взаимодействия роботов с человеком требуют решения проблем удаленного взаимодействия с реальными и виртуальным робототехническими системами, в частности, ограничения информации по каналу связи устройство-человек. При использовании существующих каналов связи отсутствуют тактильные и ряд звуковых данных, а видео

информация представляется в урезанном виде по сравнению с непосредственным наблюдением как за управляемой системой, так и за другими пользователями, осуществляющими либо управление этой же системой (разделение операторских функций), либо же другими системами в общем пространстве [16].

Одним из решений защищенного управления отдельными интеллектуальными роботами и их коалициями представляет собой применение алгоритмов шифрования каналов связи; многофакторной аутентификации; средств управления доступом, мониторинга, защиты от установки вредоносного программного обеспечения (в том числе на этапах инициализации новых версий ПО), локального и централизованного поиска уязвимостей, исправления и управления конфигурациями агентов.

Заключение

Проведенные исследования показали, что требуется разработка модели безопасности интеллектуальных робототехнических систем, функционирующих с использованием интерфейса интернета вещей. Базовые механизмы обеспечения защищенности должны учитывать особенности использования интерфейса интернета вещей при выполнении основных сценариев выполнения индустриальных задач робототехнических комплексов прикладного назначения. Алгоритм для модели управления измерительными компонентами, позволяет получить в необходимые моменты времени совокупность оценок измеряемых физических величин, показателей их точности, а также устранить систематические погрешности. Полученные оценки величин могут быть использованы в качестве априорной информации в принятии управленческих решений. Используемые модели управления для мониторинга, построенные на концепции интернета вещей, обладают преимуществами: взаимодействие измерительных компонент без вмешательства человека и возможность быстрого реагирования при изменениях каких-либо параметров окружающей среды, в частности для задач [17]. Оригинальность разработанной модели заключается в учете таких факторов, как помехоусточивость измерительных каналов, отказоустойчивость системы в целом, воспроизводимость эталонного сигнала, а также единый формат передачи

измерительной информации, который воспринимают все компоненты системы в целом.

Исследование выполнено при частичной финансовой поддержке гранта РФФИ № 19-08-00331

Литература:

1. *S.M. Nguyen, C. Lohr, P. Tanguy, Y. Chen.* Plug and Play your Robot into your Smart Home: Illustration of a New Framework // KI – Künstliche Intelligenz. – 2017. – Vol. 31. № 3. – P. 283-289.

2. *Павловский В.Е.* Эвристический алгоритм обнаружения изолированных препятствий мобильным роботом по дальномерным данным // Искусственный интеллект и принятие решений. – 2016. – №4. – С. 93-105.

3. *Филимонов А.Б., Филимонов Н.Б.* Некоторые аспекты автоматизации систем управления беспилотными мобильными средствами // Мехатроника, автоматика и робототехника. – 2018. – № 2. – С. 35-38.

4. *Атакищев О.И., Титенко Е.А., Скорняков К.С., Заичко В.А., Риос А.П.* Модель и методы управления сложными техническими объектами на основе продукционной парадигмы // Известия ЮФУ. Технические науки. – 2012. – №3(128). – С. 181-187.

5. *Визильтер Ю.В., Вишняков Б.В., Выголов О.В., Горбацевич В.С., Князь В.А.* Технологии интеллектуальной обработки информации для задач навигации и управления беспилотными летательными аппаратами // Труды СПИИРАН. – 2016. – №2(45). – С. 26-44.

6. *Лохин В.М., Манько С.В., Романов М.П.* Развитие технологий применения аппарата теории автоматов для управления многоагентными робототехническими системами // Робототехника и техническая кибернетика. – 2016. – №2(11). – С. 3-7.

7. *Карпов В.Э.* Модели социального поведения в групповой робототехнике // Управление большими системами: сборник трудов. – 2016. – № 59. – С. 165-232.

8. *C.R. Tinoco, D.A. Lima, G.M.B. Oliveira.* An improved model for swarm robotics in surveillance based on cellular automata and repulsive pheromone with discrete diffusion // International Journal of Parallel, Emergent and Distributed Systems. – 2017 (2019). – Volume 34. Issue 1. – P. 53-77. doi: 10.1080/17445760.2017.1334886

9. *Kuznetsov A.V.* A Model of the joint motion of agents with a three-level hierarchy based on a cellular automaton // Computational Mathematics and Mathematical Physics. – 2017. – Vol. 57. № 2. – P. 340-349.

10. *Васильев И.А., Половко С.А., Смирнова Е.Ю.* Организация группового управления мобильными роботами для задач специальной робототехники // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2013. – № 1 (164). – С. 119-123.

11.*Петров М.П., Кашевник А.М.* Онтолого-ориентированный подход к непрямому взаимодействию пользователей и роботов для совместного решения задач // Научный вестник НГТУ. – 2017. – Т. 66. №1. – С. 133-146.

12.*D. Kim, K.H. Jeong, B.H. Lee.* An approach to multi-agent interactive control in an intelligent space // International Journal of Control, Automation and Systems. – 2015. – Vol. 13. № 3. – P. 697-708.

13.*Tzafestas S.G.* Mobile robot control and navigation: a global overview // Journal of Intelligent & Robotic Systems. – 2018. – Vol. 91. – P. 35-58. doi: 10.1007/s10846-018-0805-9

14.*S.F. dos Reis Alves, H. Ferasoli.* Intelligent control architecture for assistive mobile robots // Journal of Control, Automation and Electrical Systems. – 2016. – Vol. 27. № 5. – P. 515-526.

15.*Туровский Я.А., Харченко С.С., Мещеряков Р.В., Исхаков А.Ю., Исхакова А.О.* Алгоритмическое обеспечение интерфейса управления робот-человек при выделении зрительных вызванных потенциалов на основе многомерного индекса синхронизации // Известия ЮФУ. Технические науки. – 2020. – № 1 (211). – С. 66-78.

16.*Мещеряков Р.В., Исхаков А.Ю., Евсютин О.О.* Современные методы обеспечения целостности данных в протоколах управления киберфизических систем // Информатика и автоматизация. – 2020. – Т. 19. № 5. – С. 1089-1122.

17.*Ананьев П.П., Плотникова А.В., Тимофеев А.С., Мещеряков Р.В., Беляков К.О.* Проблемы тестирования робототехнических систем для перемещения по космическим объектам // Робототехника и техническая кибернетика. – 2021. – Т.3. № 9. – 180-185.

Абросимов В.К., Райков А.Н.

Ситуационная осведомленность для безопасной и эффективной работы агророботов

Аннотация: Предложено использовать подход ситуационной осведомленности, который ранее использовался преимущественно в условиях чрезвычайных и нештатных ситуаций, для обеспечения безопасности и эффективной работы агророботов на полях. Сформулирован состав параметров, определяющих поведение агророботов, определен состав необходимых исходных данных.

Ключевые слова: агроробот, большие данные, искусственный интеллект, ситуационная осведомленность

Подход под названием «ситуационная осведомленность» (СО) получил свое наиболее полное содержательное оформление после известных терактов 11 сентября 2001 г. и крушения в 2009 г. самолета Airbus A330. Этот подход был предложен и использован при исследовании таких бедствий [1,2].

Дальнейшее развитие подхода осуществлялось в рамках обеспечения работы групп людей в чрезвычайных обстоятельствах, например, при тушении пожаров, устранении последствий катастроф на транспорте, управлении самолетом в нештатном режиме и пр. [3].

Процесс СО охватывает отдельных лиц, группы людей, системы искусственного интеллекта, компьютеры и пр. Его реализация включает несколько этапов [1,3], имеет градацию по уровням и характеризуется различными моделями. Этот процесс может иметь аномальное поведение, которое определяется как непредвиденное отклонение от намеченного плана при некоторых обстоятельствах.

Системы СО не всегда ведут себя устойчиво и целенаправленно. Некоторые исследования представляют неформализованные когнитивные процессы, связывая участников с системами ИИ, и делая тем самым систему гибридной. Это подразумевает передачу между акторами системы СО информации в специальных шаблонах с синергетической интеграцией их

возможностей [4]. Непредсказуемые и ложные сообщения также возможны [5].

Под этот подход созданы специальные системы поддержки решений на основе инструментов виртуальной реальности и искусственного интеллекта (ИИ). И если в начале 2000-х считалось, что для реализации системы СО достаточно погружения акторов в виртуальную реальность с предоставлением каждому наиболее полной информации, в том числе для корректной и скоординированной ориентации каждого в пространстве и времени, то позже потребовалось разработать специальные фреймворки для ускорения взаимопонимания участников в нештатных ситуациях. Пример такого фреймворка показан на рисунке 1 [3].

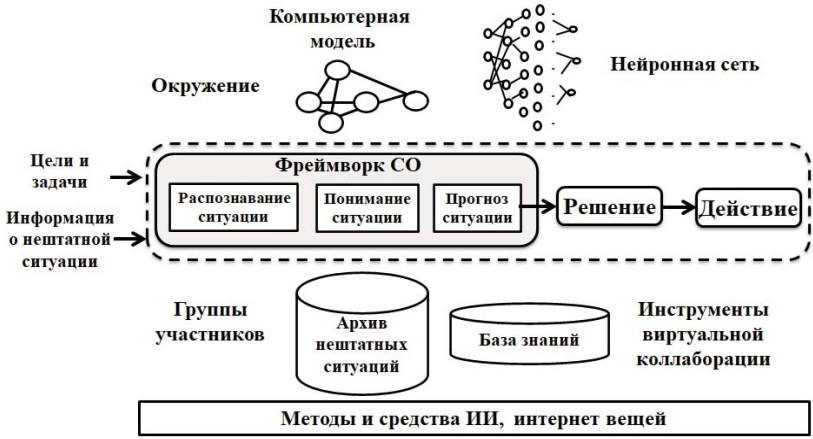


Рисунок 1 – Фреймворк СО во внешнем контексте

Принято считать, что СО является подходящей структурой для коллективного компьютерного моделирования, которая помогает быстро принимать эффективные решения с использованием явной и неявной информации.

Вместе с тем, применение этого подхода и инструментария, который за ним стоит, могут быть диверсифицированы и для условий, казалось бы, далеко стоящих от экстремальной обстановки. Например, этот подход может быть использован для

реализации требований обеспечения безопасности использования агророботов, функционирующих на сельскохозяйственном поле.

Агроробот должен быть ситуационно осведомлен [6]. Для выполнения даже самых простых заданий ему требуется совсем немного информации, например, маршрут перемещения и программа действий навесного оборудования. Однако в близкой перспективе при работе на большом поле нескольких агророботов и людей необходимо будет использовать подход СО.

В общем случае система СО агроробота – это совокупность, состоящая из моделей использования ретроспективной научной и нормативной информации о растениеводстве, представления данных о погоде, поле и решаемых задачах, моделей обработки поступающей от системы интернета вещей и работающих на поле устройств, алгоритмов формирования адекватных реальной полевой ситуации решений.

Учитывая особенности работы агророботов, параметры его СО иные, чем у агронома. Агроробот действует автономно, ему задана некая цель и определены задачи, обладает функционалом, определяются его возможности и ресурсы. В рамках своих ролей агроробот способен действовать и наблюдать окружающую среду лишь в сфере ответственности в силу ограничений собственных систем зрения и навигации. Для перемещения робот задействует систему исполнительных механизмов с датчиками положения, наклона, перемещения и др., активизирующих функции движения: маневр, остановку и др.

Информация, определяющая поведение робота, может быть задана в виде следующей совокупности параметров:

- идентификатор агроробота;
- роль, выполняемая агророботом (взятие проб почвы, мониторинг поля, борьба с сорняками, борьба с вредителями, внесение удобрений);
- маршрут движения агроробота в среде, которая представляется в виде совокупности точек на местности с GPS координатами;
- ценность агроробота и цепочка ценностей;
- точка, где в определенный момент находится агроробот;
- прогнозируемая точка пространства, в которую перемещается агроробот;

- функционал и ресурсы агроробота;
- коэффициент, отражающий степень автономности агроробота;
- скорость движения и ограничительный диапазон;
- диапазон высот работы (для беспилотного летающего агроробота);
- вероятность правильного распознавания болезни растений;
- вероятность правильного распознавания вредителей различного типа и др.

В зависимости от уровня решаемых роботом задач можно ввести понятия ситуационной осведомленности агроробота «в большом» и «в малом». «Ситуационная осведомленность в большом» характеризуется максимальной автономностью, он может вырабатывать самостоятельно и исполнять поступающие команды. Но высокая степень автономности требует, чтобы все задачи (получение информации, анализ, распознавание, прогнозирование ситуации и принятие решения) осуществлялись в формате on-line непосредственно на борту агроробота, что требует значительных вычислительных ресурсов, а также решения безопасности функционирования агроробота как для людей, так и получения урожая.

При «ситуационной осведомленности в малом» агроробот выступает в качестве обеспечивающей роботизированной платформы, носителя навесного оборудования. Здесь главное состоит в обеспечении надежного движения по заданному маршруту. Это требует построения специально организованной информационно-коммуникационной сети.

Существующие облачные решения уже содержат сведения, необходимые для обеспечения СО агроробота: цифровые карты и историю полей, данные метеостанций и др. Физически в облаке формируется база данных с довольно универсальной структурой. В перспективе она может дополняться до больших данных, содержащих и неструктурированную информацию.

В последнее время в России стал использоваться термин «скаутинг» в контексте мониторинга состояния посевов. Агроскаут – специалист агроном-информационщик. Предполагается, что он мониторит около 10 тыс. га, по которым он выезжает на осмотр, контролирует ситуацию, делает рекомендации. Среди зарубежных

программ-аналогов мониторинга полей данный термин фигурирует в наименованиях программ и мобильных приложений – Landscout, Mavrx Scout, Croptivity Scouting Solution, Agworld Scout и др.

Однако, такие данные, например, как текущее положение агроробота на поле, наличие на нем препятствий, взаимное положение относительно других работающих агромашин механизмов и людей на поле, обнаруженные ситуационно при анализе снимков фото- и видеоаппаратуры болезни растений и вредителей зачастую могут быть приобретены лишь в движении самого агроробота.

В перспективе для обеспечения безопасной и эффективной работы гибридной системы с агророботами предстоит определить состав базы необходимых и достаточных данных СО агророботов, осуществить интеграцию по информации и управлению сервисов, предоставляемых агророботами, синхронизацию этих сервисов с сервисами систем агропредприятий. СО агроробота важна не сама по себе, а должна быть частью общей «ситуационной осведомленности агронома» и быть тесно связанной с этой системой по информации и управлению.

В этом контексте эффективным окажется построение системы обеспечения безопасности роботов на сельскохозяйственных полях при использовании концепции Интернета сельскохозяйственных вещей [7]. В результате реализации групповой стратегии управления создается и совершенствуется сетевая сервис-ориентированная инфраструктура взаимодействия сельскохозяйственных машин, включая агророботов, на поле. В группе автономно движущихся роботов в зависимости от происходящих в среде событий и ситуаций возникают и ликвидируются разные связи роботов. Процессы образования новых связей носят спонтанный, заранее неизвестный характер, который определяется складывающейся в среде ситуацией и вновь возникающими событиями. При этом системы роботов, стоящие выше в ролевой иерархии, активизируют системы управления нижестоящих роботов, меняя их роли; если роботы равноправны, то вопросы взаимного управления системами решаются в рамках переговоров на основе принципа коллективизма.

Работа выполнена при поддержке РНФ, проект № 21-18-00184 «Социогуманитарные основания критериев оценки инноваций, использующих цифровые технологии и искусственный интеллект»

Литература:

1. Endsley M.R. Situation awareness in aviation systems / Garland, D.J., Wise, J.A., Hopkin, V.D., eds. Handbook of aviation human factors. – Mahwah, NJ, USA: Lawrence Erlbaum Associates, 1999. – P. 257-276.

2. *Salmon P.M., Walker G.H., Stanton N.A.* Pilot error versus sociotechnical systems failure: a distributed situation awareness analysis of Air France 447. – Theoretical Issues in Ergonomics Science. – 2016. – Volume 17. Issue 1. – P. 64-79.

3. Raikov A.N. Accelerating Decision-Making in Transport Emergency with Artificial Intelligence / Second International Virtual Conference on Multidisciplinary Research 2020. – Advances in Science, Technology and Engineering Systems Journal (ASTESJ). – 2020. – Vol. 5. № 6. – P. 520-530.

4. Crowder J.A., Carbone J.N. Collaborative shared awareness: Human-AI collaboration / International conference on information and knowledge engineering. – Athens: WorldComp, 2014. – P. 1-6.

5. *Illankoon P., Tretten P., Kumar U.* Modelling human cognition of abnormal machine behavior // Human-Intelligent Systems Integration. – 2019. – Vol. 1. – P. 3-26.

6. *Абросимов В.К., Гайдин М.В.* Имитационная модель формирования ситуационной осведомленности группой автономных роботов в условиях потенциальных угроз // Известия ЮФУ. Технические науки. – 2019. – № 1(203). – С. 50-61.

7. *Abrosimov V., Godzhaev Z., Prilukov A.* Agricultural Robots in the Internet of Agricultural Things // Agricultural Mechanization in Asia, Africa and Latin America. – 2020. – Vol. 51. №3. – P. 87-92.

Исхаков С.Ю., Мельников А.К., Исхаков А.Ю.

О применении техник проактивного поиска угроз в работе робототехнических комплексов

Аннотация: Рассмотрены техники проактивного поиска угроз для выявления таргетированных атак без использования вредоносного программного обеспечения. Проводится анализ возможности их интеграции в инфраструктуру робототехнических комплексов. Результаты проведенного эксперимента на киберполигоне РТК подтверждают эффективность обнаружения сложных целенаправленных атак, при этом отмечается важность применения не только множества источников индикаторов, но и необходимость комплексирования методов обогащения событий и тактик.

Ключевые слова: кибербезопасность, индикаторы компрометации, робототехнические комплексы, сервисные данные, модель атак

Введение

Одним из ярко выраженных трендов в решении задач информационной безопасности сегодня является развитие методов выявления угроз, в реализации которых не задействовано вредоносное программное обеспечение (ПО). Основной целью является выравнивание темпов конверсии проактивных техник обнаружения и инструментов автоматизации управления ИТ-инфраструктурой. При этом одной из сфер применения алгоритмов, позволяющих выявлять ранее неизвестные кибератак, являются высокоавтоматизированные отрасли промышленности, такие как робототехника и киберфизические системы.

Среди причин подобных тенденций можно выделить, в первую очередь, ограниченность использования классической антивирусной защиты на базе сигнатур и эвристического анализа (не позволяют выявить бесфайловые атаки и несанкционированное применение легитимного ПО). Кроме того, количество внедряемых на объектах средств защиты зачастую так велико, что генерируемые ими данные о возможных инцидентах сложно поддаются анализу.

В данной работе рассматриваются проактивные техники поиска угроз и проводится анализ возможности их применения в инфраструктуре робототехнических комплексов.

Состояние исследований

Общим фактором в современных техниках поиска угроз является формирование наборов индикаторов компрометации, которые позволяли бы выявить ранее неизвестную атаку на ранних стадиях. Поскольку эффективность таких обнаружений сводится к реальной возможности реагировать на угрозу, то необходимо ранжировать подобные индикаторы в соответствии с их значимостью. Проведенный обзор литературы выявил широкую вариативность методов, подходов и техник моделирования различных угроз [1]. В работе [2] поднимается проблема высокой сложности индикаторов компрометации для представленных моделей, формализующих базовый набор действий для детектирования злоумышленника. Но еще более сложной задачей является задача интерпретации индикаторов для различных гетерогенных инфраструктур, в том числе с применением робототехнических комплексов различного класса [3].

Аспекты проактивного анализа и его организации на объектах критической инфраструктуры, а также в системах реального времени рассмотрены в [4-5]. В исследованиях [6-8] отмечаются методологические аспекты внедрения Threat Intelligence для повышения уровня информационной безопасности, рассматриваются основные факторы влияния на данный процесс.

Очевидно, что подходы, ориентированные на комплексирование информации о злоумышленниках и ресурсах, могут быть использованы для моделирования как технических, так и нетехнических угроз. При этом одна из основных целей применения таких подходов – обеспечить возможность предоставления полезного базиса для оценки риска.

Постановка задачи

В качестве исследуемого объекта была выбрана действующая георасределенная ИТ-инфраструктура, в состав которой входит также несколько киберфизических систем – робототехнических комплексов. Авторами был проведен предварительный поиск

достоверных источников сведений об индикаторах кромпрометации, в результате чего было выделено 90 платформ. При этом 12 из них в результате детального анализа были исключены из перечня вследствие низкой частоты актуализации информации. Исследованные платформы применяют общепринятые форматы описания и структурирования данных (STIX/MISP, JSON, CSV, TXT и т.д.).

Для сокращения разрыва между успешными случаями проведения атак и возможностями их обнаружения необходимо не только опираться на различные типы индикаторов компрометации, но и использовать потенциальные источники обогащения данных. На исследуемом объекте был внедрен прототип системы класса SOAR, которая позволяет связать их вместе и определить критичность отдельного оповещения, придавая больше контекста путем объединения данных из различных источников. В таблице 1 представлена применяемая в ходе исследования классификация приоритетов инцидентов.

Таблица 1 – Примеры детектирования инцидентов

Тип оповещения (инцидента)	Вероятность реализации угрозы	Возможные действия
1	2	3
Фиксация нежелательного ПО (класс “not-a-virus”) средствами классических антивирусов без признаков ущерба для затронутых сегментов	Низкая	Запрос к вендорам АВЗ на корректировку логики обнаружения; Внесение исключений в правила детектирования; Автоматизированное восстановление объекта
Обнаружение вредоносного ПО (класс шифровальщиков, кейлоггеров и т.д.) с признаками ущерба для затронутых сегментов	Средняя	Анализ вредоноса (песочницы, поиск по источникам индикаторов компрометации, запрос вендору) Внесение исключений в правила детектирования

Продолжение таблицы 1

1	2	3
Выявление индикаторов, относящихся к классу техник и процедур различных APT-группировок, а также вредоносная активность, связанная с применением легитимного ПО	Высокий	Оперативно реагирование, принятие мер по локализации заражения; Организация расследования с применением техник форензики; Восстановление объектов вручную

При формировании таблицы 1 использовались следующие критерии классификации выявленных инцидентов:

– определение этапа атаки по модели Cyber Kill Chain, на котором была зафиксирована активность;

– результат обогащения индикаторов компрометации данными из смежных систем (периодичность и количество связанных событий, аномалии в поведенческом анализе сущностей);

– степень критичности сегмента и влияние угрозы на нарушение защищенности смежных участков инфраструктуры;

– возможность и сложность восстановления затронутых систем (требуемые показатели доступности информационных систем).

Эксперимент

В ходе исследования за 10 месяцев было зафиксировано 1259 оповещений, большая часть которых сгенерирована в результате анализа событий от узлов инфраструктуры РТК с применением техник проактивного поиска угроз на основе индикаторов типа TTP (фиксация техник, тактик и процедур). При этом окончательно подтвержденными инцидентами среди них было признано менее 3%.

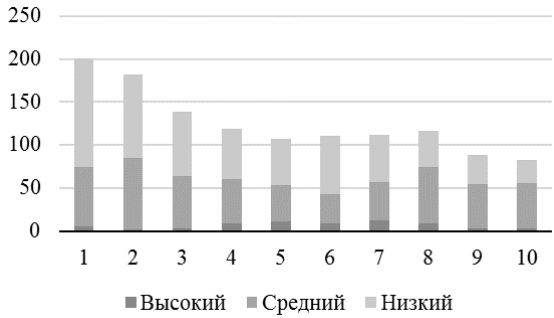


Рисунок 1 – Распределение инцидентов по вероятности реализации угрозы

С одной стороны, основная причина низкого уровня конверсии связана со сложностью задачи отличить легитимную активность в работе РТК от злонамеренной, что является вычислительно трудоемкой задачей и требует расчета точных распределений либо их точных приближений [9]. С другой стороны, несмотря на то, что большая часть инцидентов относится к низкой и средней вероятности реализации угрозы (рисунок 1), та малая доля реально подтвержденных инцидентов, обнаруженных проактивными методиками относилась в основном к высокому уровню реализации угрозы. Диаграмма на рисунке 2, в свою очередь, отражает значительное преимущество проактивных техник на основе индикаторов компрометации (*K1*) по общему количеству детектов (*K2* – эмуляция угроз, *K3* – ручное обнаружение, *K4* – анализ трафика).

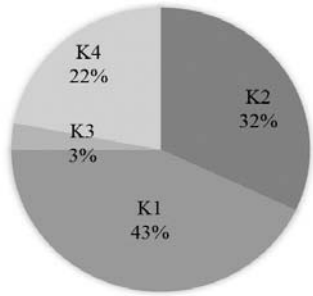


Рисунок 2 – Распределение инцидентов по методам обнаружения

Заключение

В ходе исследования была проведена оценка применения техник проактивного поиска угроз в работе робототехнических комплексов. Результаты эксперимента показали, что методы обнаружения сложных целенаправленных атак, а также ранее неизвестных векторов угроз являются высокоэффективными в данной отрасли промышленности, но требуют не только использования множества источников индикаторов, но и методов обогащения событий и тактик проактивного поиска угроз.

Исследование выполнено при частичной финансовой поддержке гранта Президента Российской Федерации в рамках научного проекта №МК-2421.2020.9 (исследование проактивных алгоритмов), а также гранта РФФИ №19-01-00767 (апробация алгоритмов на робототехнических комплексах)

Литература:

1. *Tatam M., Shanmugam B., Azam S., Kannoorpatti K.* A review of threat modelling approaches for APT-style attacks // Heliyon. – 2021. – Vol. 7. Issue 1. – P. 1-19.

2. *Liao X., Yuan K., Wang Z., Li Z., Xing L., Beyah R.* Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence / Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. – 2016. – P. 755-766.

3. *Hughes J., Cybenko G.* Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity // Technology Innovation Management Review. – 2013. – Vol. 3(8). – P. 15-24.

4. *Bianco D.J.* The Pyramid of Pain // Enterprise Detection & Response. – 2013. – URL: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (дата обращение 01.10.2021).

5. *Mokaddem S., Wagener G., Dulaunoy A., Iklody A.* Taxonomy driven indicator scoring in misp threat intelligence platforms // arXiv. – 2019. – Vol. 1902.03914. – P. 1-10.

6. *Belur J., Tompson L., Thornton A., Simon M.* Interrater Reliability in Systematic Review Methodology: Exploring Variation in Coder Decision-Making // Sociological Methods & Research. – 2018. – Vol. 50. Issue 2. – P. 837-865.

7. *Hoffmann R.* Markov Models of Cyber Kill Chains with Iterations / Proceedings in the 2019 International Conference on Military Communications and Information Systems (ICMCIS). – 2019. – P. 1-6.

8. *Дрянных Ю.Ю., Жуков В.Г.* О необходимости внедрения threat intelligence // Решетневские чтения. – 2017. – №21-2. – С. 398-399.

9. *Левин И.И., Дордопуло А.И., Писаренко И.В., Мельников А.К.* Управление расчетом точных приближений распределений вероятностей значений статистик на гибридных вычислительных системах / XIV Всероссийская мультиконференция по проблемам управления (МКПУ-2021): материалы XIV мультиконференции (27 сентября-2 октября 2021 Дивноморское, Геленджик) в 4 т. / Т. 2. – Управление в распределенных и сетевых системах (УРСС-2021). – Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2021. – С. 261-266.

Пискурева Т.А., Махов А.Н.

Цифровая трансформация и импортозамещение во взаимосвязи обеспечения безопасности ядерного объекта

Аннотация: Переход на импортонезависимые решения и цифровая трансформация идут в ногу с обеспечением безопасности на базе использования отечественных программных продуктов и технических средств.

В работе рассматривается взаимосвязь стратегии цифровой трансформации и импортозамещения с задачами по обеспечению безопасности ядерного объекта, обращается внимание на роль человеческого фактора при переходе на использование новых импортонезависимых решений, на важность формирования организационной культуры и культуры безопасности.

Ключевые слова: цифровизация, цифровая трансформация, импотрозамещение, цифровые продукты, системы защиты, ядерный объект, культура безопасности

Изменения, которые происходят в мировом порядке, глобальный кризис и пандемия сформировали новую повестку, следуя которой Россия вступила на путь глубокой цифровой трансформации государства.

Цифровая трансформация – это внедрение цифровых технологий в различные сферы деятельности общества. Что касается организаций, то цифровая трансформация – это, прежде всего, преобразование структуры самой организации, стратегии ее развития, презентации производимых продуктов и услуг, изменение организационной культуры.

Однако нельзя говорить об эффективности такой модели без должной модернизации, разработки и внедрения новых IT-технологий. Откуда же брать эти современные информационные технологии, способные создавать условия, как устойчивого экономического развития, так и эффективную систему безопасности? Это может быть достигнуто только цифровым суверенитетом, включающим в себя модель программного и аппаратного импортозамещения. Вместе с тем, цифровой суверенитет – более широкое понятие, чем импортозамещение. Оно включает в себя обеспечение информационной безопасности, возможность защиты от кибератак и кибершпионажа, обеспечение бесперебойного функционирования сети Интернет. А в условиях массовой глобализации, без политики импортозамещения говорить о 100-процентной кибербезопасности нельзя, да и невозможно.

Государственным структурам и компаниям с госучастим установлен план по переходу на отечественный софт в соответствии с национальной программой «Цифровая экономика РФ»[1]. К 2024 году – более 70% в госорганизациях и не менее 50% в государственных компаниях.

В системе Росатома успешно выполнена трансформация информационных технологий (ИТ), которая обеспечила эффективное протекание бизнес-процессов предприятий отрасли.

Трансформация ИТ была ориентирована на выполнение работ по внедрению корпоративных информационных систем в научно-производственную деятельность предприятий и обеспечение информационной безопасности.

В рамках трансформации ИТ внедрены, тиражированы и используются в научно-производственной деятельности предприятий Росатома различные корпоративные информационных системы, такие как, Единая отраслевая система электронного документооборота на базе EMC Documentum (ЕОСДО), которая обеспечивает скорость прохождения документов, повышает

эффективность работы сотрудников; Информационная система 1С:ERP Росатом, позволяющая эффективно управлять активами; Информационная автоматизированная система по управлению персоналом на базе SAP ERP HCM (ИАСУП), которая позволяет придерживаться единой политики кадрового менеджмента; Информационная система управления отношениями с поставщиками SAP SRM, позволяющая оперативно совершать закупочные процедуры, обеспечивая их контроль и ряд других информационных систем по автоматизации процессов подготовки отчетности, бюджетированию, управлению имущественными активами, энергоэффективностью, инвестиционными проектами, результатами интеллектуальной деятельности, обучением.

Использование информационных систем сокращает сроки подготовки и введения в действия решений, обеспечивает сохранность документов, а также автоматизацию и унификацию бизнес-процессов в соответствии с единой корпоративной учетной политикой.

После завершения цифровой трансформации информационных технологий, предприятия контура Росатома перешли в новую фазу цифровой трансформации самих организаций. С этой целью реализуется Единая цифровая стратегия Росатома, которая ориентируется не только на стратегические цели отрасли, но и на содействие в реализации национальной программы «Цифровая экономика РФ».

В состав Стратегии входят пять взаимосвязанных элементов: «Внутренняя цифровизация», «Цифровые продукты», «Содействие цифровизации-цифровая экономика РФ», «Организационные изменения», «Цифровая культура».

Стратегия состоит из 10 программ и нескольких горизонтов и этапов. В числе ее горизонтов следующие:

- долгосрочный горизонт 2030+ – формирование конкурентоспособной цифровой компании;
- горизонт государственных задач 2024 – достижение задач, зафиксированных в «майских указах» Президента;
- среднесрочный горизонт 2021 – решение задач внутренней цифровизации и создание условий для достижения целей государственного горизонта и видения «Цифровой Росатом» 2030;
- краткосрочный горизонт – решение наиболее важных и срочных бизнес-задач цифровизации на основе дорожных карт.

Основная задача Стратегии – создание устойчивой и безопасной конкурентной инфраструктуры, разработка и внедрение сквозных технологий, использование преимущественно отечественных программных продуктов и обеспечения безопасности информации и информационной инфраструктуры.

Предприятия Росатома идут по пути продуктизации внутренних разработок. Первым цифровым продуктом, выведенным на рынок, стал пакет программ для инженерного анализа и суперкомпьютерного моделирования класса CAE (Computer-Aided Engineering), в который входят модули «Логос Аэро-Гидро», «Логос Тепло» и «Логос Прочность» (расчетные коды), «Волна» – программно-вычислительный комплекс. Разработанная цифровая платформа Multi-D помогает управлять всеми этапами сооружения АЭС и других сложных объектов капитального строительства, система «Призма 2.0» позволяет управлять дискретным производством, связывая конструкторскую документацию и производство в цехах, система «Цифровое предприятие» обеспечивает управление предприятием и производством, платформа «Пилот» обеспечивает контроль и управление доступом для массовых мероприятий, установлена практически на всех стадионах страны, где проводились Олимпийские игры и Чемпионат мира по футболу.

Разработки предназначены как для отраслевого использования, так и для внешнего пользователя, среди них – самый большой в Европе ЦОД «Удомля».

Стоит выделить и разработки в области цифровой энергетики, системы управления спросом, сетевое и телекоммуникационное оборудование, а также ряд платформ – образовательную, «Цифровой добычной комплекс», коммуникационную платформу Atom Space для on-line общения сотрудников предприятий Росатома.

Переход на импортонезависимые решения и цифровая трансформация идут в ногу с обеспечением информационной безопасности на базе использования отечественных программных продуктов и технических средств. Современный рынок продуктов по информационной безопасности позволяет обеспечить защиту государственных интересов, бизнеса и обеспечить защиту информации, циркулирующей в защищаемых ресурсах ядерных

предприятий. Необходимо отметить, что отечественные ИТ-решения не уступают по функционалу и уровню сервиса защиты зарубежным аналогам [2]. Важное преимущество отечественных решений – они создаются с учетом российской специфики и рекомендованы регуляторами. Наиболее используемые решения отечественных производителей в части антивирусной защиты, защиты веб-приложений, защиты от утечек конфиденциальной информации, средств защиты от несанкционированного доступа, анализа защищенности, криптографической защиты информации и другие.

Большое внимание уделяется контролю и предотвращению нарушений информационной безопасности с применением DLP-систем и SIEM-платформ.

Решая вопросы цифровой трансформации и импортозамещения, мы понимаем, что человек был и остается основным гарантом эффективности и безопасности при любых технических и программных усовершенствованиях [3]. Вариативность развития событий, несовершенство инструкций, а главное – социально-психологическая природа человека как субъективного фактора нестабильности и неоднозначности и в восприятии, и в оценке событий – приводит к необходимости учета Человеческого фактора и формирования культуры безопасного внедрения и использования цифровых технологий посредством подбора, отбора, обучения и мотивации персонала. Высокая культура безопасного внедрения и использования информационных технологий, культура информационной безопасности базируется на развитой организационной культуре. С целью единого подхода к развитию культуры безопасности на ядерных объектах реализуется Единая отраслевая политика культуры безопасности. На объектах использования атомной энергии понимают, что культура безопасности должна быть элементом индивидуальных убеждений каждого работника, превалирующим фактором профессионального поведения в любом сегменте деятельности [4].

Крайне важно также отметить, что необходимо максимально открыто обсуждать любой опыт – независимо от того, приобретен ли он ценой достижений или ошибок. Возможность увидеть реальные плюсы и минусы будет мощным мотиватором к внедрению отечественных программных продуктов, а также

механизмом обратной связи, необходимой при переходе к цифровой трансформации и импортозамещению.

Литература:

1. Программа «Цифровая экономика Российской Федерации». Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р. – URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 10.10.2021).

2. *Гарифуллин Б.М., Зябриков В.В.* Цифровая трансформация бизнеса: модели и алгоритмы // Креативная экономика. – 2018. – Том 12. № 9. – С. 1345-1358.

3. *Пискурева Т.А., Завидова М.Ю., Сергеев М.С.* Вопросы кадровой безопасности. Зоны ответственности при обеспечении комплексной безопасности ядерного объекта / Проблемы управления безопасностью сложных систем. Материалы XXVI Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС-2018) (19 декабря 2018 г. Москва). – М.: ИПУ РАН, 2018. – С. 364-369.

4. *Piskureva T.A*. Practical Approaches to Nuclear Security Culture Assessment // 1540 COMPASS. – 2015. – Issue 9. – P. 30-33.

Plotnikov N.I.

Method of individual properties soft computing on the example of the civil aviation flight crew safety management

Abstract: Theory and methods of the characteristics of specialists remain uncertain. Statistical data and expertise may be piecewise defined, inaccurate and inconsistent. To calculate the dependability of flight crews based on workload and experience, it is necessary to establish indicators and values of acceptable accuracy, using fuzzy measures. It is proposed soft computing, statistical and expert methods for calculating the properties of a person and social groups in the management of dangerous professions. This makes it possible to calculate the dependability of the pilot properties with an assessment of flight safety risk levels for making management decisions. The results of the work are new standards for the workload of flight crews recommended for civil aviation.

Keywords: Soft Computing, Aviation, Accidents, Safety, Pilot, Crews, Workload

Introduction

Annual unpredictable aviation accidents (AA) have a huge international resonance, occur for decades and are a threatening reality of flight safety of the world civil aviation (CA) [1]. The commercial pressure of competition forces airlines to reduce the cost of purchasing, leasing, and maintenance of aircraft. The air carrier saves on professional training of personnel, on an arbitrary increase in the workload standards, on the use of flight crews with minimal and untenable experience in conditions of chronic fatigue. This paper explores the problem of existent standards of assessing human resource evaluation and regulatory approach for aviation safety management. The proposed method makes it possible to perform statistical analysis, expert assessments and calculations of the rationing of the work of flight specialists. The author presents his own approach to the theory of soft computing (SC) and mathematical definitions. Application of this approach makes it possible to analyze the existing statistics and obtain new quantitative data of dependability AA of CA pilot professional experience properties [2]. The result of the work is an example of development new standards recommended for CA flight crews.

Problem

Until now, the knowledge, theory and methods that could take into account the differences in the characteristics of any specialists remain uncertain, which leads to the use of untenable standards of professional training and labor rationing [3]. International regulatory standards constitute problematic content in security and safety terminology. To calculate the dependability of flight crews based on workload and experience, it is necessary to establish indicators and values of acceptable accuracy, using fuzzy measures. Probabilistic measures indicate relatively accurate and differentiated data. Thus, the relevance of the topic of this study is the lack of theory and methods for calculating the properties of objects for the purposes of effective, safe regulation and cockpit resource management (CRM) [4].

Soft computing method

The concept of SC was introduced by the founder of fuzzy set theory Lutfi A. Zadeh, 1994 [5]. In the understanding, SC is also revealed in the following directions: pseudo-physical logic, pseudo-quantitative calculus, and plausible reasoning. SC allows to define values by shifting the set object property towards strong scales. In the future, a new approach and interpretation of SC in fuzzy transitions of object states, calculations in combination with heatmaps, and examples of practical developments are presented.

The author does not know the formal definitions of SC in the scientific literature. To output the definitions of SC, let's accept the following justification for the observed (measured, estimated) boundaries values of object properties. Let the segment [a, b] contain subsets of the observed values of the value X belonging to the set R, figure 1.

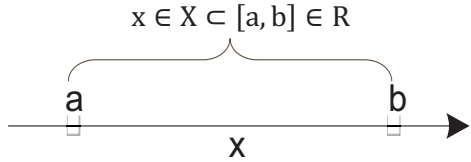


Figure 1 – SC definitions output

Enter the following conditions for calculating object values.

Condition A. The values of the observed quantities belong to any of the subsets, including the values a and b (A):

$$x \in [a, b] \text{ или } a \leq x \leq b. \qquad \{A\}$$

Def-1. Setting the values of the observed quantities in accordance with the condition {A} is called the method of hard estimation (evaluation) (HE).

The method HE calculates the exact (point) values of the values $x \in X$ of the two (both) boundaries of the segment [a, b] belonging to the set R.

Condition B. The values of the observed quantities at point [a] do not belong to any of the subsets (B):

$$x \in [a, b) = [a, b] \backslash \{b\} \text{ или } a < x \leq b. \qquad \{B\}$$

Condition C. The values of the observed quantities at point [b] do not belong to any of the subsets (C):

$$x \in (a, b] = [a, b] \backslash \{a\} \text{ или } a \leq x < b. \qquad \{C\}$$

Def-2. Setting the values of the observed quantities in accordance with the conditions {B and C} is called the soft measurement (SM).

The method SM sets the calculation of exact (point) values of values x ∈ X for only one (any) of the boundaries of the segment [a, b] belonging to the set R.

Condition D. The values of the observed quantities in the region [a, b] do not belong to any of the subsets (D):

$$x \in (a, b) = [a, b] \backslash \{a, b\} \text{ или } a < x < b. \qquad \{D\}$$

Def-3. Setting the values of the observed quantities in accordance with the condition {D} is called the soft estimation (evaluation) method (SE).

The method SE calculates the exact (point) values of the values x ∈ X of none of the boundaries of the segment [a, b] belonging to the set R.

Thus, let us do SC general formal definition output.

Def-4. Soft computing is a set of methods: hard estimation (HE), soft measurement (SM), soft estimation (SE) in metric and non-metric scales with the ability to simultaneously process quantitative numerical and qualitative linguistic data.

The presented interpretation of SC can be considered as the notion of the power of a finite universal set Ω, where fuzzy (soft) measures (1):

$$\Omega : \{\mu\_SM, \mu\_HE, \mu\_SE\} \qquad (1)$$

are indicators of data inaccuracy.

The powers of these measures are minimal for single-point sets. The most accurate values of the objects are measures μ_SM, less accurate μ_HE, and the greatest inaccuracy measures have μ_SE, in the limiting case μ_SE≅Ω.

The largest part of the values of the properties and states of organizations, social groups, and people is determined by the SC methods, which are used in conjunction with the heatmap model, the "traffic light model". The completed and presented theoretical work is a

prerequisite for experimental and applied developments carried out by the author of this work.

Task statement

Further applied calculation work is aimed at establishing fuzzy intervals of pilot experience indicators that correspond to the rules of calculation by definition SC. Expert assessments performed in the work form the basis of the normative values of the experience of flight specialists which are the basis for flight standards. Enter the following symbols and numeric values for experience properties of an individual: [μ_SM] soft measurements have square brackets, (μ_HE] hard estimates can have a square bracket on one side, a round bracket on the other, (μ_SE) soft estimates have parentheses. Let's explain SC options in management decisions examples levels (table 1).

Table 1 – Example of management task

Pilot experience, flight ours values levels	Risk levels probability P: AA per million flight per year (heatmap, traffic lights)	SC options	Management decisions example
{1} big	P = AA 10^{-7} (green)	(μ_HE]	free, strong
{2} middle	P = AA 10^{-6} (yellow)	(μ_SE)	free, free
{3} small	P = AA 10^{-5} (red)	[μ_SM]	strong, strong

{1} Free decisions making are applying about increasing pilot flight ours values. Strong decisions concerns to control pilot age over 60 years.

{2} Free decisions space.

{3} Strong decisions about first admission to work of a pilot. Strong decisions about transition of the co-pilot to the position of the captain.

Thus, decisions depend of scientifically founded pilot experience values.

Expert assessments

The method of expert assessments includes: preliminary selection of experts, organized assessment procedures, development of a matrix of SC values, data processing, analysis and output of indicator values.

Expert assessments were carried out by the author over a long period in 1994-2014. The main criterion for selecting experts was professional work experience. The examination involved 42 professional pilots with extensive flight experience. Among the experts were both active pilots and those who retired from their flying careers. Characteristics of the experts' indicators: age: 34-75 years; flight experience: 16-47 years; total flight time: 8000-26000 hours: flight hours pilot in command (PIC): about half of the total flight time; number of mastered aircraft: 4-12 types; geography of experience: international. Expert assessments were carried out through questionnaires, surveys and final discussions of the results. These values are derived in organized procedures with the participation of professional pilots with extensive flight experience. The task includes the output of the values of the number of flight hours and the number of flights in the periods: monthly, annually, as well as the subsequent averaging of these values in three months and in half a year. The results are the final development of the CA standardization. The values of the pilot's operational dependability indicators are set:

[minimum (nominal) maximum]:
flight hours: monthly [20 (50] 80], annually [150 (400] 800];
number of flights: monthly [5 (10] 20], annually [30 (75] 200].

The novelty of the results is to establish the accounting of indicators for time periods: flight task (day), month, 90 days, six months, year. This structure and the established values of indicators allow for continuous monitoring and rationing of operational dependability of flight resources to ensure flight safety.

Conclusion

Some fragments and a detailed description of the developed theory, method, experiments and expert assessments is presented in the paper [7]. It should be noted that in the work performed, the most important are the new theoretical results of calculating the experience of professional pilots, corresponding to the established levels of accident risks. However, the work also confirms practical evidence of the implementation of the results in a large multi-year project with the participation of the author in 2011-2014 at Volga-Dnepr Airlines (Russian Federation) [7].

References:

1. *Kane M.R.* Air Transportation. – USA, Iowa: Kendall Hunt Publishing Company, 1990. – 500 p.

2. *Plotnikov N.I.* The Development of the Subject Domain Observation Complex for Management Purposes / 2018 14th International Scientific-Technical Conference APEIE – 44894. – NSTU, 2018. – Vol. 1. Part 1. – P. 268-272.

3. *Shappell S.A., Wiegmann D.A*. The Human Factors Analysis and Classification System (HFACS) / FSF Flight Safety Digest. – 2001. – № 2. – P. 15-28.

4. *Wiener E.L., Kanki B.G., Helmreich R.L.* Cockpit Resource Management. – USA. N.Y: Academic Press, 1993. – 519 p.

5. *Zadeh L.A.* Fuzzy Logic, Neural Networks, and Soft Computing // Communications of the ACM, March 1994. – 1994. – Vol. 37. № 3. – P. 77-84.

6. *Broach D., Joseph K.M., Schroeder D.J.* Pilot age and accident rates report 3: an analysis of professional air transport pilot accident rates by age. – Civil Aeromedical Institute, Human Resources Research Division, FAA. – 2003. – 63 p.

7. *Plotnikov N.I.* "Automated system for predicting and preventing accidents at the organization and production of air transport". The intermediate stage № 4: «Adaptation of the developed algorithms and software AS». – Scientific- and-technical report «2010-218-02-068», № State registration 01201150118 from 12.01.2011, № 194. – Ulyanovsk. – 2012. – 1340 p. / N.I. Plotnikov – Section 3. – P. 154-238; Applications: I, K, L, M, N. – P. 1048-1258. (in Russian).

Баранов Л.А., Балакина Е.П., Сидоренко В.Г.

Безопасное диспетчерское управление в условиях использования интеллектуальных беспилотных систем управления движением городского внеуличного транспорта

Аннотация: Рассмотрены принципы построения Интеллектуальной системы управления движением городским внеуличным рельсовым транспортом, приведены функции уровней иерархии системы, описаны задачи, решаемые в различных ситуациях функционирования линий внеуличного транспорта.

Показана роль диспетчерского управления при использовании интеллектуальных беспилотных систем. Отмечена роль использования тренажерных комплексов в составе системы, обеспечивающих самообучение и тестовую проверку их знаний. Способы построения системы и совокупность мероприятий по повышения квалификации диспетчерского аппарата позволяют обеспечивать требуемую безопасность функционирования линии городских рельсовых транспортных систем.

Ключевые слова: управление движением внеуличным транспортом, алгоритмы оперативного управления, тренажер поездного диспетчера, безопасное диспетчерское управление, интеллектуальные транспортные системы, уровни иерархии

Интеллектуальные системы управления движением внеуличным транспортом относится к классу иерархических систем и содержат три уровня управления [1]. На верхнем уровне управления собирается информация о движении транспортных средств по всем линиям метрополитена, скоростного трамвая, электропоездов пригородного движения, имеющих остановки в черте города, осуществляется согласование движения в случаях чрезвычайных ситуаций и управление взаимодействием с другими видами транспорта (рисунок 1).

На втором уровне реализуется управление каждой линией, контролируемое диспетчерским аппаратом. Обеспечению безопасности диспетчерского управления на этом уровне посвящена данная работа.

Исходной информацией для второго уровня является плановый график движения. С третьего уровня на второй поступает информация о моментах прибытия и отправления транспортных средств на остановочные пункты. При компенсируемых отклонениях от графика движения алгоритмы второго уровня в автоматическом режиме определяют рассогласование между плановым и исполненным графиками движения и вырабатывают управление для третьего уровня. Управляющими воздействиями в данном случае являются времена хода и времена длительности стоянки транспортных средств. В этих условиях реализуются

алгоритмы, относящиеся к классу графиковых, учитывающие зависимости ограничений на управление в зависимости от расположения поездов на линии с прогнозом возмущающих воздействий, вызывающих задержки поездов на станциях метрополитена [2,3]. Ограничения на этом уровне задаются системами обеспечения безопасности движения.

Рисунок 1 – Структура Интеллектуальной системы управления движением внеуличным транспортом

При некомпенсируемых отклонениях от графика движения работают два класса алгоритмов. Первый – управление во время сбоя движения, второй – управление после ликвидации причин возникновения сбоя с целью восстановления движения по плановому графику [4]. Особенности управления движением поездов после ликвидации причин сбоя связаны с необходимостью

расстановки составов в депо или в заданных точках линии для реализации ночной расстановки и/или графика оборота составов, при котором обеспечиваются необходимые плановые осмотры поездов.

Рассмотрим участие диспетчерского аппарата при управлении во время сбоев движения. Показано [4], что все возможные сбои могут быть разделены на четыре основных типа:

- прекращение движения на участке пути;
- ограничение скорости на участке пути;
- неисправность подвижного состава, приводящая к движению с пониженной скоростью;
- неисправность подвижного состава, запрещающая его использование для пассажирских перевозок.

Каждая нештатная ситуация задается кортежем:

$$Exstraordinary\_situation=(type,time\_start,place,period) \quad (1)$$

где:

- $type$ - тип нештатной ситуации;
- $time\_start$ - время начала сбоя;
- $place$ – место возникновения сбоя;
- $period$ – период работы линии (часы пик, непик, начало движения, окончание движения), связанный с наличием резервов управления.

Для каждого сбоя разработан типовой алгоритм, входным параметром которого является кортеж (1), позволяющий учесть в качестве параметров работы алгоритма время возникновения нештатной ситуации, место ее возникновения, с учетом месторасположения по отношению к депо и станциям с путевым развитием, и диапазон резервов времен хода по перегонам и времен стоянок на станциях, используемых для управления движения.

Предложенные алгоритмы централизованного управления построены на основе обобщения опыта работы диспетчеров и исследованы методами имитационного моделирования. Инструментом для проведения моделирования является многофункциональная модель линии метрополитена, качество которой апробировано путем многолетнего использования в составе Тренажера поездного диспетчера Московского метрополитена.

Анализ качества управления проведен путем сравнения результатов моделирования с исполненными графиками реальных случаев, имеющих место на Московском метрополитене. Критерием качества работы алгоритмов является обеспечение равномерности движения на максимально возможном числе открытых для пассажироперевозок участков линии. Качество функционирования разработанных алгоритмов подтверждено анализом результатов их работы экспертной группой, в состав которой входили опытные диспетчера и работники Службы движения. Существенным параметром является время реакции системы на входную информацию о сбое, т.е. время между получением информации о начале сбоя и принятием управленческих решений. Современные средства вычислительной техники позволяют получить это время в пределах 2 секунд, что говорит о возможности использования алгоритмов в оперативном управлении.

Принципы построения алгоритмов базируются на моделях ситуаций, для каждой из которых учитывается возможности управления числом поездов, времен их хода, временем стоянки на станциях. По существу, предлагается оперативный график на период сбоя, на основании которого формируется последовательность управлений. В этом случае действия диспетчера могут идти по трем сценариям:

- согласие с предложенным алгоритмом;
- коррекция предложенного алгоритма;
- выработка собственного решения.

После ликвидации причин возникновения сбоя движения автоматически работает соответствующий алгоритм и сообщает результаты своей работы диспетчеру. Роль диспетчера при этом аналогична управлению во время сбоя.

Принципы построения данного алгоритма были выбраны после перебора всех возможных вариантов восстановления графика с целью выбора из них решения, обеспечивающего минимизацию основного критерия качества работы данного алгоритма – минимального времени вхождения в график. Очевидно, что этот подход не реализуем в условиях оперативного управления, так как время перебора и выбора лучшего по быстродействию варианта превышало 24 часа. Вместе с тем, эти данные позволили получить минимальное значение выбранного критерия, с которым возможно

сравнивать способы управления, получаемые для алгоритмов, работающих за приемлемое время. Для уменьшения числа вариантов были выбраны ограничения на управление, соответствующие требованиям комфортной перевозки пассажиров. Эти ограничения обычно используются диспетчерами в реальных ситуациях. В частности, не допустимыми являются неплановый оборот двух последовательно идущих поездов и отправление в депо двух поездов подряд, так как это может привести к скоплению пассажиров на текущей и впередилежащей станции за счет увеличения межпоездного интервала. Обязателен учет графика оборота, так как недопустимо нарушение времени осмотра подвижного состава.

С учетом указанных ограничений разработан эвристический алгоритм, время работы которого не превышает 1 мин 30 сек, за которые формируется оперативный график восстановления движения поездов. В качестве дальнейшей модернизации алгоритма решена задача экономии электроэнергии за счет перераспределения времен хода на участке между начальной и конечной оборотными станциями движения поезда.

Третий уровень – беспилотное управление поездными единицами. На этом уровне поездные единицы получают команды заданного времени хода по перегону, требуемые длительности стоянок, сигналы систем обеспечения безопасности, ограничивающие скорость движения с целью недопущения опасного сближения поездов на расстояние меньше тормозного пути. На этом же уровне происходит прицельное управление поездной единицей на остановочных пунктах, автоматическое выполнение ограничений по скорости, вплоть до полной остановки, по сигналам системы обеспечения безопасности, управление трогание поезда, управление открытием и закрытием дверей, радио-оповещение пассажиров и т.д. Следует отдельно подчеркнуть, что со второго уровня для каждой поездной единицы может быть реализована команда полной остановки поезда в любой точке пути [1].

Рассмотренное построение системы диспетчерского управления требует высокого профессионализма диспетчеров и быстродействия их реакции на предлагаемое решение. Должна быть разработана система мероприятий, обеспечивающая высокую

профессиональную готовность диспетчерского аппарата. С этой целью применяется тренажер поездного диспетчера, используемый в качестве электронного двойника линии метрополитена [5]. Разрабатывается и постоянно совершенствуется система сценариев сбойных ситуаций, тестовые алгоритмы эффективных решений. Существенным вопросом является создание методики, обеспечивающей последовательность тренировок диспетчеров, цикличность этих тренировок с контролем их эффективности [6]. Под контролем эффективности понимается выбор и обоснование критериев эффективности и разработка методических мероприятий по повышению количественных показателей этих критериев. В частности, составной частью векторного критерия является время выработки решений на сбойную ситуацию, бальная оценка эффективности принятого решения, количество неудачных решений, приводящих к уменьшению провозной способности линий во время сбоев.

Построение тренажера позволяет использовать его в режим самообучения и тестовом режиме. Имеется положительный опыт использования тренажера на Московском метрополитене для обучения и повышения квалификации поездных диспетчеров.

Совокупность указанных мероприятий позволяет получить эффективную процедуру взаимодействия диспетчерского аппарата с техническими средствами Интеллектуальной централизованной системы автоматического управления движением поездов линии метрополитена.

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. *Баранов Л.А., Сидоренко В.Г., Балакина Е.П.*, *Логинова Л.Н.* Интеллектуальное централизованное управление движением внеуличного городского железнодорожного транспорта в условиях интенсивного движения // Надежность. – 2021. – Т. 21. № 2. – С. 17-23.

2. *Баранов Л.А., Балакина Е.П., Воробьева Л.Н.* Алгоритмы для поездов метрополитена // Мир транспорта. – 2007. – №2. – С. 104-113.

3. *Баранов Л.А., Балакина Е.П.*, *Иконников С.Е., Антонов Д.А.* Централизованное управление движением поездов городских железных дорог современного мегаполиса // Наука и техника транспорта. – 2020. – №1. – С. 30-38.

4. *Балакина Е.П.* Принципы построения алгоритмов системы поддержки принятия решений поездному диспетчеру // Наука и техника транспорта. – 2008. – №2. – С. 23-26.

5. *Баранов Л.А., Сидоренко В.Г.*, *Ерофеев Е.В., Максимов В.М., Васьков Д.Б.* Тренажер поездного диспетчера линии метрополитена // Вестник Рязанского государственного радиотехнического университета. – 2012. – № 10. – С. 32.

6. *Баранов Л.А., Сидоренко В.Г., Балакина Е.П., Логинова Л.Н.* Интегрированный подход в обучении оперативных работников городских рельсовых транспортных систем // Наука и техника транспорта. – 2021. – № 2. – С. 22-31.

Сафронов А.И.

Доступность рельсовых транспортных систем города Москвы

Аннотация: В работе рассмотрены вопросы доступности, резервирования и связности единой транспортной сети города Москвы. Выполнен обзор актуального состояния вопроса организации доступной транспортной среды. Проанализированы перспективы и варианты развития единой транспортной сети города Москвы.

Ключевые слова: метрополитен, трамвай, городская электричка, московские центральные диаметры, доступность, мобильность, трассировка, инклюзивность

Развитие транспортного комплекса крупных мегаполисов связано с решением задач рационального управления пассажиропотоками, транспортными средствами, безопасностью организуемых перевозок, а также с культурой обслуживания пассажиров.

Последняя из отмеченных задач, в частности, затрагивает вопросы организации доступной транспортной среды.

Доступность городских рельсовых транспортных систем (ГРТС) города Москвы рассматривается через:

– готовность инфраструктуры ГРТС к использованию маломобильной категорией граждан;

– шаговую доступность станций и остановочных пунктов ГРТС (метрополитен и сеть центральных диаметров);

– резервирование трасс движения ГРТС при проведении плановых ремонтов путевой инфраструктуры;

– связь ГРТС с другими видами транспорта на примере нескольких современных транспортно-пересадочных узлов (ТПУ);

– наличие полносвязности сети ГРТС.

О мобильности пассажиров на общественном транспорте руководители градообразующих предприятий стали всерьез задумываться, начиная с 2003 года (с момента запуска пассажирского движения на Бутовской линии легкого метро). Так, станции, инфраструктурно готовые удовлетворить потребностям их посещения матерями с колясками, инвалидами, а также иными пассажирами, испытывающими сложности при перемещении по лестничным пролетам / эскалаторным наклонам, стали появляться не в центре, а, преимущественно, на окраинах города.

Решением вопроса удобства перемещения рассматриваемых категорий граждан на центральных станциях метрополитена стала не инфраструктурная модернизация, а создание 14 октября 2013 года специальной службы – Центр обеспечения мобильности пассажиров (ЦОМП) [1], которая в круглосуточном режиме принимает запросы от населения на сопровождение из заявленного пункта отправления в заявленный пункт прибытия с возможностью проводов на поезда дальнего следования (ПДС) и пригородные электропоезда через объекты инфраструктуры, не имеющие отношения к Московскому метрополитену.

Максимальную нагрузку на инфраструктуру, согласно материалам, посвященным исследованиям пассажиропотоков, опубликованных в открытых источниках [2], испытывает Московский метрополитен. Он покрывает большую часть города.

Но даже в этих условиях остаются районы, которые не имеют связи со станциями метрополитена в шаговой доступности.

Шаговая доступность определена в радиусе одного километра от оси станции, что эквивалентно 10-15 минутам передвижения пешком. Проведенный анализ позволил выявить все проблемные районы.

Количество проблемных районов на карте резко сокращается, если принять во внимание наличие в них альтернативных видов ГРТС, таких как, например, действующих трасс первых двух Московских центральных диаметров (МЦД), трамвайных линий, переданных под управление ГУП «Московский метрополитен» 11 января 2021 года [3].

В перспективе до 2027 года за счет ввода в эксплуатацию новых станций метрополитена, утвержденных действующим генеральным планом развития города Москвы, ликвидируются многочисленные проблемные районы на севере, северо-западе и юге столицы [4].

Еще часть проблемных районов в перспективе будет устранена по завершении ввода в эксплуатацию всех пяти заявленных трасс МЦД. Наиболее значимый вклад в улучшение транспортной доступности должен внести *D5*, однако его трасса и по сей день застопорилась на этапе проектирования и согласования.

Итого, неудовлетворительная транспортная доступность сохранится в южной части Каширского шоссе в районе Орехово-Борисово Южное, в районе Капотня, на востоке района Люблино, в реорганизованной промзоне «Очаково», в поселке Восточный.

Развитие путевой инфраструктуры метрополитена – это только одна из сторон вложения денежных средств. Другая сторона – это поддержание существующей инфраструктуры в состоянии, обеспечивающем безопасные перевозки. Практика эксплуатации метрополитена показывает, что далеко не все проблемы решаются проведением плановых ремонтов в ночное время. На некоторых, наиболее старых участках линий метрополитена, необходимо проводить длительные работы, сопровождающиеся полным закрытием одной или нескольких станций.

Руководство ряда метрополитенов мира, в частности, западноевропейских, обладающих более давней историей эксплуатации, нежели Московский метрополитен, решает проблему, связанную с необходимостью проведения длительных ремонтных работ, за счет дублирующих участков путевой инфраструктуры.

Старые районы городов, расположенные в исторических центрах, содержат резервы путевой инфраструктуры, состоящие из нескольких линий. Обрывов движения там не происходит при возникновении необходимости проведения длительных ремонтов.

Упомянутое резервирование имеет место в метрополитенах Мюнхена, Парижа, Барселоны и других.

На Московском метрополитене в настоящее время имеются три явных участка, обладающих взаимным резервированием. Из них, согласно реализации, только один создан принципиально как резервный – это юго-восточная часть Некрасовской линии, разгружающая юго-восточную часть Таганско-Краснопресненской линии. Остальные два участка обособились случайно. В одном случае – это «эхо войны» (Филевская и Арбатско-Покровская линии на западе взаимно резервируют друг друга, находясь на различной глубине залегания), в другом – это многократная корректировка трасс линий при столь же многократной корректировке генерального плана развития Москвы при геополитическом переходе от СССР к Российской Федерации (Серпуховско-Тимирязевская и Люблинско-Дмитровская линии на севере).

Задача полноценного резервирования линий метрополитена постепенно решается за счет реализации программы развития городских электричек – МЦД.

Идея МЦД для современного мира не нова. Аналогичные проекты существуют, например, в Париже (*RER – Réseau Express Régional*), Мюнхене (*S-Bahn – Stadtschnellbahn),* а также в других крупных городах Западной Европы.

Отсутствие полноценного дублирования линий Московского метрополитена вынуждает изыскивать резервы при использовании связи с наземным общественным транспортом (НОТ). На сегодняшний день при необходимости закрытия участков линий метрополитена вводятся компенсационные автобусные маршруты (КМ).

Конечные станции, а также точки города, находящиеся на границах Административных Округов (АО) столицы, в обязательном порядке содержат ТПУ, включающие в себя торговые площади и разветвленную сеть остановочных пунктов НОТ, увязывающих между собой АО и региональные населенные пункты. Административное деление города Москвы оказывает

существенное влияние на маршрутную сеть НОТ. Соседние АО, как правило, связываются 1-3 прямыми маршрутами с довольно большими интервалами движения, достигающими получаса.

Иметь в распоряжении полносвязные транспортные сети – задача особого стратегического назначения для города. Так, например, трамвайную сеть Москвы передали ГУП «Московский метрополитен» с целью решения вопросов ремонта путевой инфраструктуры, улучшения движенческой составляющей и реализации полносвязной сети во всем городе [3].

Полносвязность железнодорожной сети Москвы – серьезная проблема для современных градостроителей. Далее в работе рассматривается сложность реализации *D5*. Урбанистами в помощь городу при решении вопросов трассировки *D5* была предложена схема модернизация заброшенной Симоновской железнодорожной ветки, являющейся продолжением Перовской соединительной ветки [5]. Этот шаг позволяет обойтись без выхода трассы *D5* на Курское направление Московской железной дороги (МЖД) и реализовать рациональную связь Ярославского и Павелецкого железнодорожных направлений МЖД.

Городские власти предложили и продолжают настаивать на том, чтобы маршрут *D5* после перехода с Ярославского направления МЖД на Митьковскую эстакаду проходил через часть Казанского направления МЖД, Перовскую соединительную ветку с выходом на Курское направление и последующим переходом на Павелецкое направление, но по проследовании станции Царицыно. При этом от Павелецкого направления в черте города Москвы остаются только две станции: Бирюлево-Товарная и Бирюлево-Пассажирская, что существенно искажает схему доступности городской электрички для большей части Павелецкого направления МЖД, расположенной в черте города Москвы [6]. Шесть станций остаются без удобных, выгодных тарифов МЦД. Этот шаг не рационален.

С недавних пор упомянутое предложение урбанистов пресечено строительством новых жилых и офисных кварталов на пути следования Симоновской железнодорожной ветки через возможный новый (Дербеневский) железнодорожный мост, который следовало бы возвести для связи Крутицкой и Дербеневской набережных.

Разработчики перспективной схемы Московского метрополитена предположили, что *D5* будет представлен тремя ответвлениями одного только Ярославского направления МЖД, и появится *D6* только из Павелецкого направления МЖД [7].

Департамент строительства города Москвы в ответ на отклик населения, проанализировавшего «любительскую» схему перспективного метрополитена, форсировал выпуск обновления раздела Интернет-портала Правительства Москвы, посвященного перспективам развития Московского метрополитена, и в течение недели выдал официальный план развития железнодорожного транспорта в столице. Не на столь же далекую перспективу, как это сделали «любители», а до 2027 года [4]. На ней в 2027 году отсутствует *D5,* и это при том, что согласно заявлениям руководителей Департамента, трасса *D5* должна окончательно обособиться к концу 2025 года.

Данный материал подготовлен в качестве обоснования необходимости изучения специфики и особенностей ГРТС, инфраструктурно связанных с Московским метрополитеном, поскольку именно они предназначены для существенного улучшения транспортной доступности столицы.

Литература:

1. Московский метрополитен. О центре мобильности. – URL: https://mosmetro.ru/passengers/services/accessibility-center/about/ (дата обращения 10.10.2021).

2. Единый транспортный портал. Итоги работы транспортного комплекса Москвы в 2020 году и планы на 2021 год. – URL: https://transport.mos.ru/common/upload/public/ prezentacii/84/raboty-tk-v-202002032021.pdf (дата обращения 10.10.2021).

3. MSK News. Новости Москвы и Московской области. Московские трамваи передали в ведение метрополитена. – URL: https://msknovosti.ru/transport/moskovskie-tramvai-peredali-v-vedenie-metropolitena/ (дата обращения 10.10.2021).

4. Комплекс градостроительной политики и строительства города Москвы. Метро. – URL: https://stroi.mos.ru/metro (дата обращения 10.10.2021).

5. МЦД-5 через Симоновскую ветку – реально ли? Яндекс.Дзен. – URL: https://zen.yandex.ru/media/mcd_mcc/mcd5-

cherez-simonovskuiu-vetku-realno-li-videoprogulka-5f293fabc4a79e57b7bd3355 (дата обращения 10.10.2021).

6. Новая линия наземного метро. МЦД-5 «Ярославско-Павелецкий». Новая линия наземного метро. – URL: https://mcd.mosmetro.ru/mcd-5/ (дата обращения 10.10.2021).

7. Схема Московского метро 2030. Схема. – URL: https://metromap.moscow/ru (дата обращения 10.10.2021).

Сафронов А.И., Овсяников Г.П.

Графоаналитическое моделирование равномерных расположений транспортных средств как способ повышения качества планирования маневровой работы электродепо метрополитена

Аннотация: В работе рассматривается один из возможных способов автоматизированной визуализации методики поиска равномерных расположений, сформулированной М.Л. Концевичем на базе алгоритма целочисленного деления Евклида. Предложенный способ визуализации позволяет просматривать как совокупность проделанных шагов работы методики, так и отдельно выполненные шаги. Рассмотрен эргономичный графический пользовательский интерфейс, адаптированный под эффективную и экономичную выдачу результатов как на экран персонального компьютера, так и на бумагу для проведения классического анализа вариантов расчета.

Ключевые слова: метрополитен, равномерность, алгоритм евклида, информационные технологии, обучение, маневровая работа, программирование

Задачи автоматизации планирования перевозочного процесса (ППП) на метрополитене решаются специалистами кафедры «Управление и защита информации» на протяжении многих десятилетий. За это время по тематике обособилось два устойчивых направления работ, неразрывно связанных друг с другом, но различных по уровню сложности:

– интеллектуальные задачи оптимизации,

– задачи визуализации и развития эргономичности графического пользовательского интерфейса (ГПИ).

Выявляемые новые задачи в каждом из упомянутых направлений позволяют ежегодно и непрерывно планировать структуры для будущих выпускных квалификационных работ (ВКР), магистерских и кандидатских диссертаций обучающихся. Это связано, прежде всего, с тем, что в разработанную на кафедре автоматизированную систему построения плановых графиков движения пассажирских поездов («АРМ Графиста»), предназначенную для ППП на метрополитене, заложены адекватные и устойчивые к изменяющейся ситуации математические модели, позволяющие проводить исследования для нужд не только Московского метрополитена, но и эффективного учебного процесса на кафедре. Последние, как правило, связаны с исследованием специфики движения иных видов городских рельсовых транспортных систем, отличных от метрополитена.

Одно из направлений развития «АРМ Графиста» свелось к решению оптимизационных задач экономии энергетических ресурсов на этапе ППП [1]. Работы, выполняемые для условий метрополитена, тесно взаимосвязаны с работами, выполняемыми для условий магистральных железных дорог [2].

Другое направление связано с совершенствованием методов, заложенных в систему, а также с визуализацией этих методов, необходимой для более удобного анализа результатов, получаемых по итогам работы алгоритмов автоматизации [3].

Вопросы визуализации методов оптимизации за счет своей наглядности еще на ранних курсах способны эффективно и быстро вовлекать обучающихся в научно-исследовательскую работу. Особо продуктивными являются ситуации, когда в параллель с увлеченностью железнодорожной тематикой у обучающихся имеется не менее сильная увлеченность информационными технологиями и программированием. Практикуемая на кафедре методика – это лучший способ организовать, так называемое, развивающее и выравнивающее обучение [4] на начальных курсах, когда параллельно обучающимися осваиваются фундаментальные общеобразовательные дисциплины, расширяющие их кругозор. И в то время, пока большинство в группах решает типовые задачи, которые, зачастую, создаются при использовании

автоматизированных системам формирования учебных заданий [5], энтузиасты нарабатывают опыт и материал для своей будущей ВКР.

Одной из особо интересных математических задач, удачно применяемых к сфере ППП на Московском метрополитене, является задача поиска равномерных расположений (РР), сформулированная М.Л. Концевичем на базе алгоритма целочисленного деления Евклида (АЕ) [6]. Идея использования результатов решений задач поиска РР на кафедре «Управление и защита информации» принадлежит Сеславину А.И. [7]. Его основная рекомендация заключалась в том, чтобы рассматривать переходные процессы равномерного ввода составов из депо на линию и равномерного снятия составов в депо с линии. В работах Сеславина А.И. показано, что алгоритм является быстродействующим. Это подтверждено, в частности, и результатами, опубликованными в [3]. В [3] так же показано, что любой результат, для которого может быть решена задача поиска РР, обязательно отвечает сформулированному критерию равномерности.

«Ядро» АЕ может быть записано следующей формулой (1):

$$G = C * N + K, \quad (1)$$

где G – количество элементов в кольце,

C – количество элементов, которое необходимо равномерно распределить (показывает общее количество серий элементов на окружности),

N – множитель, позволяющий приблизить значение равномерно распределяемых элементов к G (показывает длину меньшей серии элементов на окружности),

K – остаток, которого не хватает для того, чтобы $C*N$ сравнялся с G (показывает количество больших серий – на единицу больше N).

Работа АЕ продолжается до тех пор, пока значение K не станет равным нулю.

ГПИ созданной разработки представлен:

– кнопками, увеличивающими / уменьшающими общее количество элементов и количество маркированных элементов;

– списком для выбора изображения, соответствующего конкретному шагу АЕ, а также всех шагов АЕ сразу;

– списком информации о каждом шаге АЕ;

– кнопкой «Инвертировать цвет»;

– графической областью, на которой визуализируется РР маркированных элементов.

Подпрограмма «*UniformDistribution*» представлена тремя вложенными программными методами: «*AlgoritmEvklid*», «*StepsInformation*» и «*MarkingOfElements*».

В программном методе «*AlgoritmEvklid*» циклически заполняется матрица, содержащая в себе значения всех шагов АЕ. 1-й вектор-столбец состоит из общего количества элементов, 2-й – из количества элементов одной серии, 3-й – из количества маркированных элементов, 4-й – из количества больших серий.

На каждом шаге вектор первого шага АЕ изменяет значение своих элементов, после чего *i*-я строка матрицы присваивает себе его значение до тех пор, пока 4-й элемент не станет равен нулю. Количество строк матрицы так же изменяется на каждом шаге.

«*StepsInformation*» заполняет список информацией о каждом выполненном шаге АЕ.

«*MarkingOfElements*» изображает, зависимости от выбора шага, АЕ, равномерное распределенные элементы на окружности. Программный метод состоит из двух циклов, один из которых вложенный. У первого цикла количество итераций равно количеству шагов АЕ. В этом цикле, если в списке выбрано «все шаги АЕ», перебирается каждая строка четырехстрочной матрицы, иначе – рассматривается выбранный шаг АЕ и после первой итерации цикл завершается.

Вместе с тем выполняется расчет основного (как *Angle(360 / Matrix[i, 0]))* и дополнительного угла поворота элементов, после чего зарисовывается окружность выбранного или очередного *i*-го шага.

Количество итераций второго цикла соответствует количеству элементов выбранного или очередного *i*-го шага. В нем осуществляется поворот элемента на угол *Angle + 1* относительно центра окружности, если дополнительный угол не равен нулю, в ином случае угол поворота остается равен *Angle*. При каждом повороте *Angle + 1* из значения дополнительного угла вычитается единица. Далее изображаются элементы и их маркировка. Маркировка для меньших серий выполняется, когда остаток от

деления на *i*-ой итерации цикла на промежуток между маркированными элементами равен нулю и до тех пор, пока значение целочисленной переменной, учитывающей количество изображенных меньших серий, не станет равным разнице между количеством маркированных элементов и количеством больших серий. После значение переменной обнуляется и на каждой итерации цикла к ней прибавляется единица. Помимо этого при маркировке больших серий из *Matrix[i, 3]* вычитается единица. Маркировка больших серий выполняется, когда остаток от деления количества изображенных меньших серий на сумму единицы и промежутка между маркированными элементами становится равным нулю и до тех пор, пока количество больших серий у выбранного или очередного *i*-го шага не станет равным нулю.

Визуализация примера работы АЕ при использовании составленного программного обеспечения показана на рисунке 1.

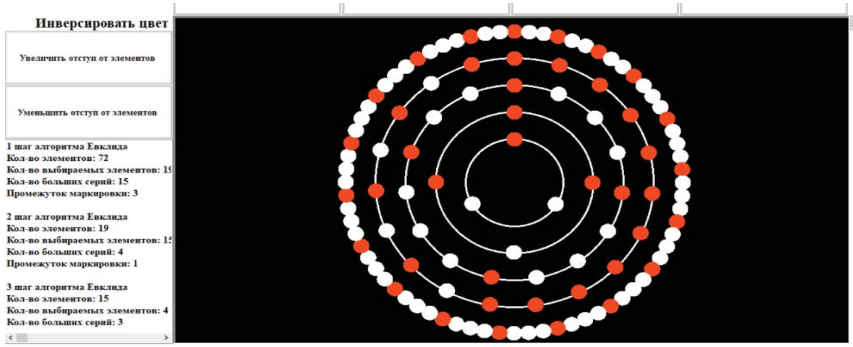


Рисунок 1 – Пример визуализации равномерных расположений 19-ти элементов среди 72-х

Планируется, что разработанное программное обеспечение в перспективе станет частью модуля анализа полученных результатов автоматизированного построения ПГД в «АРМ Графиста 2.0».

Литература:

1. *Баранов Л.А., Сидоренко В.Г., Балакина Е.П., Сафронов А.И.*. Минимизация расхода энергии на тягу поездов внеуличного городского транспорта // Электротехника. – 2021. – № 9. – С. 26-34.

2. *Савоськин А.Н., Гарбузов И.И.* Сравнительный анализ эффективности работы двух- и четырехсекционных электровозов ЭС5К // Электротехника. – 2017. – № 9. – С. 37-40.

3. *Сидоренко В.Г., Сафронов А.И.* К вопросу об оценке быстродействия метода выравнивания временных интервалов // Информатизация образования и науки. – 2014. – № 1(21). – С. 120-130.

4. *Абушкин Д.Б.* Подготовка будущих учителей информатики по дисциплине «Практикум по решению задач на ЭВМ» на основе методики выравнивающего и развивающего обучения. – Диссертация на соискание ученой степени кандидата педагогических наук. – Москва, 2011. – 180 с.

5. *Абушкин Д.Б.* Автоматизированная система формирования учебных заданий // Вестник Российского университета дружбы народов. Серия: Информатизация образования. – 2010. – № 1. – С. 41-43.

6. *Концевич М.Л.* Равномерные расположения // Квант. – 1985. – № 7. – С. 51-52, 59.

7. *Сеславин А.И., Сеславина Е.А.* Принципы равномерности в задачах управления потоками пассажирского транспорта // Прикладная информатика. – 2009. – № 2(20). – С. 91-95.

Полюхович М.А.

Основы информационного обеспечения процесса передачи электроэнергии в условиях деструктивного воздействия гидрометеорологических факторов

Аннотация: Рассмотрена проблема устойчивости процесса передачи электроэнергии в условиях деструктивного воздействия гидрометеорологических факторов окружающей среды. Для решения данной проблемы предлагается осуществлять информационное обеспечение процесса передачи электроэнергии посредством применения геоинформационной системы. Данный подход позволяет установить требуемый показатель эффективности системы управления в условиях неопределенности окружающей среды.

Ключевые слова: система управления, передача электроэнергии, гидрометеорологические факторы, геоинформационная система, модель принятия решений

В настоящее время инфраструктура человеческой деятельности характеризуются высокой энергоемкостью. Это означает, что энергетическое планирование должно быть сосредоточено и на экономии и сокращении энергопотребления, и на внедрении систем обеспечения безопасности объектов электроэнергетической отрасли таким образом, чтобы обеспечить устойчивое развитие человеческого общества, что предполагает бесперебойное электроснабжение объектов инфраструктуры любого назначения. Говорить о нормальном (штатном) функционировании объекта можно только при условии обеспечения его безопасности. Безопасность – свойство системы сохранять свое предназначение [1] (в данном случае – электроснабжение потребителей).

Научно-педагогической школой «Системная интеграция процессов государственного управления» (Санкт-Петербургский политехнический университет Петра Великого) разработан естественно-научный подход, базирующийся на законе сохранения целостности объекта [2]. На основе данного подхода можно осуществлять системную интеграцию процессов обеспечения безопасности, что и является, по мнению автора, решением существующей проблемы.

Проблемы электроснабжения потребителей в условиях деструктивного воздействия гидрометеорологических факторов окружающей среды вынуждают искать решение в применении современных технологий, что позволяет поддерживать принятие решений, обеспечивая комплексную политику по управлению безопасностью. Однако такой подход, который обеспечивал бы системное взаимодействие передовых технологий с системой поддержки принятия управленческих решений при возникновении угроз, пока достаточно не проработан.

Системы управления, в частности, безопасностью или электроснабжением, довольно чувствительны к принятию определенного управленческого решения. Так как от лица, принимающего решение (ЛПР), зависит то, в каком состоянии будет находиться система. Состояние системы в определенный момент времени – множество ее существенных свойств в этот

момент времени. Одна из основных задач системного анализа – установление причинно-следственных связей выходов системы с ее входами и состоянием, что позволяет достигать цели деятельности. Очевидно, что для создания рационально организованной системы необходимо иметь математическую модель решения ЛПР [3].

Пространственные данные имеют фундаментальное значение для установления взаимосвязи между различными явлениями. Для этого их необходимо собирать, хранить, анализировать и представлять с помощью специально разработанных платформ. Геоинформационные системы (ГИС) являются наиболее подходящими платформами для этих целей. Интеграция ГИС и процессов обеспечения безопасности позволяет автоматически оценивать ситуацию на определенной территории и принимать необходимые меры по устранению возможной угрозы.

Интеграция системы управления безопасностью объекта и ГИС необходима для обеспечения бесперебойного электроснабжения потребителей. Полученная в результате интегрированная система может использоваться в качестве системы поддержки принятия решений и предоставлять необходимую информацию ЛПР.

В системе управления безопасностью обратная связь с инструментами ГИС позволяет ЛПР определять приоритеты действий. Функциональные возможности инструментов ГИС показывают, что они могут использоваться в качестве систем поддержки принятия управленческого решения для территориально-распределенных объектов [4], таких как электрические сети.

Разработанное информационное обеспечение процесса передачи энергии в условиях деструктивного воздействия гидрометеорологических факторов позволяет при ограничениях на ресурсы осуществлять целевую деятельность объектов электроэнергетической системы – электроснабжение потребителей электроэнергией.

При этом появляется возможность не только определять показатель эффективности системы управления, но и задавать его требуемое и допустимое значение, учитывая при этом экономические затраты и выгоды, ограничения на материальные и деятельностные ресурсы.

Важной переменной, возникающей при принятии управленческого решения, является, на личный взгляд автора, показатель квалификации руководителя. Определение данного показателя представляет собой довольно трудную задачу, поэтому дальнейшие исследования планируется проводить в данном направлении.

В ходе проведенного исследования была разработана интегрированная система информационного обеспечения процесса передачи электроэнергии в условиях деструктивного воздействия гидрометеорологических факторов на основе процессов обеспечения безопасности и ГИС. Была определена концепция модели принятия решений в условиях неопределенности окружающей среды.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-38-90225

Литература:

1. *Лепешкин О.М., Лепешкин М.О., Бурлов В.Г.* Синтез модели процесса управления техническими системами на основе теории радикалов / Тезисы докладов XIV Всероссийской научной конференции «Нейрокомпьютеры и их применение» (Москва, 15 марта 2016 г.). – М.: Московский государственный психолого-педагогический университет, 2016. – С. 18-В.

2. *Бурлов В.Г.* Методология оценивания и управления рисками возникновения ЧС в организационно-технических и социально-экономических системах / Материалы девятой Всероссийской научно-практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций «Региональные риски чрезвычайных ситуаций и управление природной и техногенной безопасностью муниципальных образований». – М.: Центр стратегических исследований гражданской защиты МЧС России, 2004. – С. 220-233.

3. *Burlov V.G., Popov N.N.* Management of the application of the space geoinformation system in the interests of ensuring the environmental safety of the region / Advances in the Astronautical Sciences. – 2017. – P. 751-760.

4. *Булатова Г.Н., Афанасьева Н.И., Семанов Д.А.* Интегральное эколого-экономическое моделирование регионов с использованием ГИС-технологий // Георесурсы. – 2017. – №4. – С. 383-392.

Евдокимова А.В.

Анализ пожарной безопасности теплоцентрали на основе изучения пожароопасных ситуаций

Аннотация: В данной работе были изучены статистические данные в области возникновения пожаров на производствах, основные пожароопасные ситуации, возникающие на предприятиях энергетики, в частности теплоцентрали, на основе этого было построено «дерево событий». Проведен анализ пожарной безопасности теплоцентрали.

Ключевые слова: пожарная безопасность, теплоцентраль, дерево событий, пожар, анализ

Любая деятельность потенциально опасна – общеизвестная аксиома. Из данного выражения следует, что любой процесс (в данном случае генерация электроэнергии и тепла) влечет за собой как позитивные, так и негативные последствия. Проблема возникновения пожароопасных ситуаций во время работы теплоцентрали является актуальной в наши дни. Согласно данным Статистического сборника МЧС России в период с 2016 по 2020 год наблюдается рост возникновения пожаров на объектах производственного назначения (теплоцентраль относится к данной категории) (рисунок 1, количество в ед.) [1].

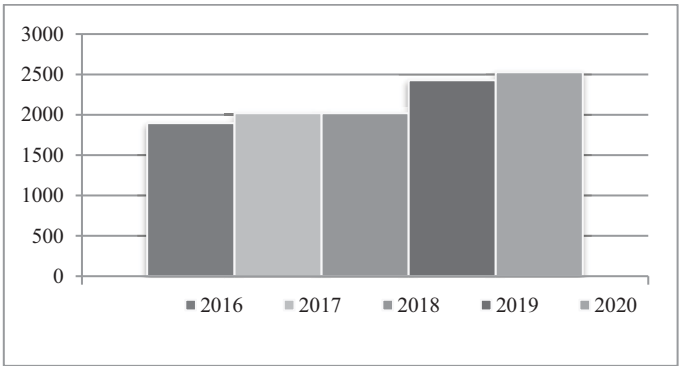


Рисунок 1 – Количество пожаров (ед.) на объектах производственного назначения за 2016-2020 гг.

Это довольно весомый показатель, ввиду чего проблема возникновения чрезвычайной ситуации на ТЭЦ, в частности пожара или взрыва, является актуальной на сегодняшний день.

Пожар – это такое явление, которое часто носит случайный характер, и которое невозможно исключить полностью из человеческой жизни. Обеспечение пожарной безопасности является важной функцией государства [2]. Именно поэтому перед человечеством была, есть и будет задача минимизации пожарной опасности. В связи с чем цель данного исследования заключается в изучении потенциально возможных пожароопасных ситуаций и анализе пожарной безопасности на предприятии. Для достижения поставленной цели были выполнены ниже представленные задачи:

1. Анализ особенностей работы ТЭЦ.

2. Изучение потенциальных опасностей, возникающих на ТЭЦ.

3. Анализ возможных пожароопасных ситуаций на основе дерева событий.

4. Анализ состояния пожарной безопасности на предприятии энергетики.

Решение задач было осуществлено при помощи следующей цепочки методов научного исследования: постановка проблемы, изучение литературы для формирования теоретической базы знаний, нормативно-правовых документов в области пожарной безопасности, анализ основных причин возникновения пожаров и взрывов на ТЭЦ, построение дерева событий, синтез полученных данных.

Под теплоцентралью стоит понимать предприятие, основным продуктом которого является производство тепловой энергии в виде подачи горячей воды или пара в центральную систему отопления для бытовых и промышленных нужд, в качестве побочного продукта выступает выработка электроэнергии. Данное предприятие является опасным производственным объектом и имеет класс функциональной пожарной опасности Ф5.1.[3,4]. Подобные предприятия, где обращаются, хранятся, перерабатываются горючие вещества и материалы, являются источниками повышенной опасности, ведь на них возможны аварии с последующим возникновением пожара, взрыва. Так например, согласно данным [5], 92% крупных аварий, сопровождающихся пожаром, возникли на ТЭЦ из-за отказа в работе того или иного

оборудования. Также существуют и иные причины. Среди помещений, в которых сосредоточена основная пожарная нагрузка, находятся: машинный зал, турбинный и котельный цех, мазутохранилища и трансформаторы [6].

На теплоцентрали имеется большое количество оборудования, работающего под давлением, систем охлаждения и смазки, комплексов энергоснабжения. Подобное сочетание служит источником потенциальной опасности. Ниже представлен перечень основных причин (опасностей) возникновения пожаровзрывоопасной ситуации на ТЭЦ:

- отказ в работе оборудования;
- взрыв угольной пыли;
- разгерметизация резервуара;
- короткое замыкание;
- коррозия оборудования;
- нарушение целостности систем смазки;
- обрушение строительных конструкций и др.

Для анализа развития аварийной ситуации была рассмотрена одна из вышепредставленных опасностей. Анализ был проведен при помощи метода построения дерева событий (рисунок 2) [7]. В качестве исходного события выбрано разрушение емкости под давлением (истечение газовой фазы).

Из рисунка 2 следует, что инициирующее событие (разрушение емкости) в зависимости от разных условий развития события может привести к разного рода пожарам. Подобный подход (построение «дерева событий») позволяет анализировать развитие аварийной ситуации, а также расчетным путем оценивать вероятность ее возникновения.

Анализ пожарной безопасности теплоцентрали сводится к процедуре рассмотрения каждого инициирующего события в отдельности. При этом становится ясно, что необходимо предотвращать их возникновение.

Резюмируя вышесказанное, проблемы в области обеспечения пожарной безопасности производственных объектов, в частности в области энергетики, являются актуальными в наши дни. Для минимизации риска возникновения опасностей существует необходимость разработки мер, способствующих этому. Анализ пожарной безопасности является основой для разработки комплекса

подобных мероприятий, направленных на достижения допустимого пожарного риска на ТЭЦ.

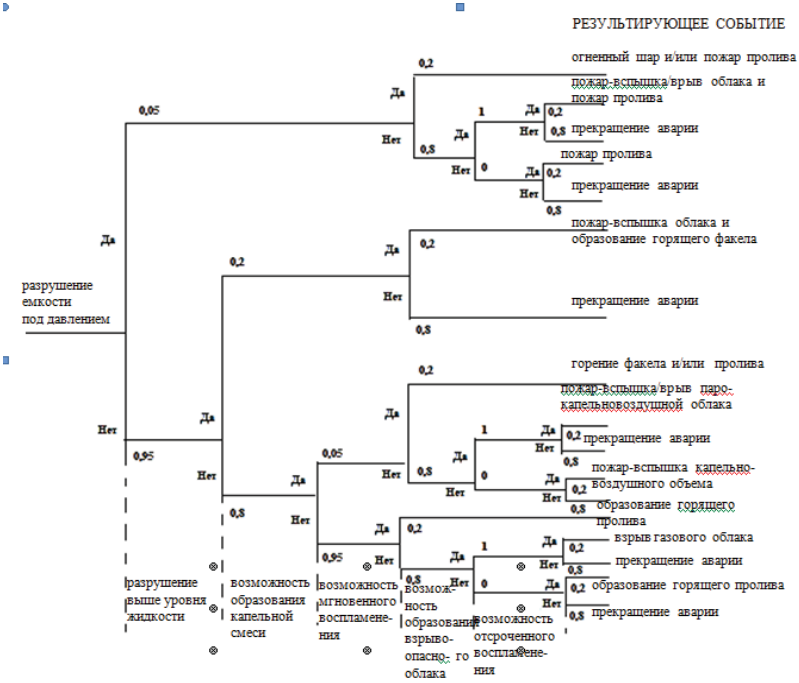


Рисунок 2 – «Дерево событий» – развитие аварии на ТЭЦ

Литература:

1. Пожары и пожарная безопасность в 2020 году: Статистический сборник / Полехин П.В., Чебуханов М.А., Козлов А.А., Фирсов А.Г., Сибирко В.И., Гончаренко В.С., Чечетина Т.А. – М.: ВНИИПО, 2021. – 112 с.

2. *Сеидахмедов Н.С.* Безопасность и снижение рисков при эксплуатации газомоторных компрессоров // Безопасность труда в промышленности. – 2020. – № 2. – С. 18-23.

3. Федеральный закон «О промышленной безопасности опасных производственных объектов» от 21.07.1997 № 116-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_15234/ (дата обращения 13.09.2021).

4. Федеральный закон «Технический регламент о требованиях пожарной безопасности» от 22.07.2008 № 123-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_78699/21fcb5ff5b429a80b88f9293abfe6b298ba05833/ (дата обращения 13.09.2021).

5. *Алехин Г.Г.* Анализ аварийных ситуаций на теплоэлектростанциях / Сборник статей по материалам VIII Всероссийской научно-практической конференции «Мониторинг, моделирование и прогнозирование опасных природных явлений и чрезвычайных ситуаций» (26 октября 2018 г. Железногорск). – Железногорск: ФГБОУ ВО Сибирская пожарно-спасательная академия ГПС МЧС России, 2018. – С. 231-236.

6. Анализ аварийных ситуаций на теплоэлектростанциях. – URL: http://lib.secuteck.ru/articles2/firesec/analiz-avariynyh-situatsiy-na-teploelektrostantsiyah (дата обращения 15.09.2021).

7. Приказ Федеральной службы по экологическому, технологическому и атомному надзору от 17 сентября 2015 года № 365 «Об утверждении руководства по безопасности «Методика оценки риска аварий на технологических трубопроводах, связанных с перемещением взрывопожароопасных газов». – URL: https://docs.cntd.ru/document/420302830 (дата обращения 15.09.2021).

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

Аннотация: Работа посвящена вопросам применения в работе интеллектуальной системы управления оперативного персонала городских рельсовых транспортных систем речевых технологий, которые имеют большое значение в задачах обучения персонала, при оценке результатов их работы и квалификации. Анализ распознанной информации имеет большое значение при решении задач обеспечения безопасности движения. Внедрение речевых технологий при распознавании голосовых команд существенно облегчит процесс взаимодействия инструктора и обучаемого с

Интеллектуальной системой прогнозирования, планирования и анализа работы диспетчеров городских рельсовых транспортных систем.

Ключевые слова: безопасность движения, речевые технологии, нейронные сети, машинное обучение, голосовые команды, распознавание, транспортная система

Основным направлением развития городских рельсовых транспортных систем (ГРТС) является переход к беспилотным технологиям и реализация принципов зеленой энергетики. Эти направления обеспечивают повышение безопасности ГРТС. Переход к беспилотным технологиям проходит поэтапно, базируется на использовании методов машинного обучения и технологий *Big Data*, которые строятся на анализе человеческого опыта [1]. В связи с этим актуальным является внедрение современных, в том числе и речевых, технологий в процесс автоматизированного централизованного управления ГРТС.

Интеллектуальная система управления (ИСУ) ГРТС включает в себя несколько специализированных систем, каждая из которых направлена на решение задач управления тем или иным видом ресурсов. Интеллектуальные системы прогнозирования, планирования и анализа работы операторов транспортных средств и диспетчеров ГРТС в рамках автоматизации процесса управления кадрами и их профессиональной подготовкой решают родственные задачи применительно к разным категориям сотрудников:

– обучение персонала;
– оценка качества подготовки персонала и его квалификации;
– оценка качества управления объектами ГРТС и выполнения работ;
– создание графика работы персонала.

При решении задач обучения персонала, оценки результатов их работы и квалификации большое значение имеет анализ речевой информации [2, 3]. Одновременно анализ этой информации значим и при решении задач обеспечения безопасности ГРТС: при построении систем контроля и управления доступом, проверке правомочности подачи команд управления в рамках решения задач многофакторной идентификации, верификации и различения дикторов [4]. Рассмотрению различных аспектов применения

речевых технологий в работе оперативного персонала ГРТС и посвящена данная работа.

Внедрение подсистемы распознавания голосовых команд существенно облегчит процесс взаимодействия инструктора и обучаемого с Интеллектуальной системой прогнозирования, планирования и анализа работы диспетчеров ГРТС.

К основным направлениям использования результатов обработки информации о голосовых командах, подаваемых оперативным персоналом, относятся:

– распознавание голосовых команд, подаваемых оперативным персоналом, и запись их в текстовый файл;

– использование текстового архива для анализа занятия и составления отчета о проведении занятия;

– получение информации о подаваемых командах, частоте и последовательности их подачи для дальнейшего использования в ходе автоматизации диспетчерского управления;

– распознавание команд из текстового или аудиофайла с целью автоматизации их выполнения в рамках функционирования средств электронного обучения;

– использование собранной информации для генерации голосовых команд в рамках функционирования средств электронного обучения;

– перенос накопленных результатов в ИСУ ГРТС в рамках централизованных систем управления движением транспортных средств при достижении достаточного уровня надежности.

К подсистеме распознавания голосовых команд предъявляются следующие требования:

– распознавание фраз независимо от их построения;

– информирование о поданной команде;

– передача команды на исполнение;

– протоколирование голосовых команд в текстовых и аудио файлах;

– автоматическое заполнение электронных приказов;

– наличие оборудования рабочих мест диспетчера напольными педалями для симплексной организации системы передачи информации;

– дополнение рабочего места инструктора сигнализацией исполнения голосовой команды;

– возможность отключения исполнения голосовой команды диспетчера инструктором;

– наличие перечня предусмотренных команд для ознакомления с ним обучаемого до тренировочного занятия.

В рамках исследования использовалась открытая модель по распознаванию русского языка, которая включает в себя скрытые марковские модели, модель смеси гауссовских распределений, глубокие нейронные сети, а именно Time-Delay Neural Networks (TDNN). Данная модель была выбрана на основе результата сравнительного анализа как модель, которая показывает самую высокую точность распознавания, по скорости работы незначительно проигрывая конкурентам. Данная модель и построенная на ее основе система для распознавания речи Kaldi подходит для научных исследований больше, чем ее аналоги [5-7].

Целью создания подсистемы распознавания голосовых команд является автоматизация процесса управления движением транспортных средств (ТС) при обучении оперативных работников (обучаемый – диспетчер) ГРТС путем автоматизированного распознавания голосовых команд диспетчера для исключения механического взаимодействия с пультом управления, которое приведет к уменьшению количества ошибок обучаемого.

В качестве основного требования к разрабатываемой системе 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 были решены следующие задачи:

1. Разработан классификатор текста по типу сообщения в нем. Каждое из предложений может быть отнесено к одному из возможных классов: информационное сообщение, управляющая команда, приказ, нераспознанное сообщение.

Для решения задачи классификации предложений используетсяется сверточная нейронная сеть. На вход нейронной сети поступает матрица размером 36×300, где размер 36 – это количество токенов (слов) в предложении (глубина текста), а 300 – глубина вектора эммбендинга для каждого слова. Преобразование

слова в числовой вектор осуществляется на основе использования предобученной на корпусе литературного текста нейронной сети (размер корпуса более 150Гб). Глубина текста была выбрана исходя из 0,9-квантиля статистического распределения количества слов в предложении в собранном множестве данных.

В результате обучения нейронной сети классификации предложений на протяжении 100 итераций обучения была достигнута точность прогноза порядка 94-96% на тестовой выборке. Данный результат позволяет достаточно точно определять класс текста.

2. Сформирован классификатор управляющих команд.

Структура команд может включать в себя следующие элементы:

– субъект – адресат (может быть один на несколько команд);

– объект, на управление которым направлена команда, сценарий поведения которого она задает;

– непосредственно команда;

– уточнение места или времени, определяющих конкретную реализацию команды.

Разработана семантическая сеть, отражающая связи элементов в команде.

Команды можно классифицировать по объекту управления (команды управления маршрутами, команды управления стрелками и сигналами и т.д.) и типу действий (запрет на движение, разрешение на движение и др.).

3. Разработан алгоритм классификации команд диспетчера на основе обработки текста.

Алгоритм состоит из следующих шагов:

– формируется классификатор возможных видов эталонных команд, в котором каждое слово в команде представляется в виде числового вектора на основе предобученной нейронной сети;

– для каждого слова в тексте вычисляется числовой вектор на основе предобученной нейронной сети;

– каждая эталонная команда «скользящим окном» проходит по тексту и вычисляет расстояние между матрицей эталонного вектора и участком анализируемого текста с использование метрики;

– в случае, если расстояние между эталонным текстом и

окном меньше заданного порога t (в рамках текущего исследования использовался порог $t = 0.5$), то система выдает информацию о том, что команда найдена в тексте.

Оценку качества предложенного метода распознавания слитной речи проведем по следующим показателям:

– доля правильно распознанных команд;
– доля ошибочно распознанных команд;
– доля нераспознанных команд.

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.

4. Разработана структурная схема подсистемы распознавания голосовых команд, которая включает элементы, реализующие следующие действия:

– генерация аудиофайлов;
– преобразование аудиофайла в текст;
– разделение диалога на блоки-предложения, которые используются для классификации;
– лемматизация;
– нормализация текста;
– эмббединг;
– классификация текста по типу сообщения в нем – отнесение каждого из предложений к одному из возможных классов: информационное сообщение, управляющая команда, приказ, нераспознанное сообщение;
– классификация текста внутри класса путем расчета метрики между входным текстом и вектором эталонных примеров;
– поиск наименования субъектов, объектов, уточнения места или времени в тексте на основе информации о классе команды;
– в случае, если сообщение требует выполнения команды и реализации конкретных действий, данные о команде поступают на вход блоков управления и исполнения средств электронного обучения.

В дальнейшем планируется проверка работы разработанных алгоритмов на увеличенном объеме данных.

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. *Алексеев В.М., Баранов Л.А., Кулагин М.А., Сидоренко В.Г.* Построение архитектуры интеллектуальной системы управления городской рельсовой транспортной системой // Мир транспорта. – 2021. – Т. 19. – № 1 (92). – С. 18-46.

2. *Баранов Л.А., Сидоренко В.Г., Балакина Е.П., Логинова Л.Н.* Интегрированный подход в обучении оперативных работников городских рельсовых транспортных систем // Наука и техника транспорта. – 2021. – № 2. – С. 22-31.

3. *Горелик В.Ю., Краишкин А.В.* Увеличение надежности работы диспетчера по управлению движением за счет дополнительного канала передачи информации // Наука и техника транспорта. – 2005. – № 1. – С. 78-81.

4. *Шалимов И.А., Милошенко А.А.* Обзор моделей идентификации и информативные параметры речевого сигнала // Специальная техника. – 2009. – №5. – С. 37-46.

5. *Khromov S.K, Kulagin M.A., Sidorenko V.G.* Machine Learning Application For Support For Automated Control Systems Users / Journal of Physics: Conference Series. – Volume 1680. – Computer-Aided Technologies in Applied Mathematics. – 2020. – P. 012019.

6. *Беленко М.В., Балакшин П.В.* Сравнительный анализ систем распознавания речи с открытым кодом // Международный научно-исследовательский журнал. – 2017. – №. 4-4 (58). – С. 13-18.

7. *Марковников Н.М., Кипяткова И.С.* Аналитический обзор интегральных систем распознавания речи // Труды СПИИРАН. – 2018. – №3(58). – С. 77-110.

Анохин А.М.

Анализ прикладных путей повышения метрологической надежности измерительных преобразователей

Аннотация: Рассмотрены вопросы обеспечения метрологической надежности измерительных преобразователей физических величин. Намечены пути повышения качества физических измерений, связанные с выбором элементной базы, конкретизацией схемотехнических решений, организацией режима работы преобразователей.

Ключевые слова: сенсорезистор, первичные преобразователи, пороговый переключатель, самонагрев, терморегулирование, сенситивный резистор, терморезистор

Качество физических измерений оценивается по степени присутствия в результатах измерений систематических погрешностей методического и инструментального происхождения.

Большинство применяемых в электронной сенсорике первичных преобразователей является сенситивными резисторами, то есть резисторами, активное сопротивление которых чувствительно к измеряемой физической величине какой-либо природы. Сенситивные резисторы включаются в цепь измерительного моста и по характеру изменения рабочего тока резистора, модулируемого воздействием физической величины, судят об этой величине. Физическим носителем измерительного сигнала является рабочий ток сенсорезистора. Это приводит к выделению в преобразователе тепловой энергии, т.е. к его самонагреву и росту избыточной температуры. Фактор самонагрева особенно негативен в плане обеспечения качества метрологических характеристик и функциональной надежности измерительных преобразователей. Его последствия таковы:

– тепловая инерционность, то есть потребность в дополнительном времени выхода на установившийся тепловой режим работы преобразователя, соответствующий заданному уровню мощности измерительного сигнала;

– температурный «смаз» характеристики преобразования, то есть неуправляемый переход рабочей точки с одной характеристики

на другую в температурном семействе характеристик при изменении уровня (мощности) измерительного сигнала;

– повышение порога чувствительности и общей погрешности измерения вследствие увеличения тепловых и токовых шумов преобразователя;

– влияние повышенной (избыточной) температуры первичного преобразователя на температуру измеряемой среды или объекта в точке измерения, искажающее объективность показаний;

– ускорение процесса старения структуры первичного преобразователя, интенсификация отказов в его работе и общее снижение достоверности результатов измерений.

Перечисленные факторы приводят к определенным трудностям в развитии непосредственно сенсорных функций измерительных преобразователей и главной проблемой, препятствующей улучшению их метрологических характеристик, является фактор самонагрева первичного преобразователя рабочим, т.е. измерительным током.

В контексте данной проблемы эффективным представляется путь исключения систематических погрешностей измерений еще до начала измерений (в частности температурных, вызванных самонагревом), т.е. на этапе проектирования измерительных средств.

Для этого необходимо:

– отказаться от использования рабочего тока первичного преобразователя в качестве физического носителя измерительной информации, то есть в качестве информативного параметра измерительного сигнала;

– использовать в качестве информативного параметра измерительного сигнала преобразователя порогового потенциала переключения бистабильной полупроводниковой структуры из закрытого состояния в открытое.

– применить в качестве бистабильных полупроводниковых структур схемы негатронов с переключательной вольтамперной характеристикой S-типа (однопереходные транзисторы, S-диоды, тиристоры и схемы транзисторно-резисторных эквивалентов тиристора);

– исследовать зависимости порога переключения S-негатрона от воздействия физических величин различной природы и применить их для построения измерительных преобразователей;

– организовать импульсный режим измерения путем опроса состояния проводимости S-негатрона нарастающими по амплитуде счетными импульсами со стробированием по пороговой амплитуде.

Итак, для улучшения метрологических характеристик первичных преобразователей, прежде всего, необходимо насколько схемотехнически возможно минимизировать рабочий ток первичного преобразователя и отказаться от его использования в качестве физического носителя измерительной информации, то есть в качестве информативного параметра измерительного сигнала. В качестве информативного параметра измерительного сигнала целесообразно использовать пороговый потенциал переключения бистабильной полупроводниковой (п/п) структуры из закрытого состояния в открытое. При этом закрытое состояние как высокоомное (условно непроводящее) должно быть первичным, а открытое низкоомное – вторичным. В бинарном представлении это логические «0» и «1» (или наоборот) по аналогии с работой триггера или ключа напряжения.

Для реализации такого подхода необходимо решить три задачи:

– какую элементную базу использовать в качестве бистабильной полупроводниковой структуры?

– как придать бистабильной полупроводниковой структуре сенсорные свойства?

– как организовать режим ее работы и в каком схемотехническом исполнении?

Бистабильное состояние в работе присуще полупроводниковым приборам класса «негатрон», то есть приборам на вольтамперной характеристике (ВАХ) которых имеется участок с отрицательным дифференциальным сопротивлением [1]. Среди них различают Λ-, N- и S-типы в зависимости от формы ВАХ. В качестве сенсорной бистабильной структуры целесообразно использовать S-негатроны, на ВАХ которых начальный участок высокоомный (соответствует закрытому состоянию) и протяженный.

К подклассу S-негатронов относятся S-диоды, одноперехо́дные транзисторы (ОПТ), тиристоры и их транзисторно-резисторные аналоги. Традиционная область применения S-негатронов по их прямому функциональному назначению – построение разного рода генераторных схем, а также силовых переключателей на тиристорах

[2]. По этой причине разработчики аппаратуры применяли к ним всевозможные приемы температурной стабилизации характеристик и в первую очередь температурной стабилизации порогового потенциала переключения.

Однако, если вместо обеспечения температурной инвариантности, еще более активировать температурную зависимость порога переключения, то таким образом можно получить температурочувствительный пороговo-переключательный первичный преобразователь. Его удобно и логично назвать «свитч-сенсор». Такого рода температурные и световые свитч-сенсоры были совместно разработаны московскими институтами ИПУ РАН и ГИРЕДМЕТ на базе технологии S-диода. Они обладают уникальной чувствительностью, в несколько раз превышающей чувствительность лучших аналогов (за это качество удостоены множества высших наград на международных форумах), и вполне могут быть применены для построения на их основе измерительных преобразователей нового типа.

Если на свитч-сенсор, измеряющий какую-либо физическую величину, подать от генератора питания нарастающее напряжение и прервать его в тот момент, когда оно достигнет порогового уровня, то по длительности сформировавшегося таким образом на выходе генератора, т.е. на входе свитч-сенсора, пилообразного импульса можно определить высоту порога и по ней установить значение из меряемой ФВ. При этом через структуру свитч-сенсора успеет пройти только один очень короткий импульс открытого состояния, длительность которого определяется временем срабатывания цепи обратной связи, прерывающей питание (порядка наносекунды).

Команду на самопрерывание целесообразно подавать по переднему фронту первого импульса, успевшего пройти на выход свитч-сенсора. Назовем этот импульс «строб-импульс отклика», а пилообразный импульс на входе свич-сенсора – «импульс опроса». Соотношение длительностей этих импульсов определяет мощность самонагрева свитч-сенсора. Она может быть на много порядков меньше, чем в традиционном варианте. При этом крутизну переднего фронта импульса опроса можно использовать как параметр управления температурой самонагрева и таким образом свести ее к очень малому, практически не влияющему на результат измерения, значению. Непрерывно подавая импульсы

опроса на свитч-сенсор и измеряя их длительность числоимпульсным методом с использованием высокочастотных счетных импульсов заполнения, можно прецизионно измерять ФВ с частотой опроса в несколько сотен килогерц [3].

Для метрологического обеспечения измерений физических величин свитч-сенсорами по предлагаемой методике необходимо ввести новое понятие характеристики преобразования, где в качестве функции вместо параметра «ток на выходе сенсора» использовать параметр «пороговое напряжение на входе сенсора», и назвать ее «пороговая характеристика преобразования» (ПХП). То есть, ПХП отображает зависимость значений порогового напряжения переключения на входе свитч-сенсора от значений измеряемой физической величины. Пороговая характеристика преобразования для температурного свич-сенсора изображена на рисунке 1.

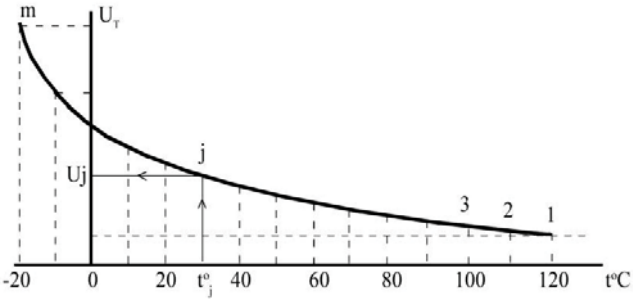


Рисунок 1 – Пороговая характеристика преобразования

Современные средства памяти и организации доступа к ней (например, флэш-память) позволяют запоминать координаты ПХП практически в любом объеме и с любым дискретом. Поэтому наряду с аналого-цифровым вариантом режима работы свитч-сенсора *возможна реализация полностью цифрового варианта* [4]. Для этого необходимо сформировать напряжение питания в виде непрерывно следующих серий (пачек) нарастающих по амплитуде очень коротких импульсов опроса, где все импульсы внутри пачки *нумерованы*. Тогда первый, прошедший через структуру свитч-сенсора импульс, то есть, пороговый импульс, сформирует

строб-импульс отклика, который укажет номер порогового импульса внутри пачки импульсов опроса и соответствующий координатный номер точки на ПХП (соответственно, значение измеряемой физической величины). Интервал времени открытого состояния S-мегатрона определяется длительностью открывающего импульса на уровне порога. При такой малой длительности открытого состояния свич-сенсора внутри измерительного цикла выделяемая в нем тепловая энергия и его самонагрев практически сводятся к нулю [5].

Литература:

1. *Дождиков В.Г., Лифанов Ю.С.* Энциклопедический словарь по радиоэлектронике, оптоэлектронике и гидроакустике. – М.: Энергия, 2008. – 612 с.

2. *Биберман Л.И.* Широкодиапазонные генераторы на негатронах. – М.: Радио и связь, 1982. – 88 с.

3. Патент РФ №2412429, Кравченко А.М. Датчик-измеритель физических величин. Бюл. № 5, 2011.

4. Патент РФ № 2344384, Кравченко А.М. Цифровой способ измерения температуры и устройство для его реализации. Бюл. №2, 2009.

5. *Кравченко А.М., Анохин А.М.* Новый подход к построению терморегуляторов на основе S-негатрона // Датчики и системы. – 2013. – №1. – С. 34-38.

Торгашев Р.Е.

Комплексный геоэкологический мониторинг лесных геоэкосистем Московского столичного региона

Аннотация: В работе изложено современное состояние геоэкологического мониторинга лесных геоэкосистем Московского столичного региона. Автором определено содержание программы мониторинга. Рассмотрен геоэкологический мониторинг отдельных природных сред с привлечением инструктивных материалов, методических рекомендаций. В работе кратко изложены виды исследований и аналитическое обеспечение при

организации экомониторинга лесных геоэкосистем Московского столичного региона.

Ключевые слова: геоэкологический мониторинг, лесопользование, геоэкосистема, Московский столичный регион, антропогенные воздействия, ландшафт, технологии спутниковой съемки

В центральной части Русской (Восточно-Европейской) равнины располагается Московский столичный регион (далее – МСР). Границы МСР очертаны междуречьем рек Волги и Оки, на рубеже постепенной смены (с севера на юг) типичных естественных природных ландшафтов подзоны южной тайги на границе с Тверской областью к лесостепным формам местности на правобережье р. Оки. В геоструктурном отношении данная территория занимает южный склон Московской синиклизы.

Современный рельеф МСР сформировался в процессе неоднократных оледенений с последующими флювиальными процессами времен деградации ледников. Ландшафтно-геоэкологический облик Московской области и города Москвы достаточно своеобразен. Объясняется это следующими особенностями: вряд ли возможно встретить другой такой многомиллионный столичный мегаполис, в округе которого в наше время сохранились большие массивы лесов, болот, истоки малых и средних рек, охотничьи угодья, компактные острова непреобразованных географических ландшафтов и патриархального уклада. И рядом со всем этим – все черты крайне природоемкой индустриализации: огромные урабанизационные территории с оборонными объектами и предприятиями военно-промышленного комплекса (ВПК); большие участки разрушенных и сильно загрязненных земель, сведения лесов, истощения водных ресурсов; высокая отходность производства и множество источников загрязнения окружающей среды региона.

Промышленная нагрузка особенно тесно связана с плотностью потребления энергоресурсов, но именно последний показатель имеет самые высокие корреляции с загрязнением воздушной, водной среды и лесного комплекса. Что касается устойчивости лесных геоэкосистем, то за последние четверть века установлено, что чем выше промышленная нагрузка и энергетика района, тем

ниже устойчивость лесных экосистем этой территории. Все это создает ситуацию высокой социально-экологической напряженности [1,2].

В пределах МСР выделяется пять крупных геоландшафтных физико-географических областей, в разной степени преобразованных антропогенными воздействиями:

– А. Верхневолжская зандровая равнина;
– Б. Смоленско-Окская пологоувалистая эрозионная равнина;
– В. Москворецко-Окская пологувалистая эрозионная равнина;
– Г. Мещерская аллювиально-зандровая равнина;
– Д. Заокское эрозионное плато.

Ежегодное возрастающее воздействие на природу загрязнения МСР, связанное с техногенными выбросами, определяет необходимость выявления и глубины этого воздействия на биогеоценозы и почвы, как их компоненты. Одним из необходимых условий выявления загрязнения и токсичного воздействия его на почвы послужило создание системы показателей контроля и прогнозирования уровня загрязнения почв, теоретическое обоснование которой приведено в научных аналитических работах Г.В. Добровольского (1915-2013).

Для выявления показателей почвенного мониторинга проводятся исследования большого объема почвенных характеристик в условиях загрязнения разной интенсивности и качества. Осуществление проведения почвенного мониторинга, как подсистемы мониторинга лесных геоэкосистем, преследует три важные цели: обнаружение неблагоприятных изменений состава и свойств почв под влиянием различных факторов, контроль и надзор за состоянием почв для выдачи соответствующих рекомендаций по правоприменению регулирующих мероприятий и проведению оздоровительных мероприятий, чтобы в целях предотвращения заражения лесной растительности, произрастающих на данных почвах.

При проведении геоэкологического мониторинга наблюдения за состоянием почв целесообразно проводить в тесной связи с мониторингом других компонентов геоэкосистемы: состава и количества атмосферных выпадений, состояния древостоя и других компонентов фитоценоза, состава и состояния зооценоза,

микробиоценоза, состава почвенно-грунтовых и других природных зон.

Объектом почвенного мониторинга в лесных геоэкосистемах служат, прежде всего, дернина (лесная подстилка) и верхний минеральный почвенный горизонт. При этом важно наблюдать за количеством, массой и химическим составам опада листвы и хвои. Существенное внимание целесообразно уделять биогеохимическим циклам биофильных элементов, ответственным за устойчивость биогеоценозов, изменению их или важнейших их звеньев под влиянием загрязнения.

Мониторинг почв лесных геоэкосистем МСР должен базироваться на достаточном объеме исходных характеристик почв региона исследований. Это, прежде всего, картографические материалы по составу и структуре почвенного покрова, характеристик минералогического, гранулометрического и химического состава, физических и химико-физических свойств.

Помимо вопросов, что и где измерять, необходимо знать, в каком количестве производить необходимые измерения, чтобы сезонное и пространственное варьирование измеряемых параметров не искажало или не затушевывало изменение их состояния под влиянием атмосферного загрязнения.

До настоящего времени еще не для всех параметров разработаны оценка и ранжирование антропогенного воздействия на почву, прямого и косвенного (в основном через биоту), оценка и ранжирование ответного изменения свойств почв, оценка и ранжирование параметров устойчивости почв при разного рода антропогенном воздействии.

Одним из наиболее эффективных путей сохранения окружающей среды, охраны генофонда органической и неорганической природы, лесовосстановления, поддержания геоэкологического равновесия является установление охранного режима на определенных природных территориях, т.е. ограниченное или полное исключение их из сферы хозяйственного использования.

Для повышения геоэкологической устойчивости молодого подроста лесополосы лесных геоэкосистем МСР и создания разнообразных травянистых ассоциаций необходимо осуществлять

регулирование и перераспределение определенным образом антропогенную нагрузку.

Следует понимать, что площадь большинства охраняемых и предложенных к охране территорий очень невелика: от нескольких квадратных метров до нескольких сотен га. Степень устойчивости биогеэкосистем, а, следовательно, и успешность их охраны, находятся в прямой зависимости от размера занимаемой ими территории. Крупные объекты в определенной степени способны к саморегулированию и самовосстановлению, тогда как небольшие участки крайне уязвимы и резко реагируют даже на мельчайшие отрицательные воздействия. Поэтому для уязвимых объектов необходимо выделять охранные зоны и разрабатывать режимы их хозяйственного освоения и лесопользования. Для этого следует разработать предложения о формировании вокруг скоплений, особо охраняемых и предлагаемых к охране участков природоохранных зон щадящего режима, которые должны служить, прежде всего, сохранению более ценных природных объектов и поддержанию геоэкологического равновесия на территории Московской области. Наличие в этих зонах рекреационных пространств и территорий с ограниченным хозяйственным использованием при специальном их оборудовании может способствовать решению проблемы сочетания массового отдыха на природе и ее охраны.

В ходе постоянного геоэкологического мониторинга, проводимого уже в первые два десятилетия 21 века, отметим, что в условиях густонаселенной и высокоурбанизированной, хорошо развитой в хозяйственном отношении и интенсивно используемой в рекреационных целях Московской области выделение пусть даже и достаточно густой сети относительно мелких охраняемых объектов не может решить проблемы сохранения природы. Необходимо вносить «Дополнения и изменения к кадастру особо охраняемых природных территорий Московской области», запрещать захватывать территории подобного содержания дачникам, жителям населенных пунктов, оформлять в собственность земли данной категории и осуществлять самовольную хозяйственную деятельность, нарушая природоохранное экологическое законодательство. Пересмотреть и расширить границы и количество заказников, памятников природы биологического характера, национальных парков и заповедников, а также культурных

экологических ландшафтов. Необходимо создание научно обоснованной системы достаточно обширных охраняемых территорий, для которых должны быть разработаны оптимальные формы и режимы охраны и хозяйственного лесопользования.

Предлагаем установить охранный режим еще для более чем 100 памятников природы и заказников общей площадью 100 тыс. га. Также важным элементом системы охраняемых природных территорий являются «зеленые зоны» городских округов Подмосковья и курортные леса региона. Дополняют систему и сохраняемые усадебные парки, и другие искусственные насаждения.

Для успешного функционирования все элементы системы должны быть связаны между собой природными руслами, которые могут обеспечить связь локальных популяций видов и обмен лесогенным материалом, сохранить важнейшие миграционные пути, обеспечить пополнение и естественную динамику сообществ. Роль таких зеленых лесозащитных коридоров должны выполнять лесные защитные и охранные полосы вдоль железных дорог, автомагистралей, водоохранные лесные массивы вдоль рек, ручьев, полосы отчуждения вдоль коммуникаций, участки естественной растительности среди пашен и полей, в оврагах, на неудобях, где во многих случаях успешно существуют виды местной фауны и флоры, в том числе редкие и исчезающие.

Для обеспечения лучшей сохранности флористического сообщества МСР был введен запрет на сбор свыше 100 видов растений, на сбор всех видов дикорастущих растений в пределах г. Москвы, лесопаркового защитного пояса в парках и лесопарках. Запрещена торговля всеми видами дикорастущих декоративных и лекарственных растений в пределах региона.

Одним из наиболее эффективных, но дорогостоящих видов наблюдения за лесными растительными сообществами МСР является геоэкомониторинг, основанный на технологиях спутниковой съемки. В рамках сотрудничества с подразделениями ФГУП «Рослесинфорг» специалистами «СКАНЭКС» была создана и протестирована методика высокопериодичного мониторинга лесопользования.

В результате проделанной работы специалистами был создан прообраз информационной системы мониторинга лесопользования

на базе геопортальных технологий, и методика оперативного обновления данных, основанная на технологиях прямого приема спутниковой информации и стандартизированных процедурах технологической и тематической обработки данных.

«Работы по созданию и тестированию методики были выполнены специалистами «СКАНЭКС» с использованием технологических возможностей компании по оперативному приему спутниковой информации. Обработка данных проводилась в собственном программном обеспечении «СКАНЭКС». Прообраз информационной системы был создан с использованием технологии ScanExGeoMixer» [3].

Литература:

1. *Куликова Г.Г., Новиков В.С., Тихомиров В.Н., Варлыгина Т.И.* Опыт разработки системы охраняемых природных территорий Московской области / Тезисы докладов VII Делегатского съезда Всесоюзного ботанического общества (11-14 мая 1983 г. Донецк). – Л.: «Наука», 1983. – С. 11-14.

2. *Куликова Г.Г.* Сохранение ценных ботанических объектов в Московской области / Изучение редких и охраняемых видов травянистых растений. – М.: МФГО СССР, 1983. – С. 65-69.

3. Круглогодичный мониторинг лесопользования. – URL: https://new.scanex.ru/thematic/projects/monitoring-lesopolzovaniya/ (дата обращения 14.10.2021).

Мусаев В.К.

Математическое моделирование сейсмических волн напряжений в полуплоскости вертикальной полостью из резины: соотношение ширины к высоте один к десяти

Аннотация: Решена задача о математическом моделировании нестационарных упругих волн напряжений в полуплоскости с полостью, заполненной резиной (соотношение ширины к высоте один к десяти), при сейсмическом воздействии в виде ступенчатой функции. Решается система уравнений из 8016008 неизвестных. В характерных областях исследуемой задачи получены

контурные напряжения и компоненты тензора напряжений. Полость (соотношением ширины к высоте один к десяти), заполненная резиной, уменьшает величину упругого контурного напряжения.

Ключевые слова: механика экстремальных процессов, математическое и численное моделирование; волновая теория сейсмической безопасности, комплекс программ Мусаева В.К., сейсмическое воздействие, вертикальная прямоугольная полость, резина, контурные напряжения

В работе рассматривается математическое моделировании нестационарных сейсмических волн в упругой полуплоскости с вертикальной прямоугольной полостью (соотношение ширины к высоте один к десяти), заполненной резиной.

Некоторая информация о волнах напряжений приведена в работах [1-5].

В работах [1,2] приведена информация о верификации моделирования нестационарных волн напряжений в деформируемых телах с помощью рассматриваемого численного метода, алгоритма и комплекса программ.

Рассматривается задача о воздействии плоской продольной нестационарной сейсмической волны (рисунок 1) параллельной свободной поверхности упругой полуплоскости с полостью заполненной резиной (соотношение ширины к высоте один к десяти) (рисунок 2).

Исследуемая задача впервые решена Мусаевым В.К. с помощью разработанной методики, алгоритма и комплекса программ [1-5] .

Расчеты проводились при следующих единицах измерения: килограмм-сила (кгс); сантиметр (см); секунда (с).

От точки F параллельно свободной поверхности $ABEFG$ приложено нормальное напряжение σ_x, которое при $0 \le n \le 11$ ($n = t/\Delta t$) изменяется линейно от 0 до P, а при $n \ge 11$ равно P ($P = \sigma_0$, σ_0 = 0,1 МПа (1 кгс/см^2)).

Граничные условия для контура $GHIA$ при $t > 0$ $u = v = \dot{u} = \dot{v} = 0$. Отраженные волны от контура $GHIA$ не доходят

до исследуемых точек при $0 \le n \le 1000$. Контур $ABEFG$ свободен от нагрузок, кроме точки F.

Расчеты проведены при следующих исходных данных.

Для области $ABCDEFGHI$: $H = \Delta x = \Delta y$; $\Delta t = 1{,}393 \cdot 10^{-6}$ 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.

Для области $BEDC$: $H = \Delta x = \Delta y$; $\Delta t = 0{,}934 \cdot 10^{-4}$ с; $E = 2{,}0$ МПа (20,39 кгс/см^2); $\nu = 0{,}5$; $\rho = 0{,}93 \cdot 10^3$ кг/м^3 ($0{,}948 \cdot 10^{-6}$ кгс с^2/см^4); $C_p = 53{,}55$ м/с; $C_s = 26{,}78$ м/с.

При расчетах принимается минимальный шаг по времени $\Delta t = 1{,}393 \cdot 10^{-6}$ с.

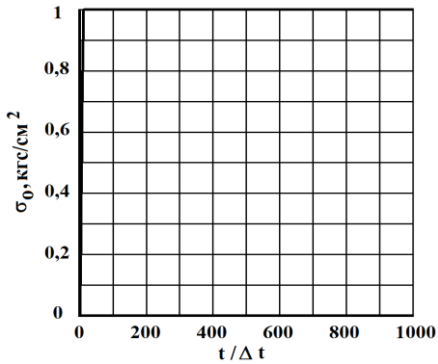


Рисунок 1 – Воздействие в виде функции Хевисайда

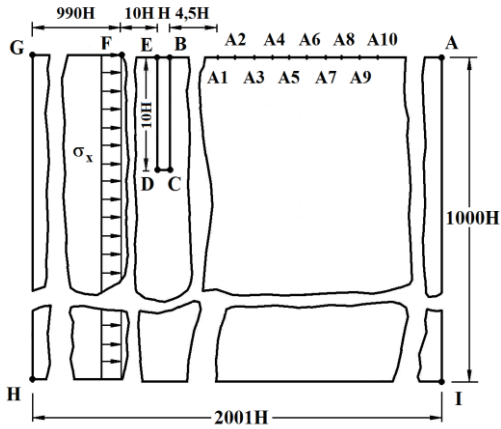


Рисунок 2 – Постановка задачи о воздействии плоской продольной сейсмической волны на упругую полуплоскость с полостью, заполненной резиной (соотношение ширины к высоте один к десяти)

На границе материалов с разными свойствами приняты условия непрерывности перемещений.

Решается система уравнений из 8016008 неизвестных.

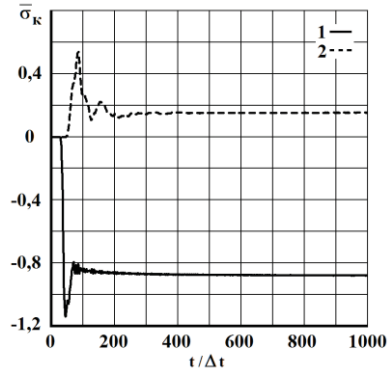


Рисунок 3 – Изменение упругого контурного напряжения $\bar{\sigma}_k$ во времени $t/\Delta t$ в точке $A1$: 1 – в задаче без полости; 2 – в задаче с полостью, заполненной резиной (соотношение ширины к высоте один к десяти)

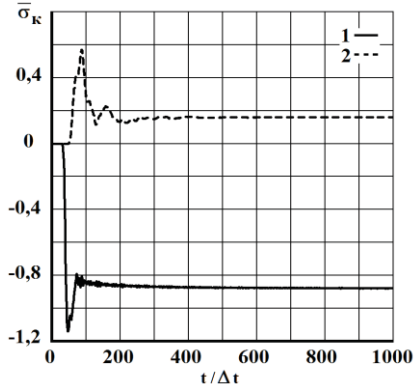


Рисунок 4 – Изменение упругого контурного напряжения $\overline{\sigma}_k$ во времени $t/\Delta t$ в точке $A2$: 1 – в задаче без полости; 2 – в задаче с полостью, заполненной резиной (соотношение ширины к высоте один к десяти)

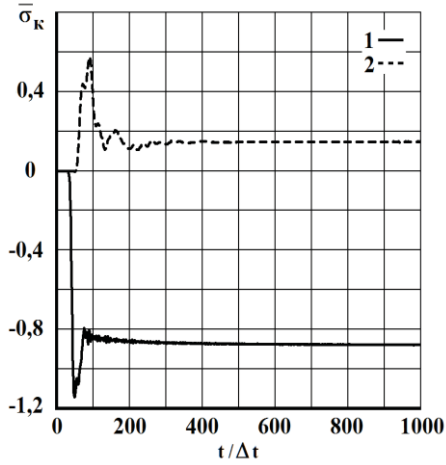


Рисунок 5 – Изменение упругого контурного напряжения $\overline{\sigma}_k$ во времени $t/\Delta t$ в точке $A3$: 1 – в задаче без полости; 2 – в задаче с полостью, заполненной резиной (соотношение ширины к высоте один к десяти)

В точках *A*1–*A*3 (рисунок 1), получено изменение упругого контурного напряжения $\overline{\sigma}_k$ ($\overline{\sigma}_k = \sigma_k / |\sigma_0|$) во времени n (рисунок 2 –5), находящихся на свободной поверхности упругой полуплоскости: 1 – в задаче без полости; 2 – в задаче с полостью заполненной нефтью (соотношение ширины к высоте один к десяти).

Расстояние между точками: *A*1 и *A*2 равно *H*; *A*2 и *A*3 равно *H*; *A*3 и *A*4 равно *H*; *A*4 и *A*5 равно *H*; *A*5 и *A*6 равно *H*; *A*6 и *A*7 равно *H*; *A*7 и *A*8 равно *H*; *A*8 и *A*9 равно *H*; *A*9 и *A*10 равно *H*).

Выводы

1. Для прогноза природной (стихийной) безопасности объектов при землетрясениях применяется численное моделирование при нестационарных волновых воздействиях. Разработаны методика, алгоритм и комплекс программ для решения линейных двумерных (плоских) задач сложной формы при волновых воздействиях.

2. Решена задача о математическом моделировании нестационарных упругих волн напряжений в полуплоскости с полостью, заполненной резиной (соотношение ширины к высоте один к десяти), при сейсмическом воздействии. Решается система уравнений из 8016008 неизвестных. Полость, заполненная резиной (соотношение ширины к высоте один к десяти), уменьшает величину упругого контурного 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.* Численное моделирование нестационарных контурных напряжений в полуплоскости с полостью (соотношение ширины к высоте один к пяти) с помощью волновой теории

сейсмической безопасности / Опасные природные и техногенные процессы в горных регионах: модели, системы, технологии. Коллективная монография. – Владикавказ: ГФИ ВНЦ РАН, 2019. – С. 446-451.

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 волн напряжений при сосредоточенном вертикальном воздействии в виде треугольного импульса: задача Лэмба // Строительная механика инженерных конструкций и сооружений. – 2021. – № 2. – С. 112-120.

Мусаев В.К.

Волновая теория сейсмической безопасности в задаче о моделировании напряжений в полуплоскости с вертикальной полостью из металла (соотношение ширины к высоте один к десяти)

Аннотация: Решена задача о математическом моделировании нестационарных упругих волн напряжений в полуплоскости с полостью, заполненной металлом (соотношение ширины к высоте один к десяти), при сейсмическом воздействии в виде ступенчатой функции. Решается система уравнений из 8016008 неизвестных. В характерных областях исследуемой задачи получены контурные напряжения и компоненты тензора напряжений. Полость (соотношением ширины к высоте один к десяти), заполненная металлом, увеличивает величину упругого контурного напряжения. Это связано с увеличением акустической жесткости полости.

Ключевые слова: волновая теория сейсмической безопасности, комплекс программ Мусаева В.К., сейсмическое воздействие, ступенчатая функция,

вертикальная прямоугольная полость, металл, акустическая жесткость, контурные напряжения

В работе приводится численное решение задачи о моделировании нестационарных сейсмических волн в упругой полуплоскости с вертикальной прямоугольной полостью (соотношение ширины к высоте один к десяти), заполненной металлом.

Некоторые вопросы в области моделирования нестационарных динамических задач рассмотрены в следующих работах [1-6].

В работах [2,3] приведена информация о физической достоверности и математической точности моделирования нестационарных волн напряжений в деформируемых телах с помощью рассматриваемого численного метода, алгоритма и комплекса программ.

Принимая во внимание определение матрицы жесткости, вектора инерции и вектора внешних сил для некоторого тела, записываем приближенное значение уравнения движения в теории упругости [2-6]

$$\overline{H}\ddot{\vec{\Phi}}+\overline{K}\vec{\Phi}=\vec{R}\,,\ \vec{\Phi}\big|_{t=0}=\vec{\Phi}_0\,,\ \dot{\vec{\Phi}}\big|_{t=0}=\dot{\vec{\Phi}}_0\,, \qquad (1)$$

где: $\overline{H}$ – матрица инерции; $\overline{K}$ – матрица жесткости; $\vec{\Phi}$ – вектор узловых упругих перемещений; $\dot{\vec{\Phi}}$ – вектор узловых упругих скоростей перемещений; $\ddot{\vec{\Phi}}$ – вектор узловых упругих ускорений; $\vec{R}$ – вектор узловых упругих внешних сил.

Таким образом, с помощью метода конечных элементов в перемещениях, линейную задачу с начальными и граничными условиями привели к линейной задаче Коши (1).

Задание различных физических свойств, для каждого конечного элемента, позволяет с помощью метода конечных элементов в перемещениях решать двумерные плоские динамические задачи теории упругости для областей различной формы [2-6].

Интегрируя по временной координате соотношение (1) с помощью конечноэлементного варианта метода Галеркина, получим двумерную явную двухслойную схему [2-6]

$$\dot{\vec{\Phi}}_{i+1}=\dot{\vec{\Phi}}_i+\Delta t\overline{H}^{-1}(-\overline{K}\vec{\Phi}_i+\vec{R}_i)\,,\ \vec{\Phi}_{i+1}=\vec{\Phi}_i+\Delta t\dot{\vec{\Phi}}_{i+1}\,, \qquad (2)$$

Таким образом, из системы с бесконечным числом неизвестных перешли к системе с конечным числом неизвестных (2).

Общая теория численных уравнений математической физики требует для этого наложение определенных условий на отношение шагов по временной координате и по пространственным координатам, а именно [2-6]

$$\Delta t = k \frac{\min \Delta l_i}{C_p} \ (i = 1, 2, 3, ..., r), \tag{3}$$

где: Δt – шаг по временной координате; Δl – длина стороны конечного элемента; r – общее число конечных элементов.

Аналитическое исследование устойчивости явной двухслойной схемы связано с большими трудностями, поэтому устойчивость явной двухслойной схемы исследуем с помощью численного эксперимента [2-6].

Результаты численного эксперимента показали, что при k = 0,5 обеспечивается устойчивость явной двухслойной схемы в перемещениях для внутренних и граничных узловых точек на квазирегулярных сетках [2-6].

Для исследуемой области, состоящей из материалов с разными физическими свойствами, выбирается минимальный шаг по временной координате (3).

Рассматривается задача о воздействии плоской продольной нестационарной сейсмической волны, параллельной свободной поверхности упругой полуплоскости с полостью, заполненной металлом (соотношение ширины к высоте один к десяти) (рисунок 1).

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).

От точки F параллельно свободной поверхности $ABEFG$ приложено нормальное напряжение σ_x, которое при $0 \le n \le 11$ ($n = t/\Delta t$) изменяется линейно от 0 до P, а при $n \ge 11$ равно P ($P = \sigma_0, \sigma_0$ = 0,1 МПа (1 кгс/см^2)). Граничные условия для контура $GHIA$ при $t > 0$ $u = v = \dot{u} = \dot{v} = 0$. Отраженные волны от контура

GHIA не доходят до исследуемых точек при $0 \le n \le 1000$. Контур *ABEFG* свободен от нагрузок, кроме точки *F*.

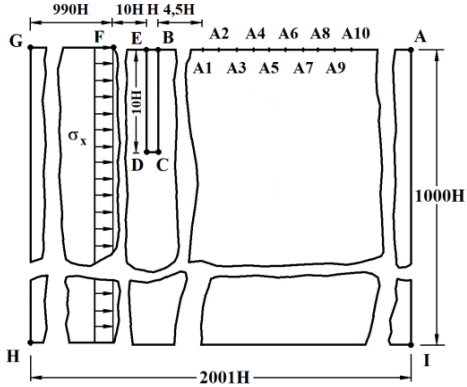


Рисунок 1 – Постановка задачи о воздействии плоской продольной сейсмической волны на упругую полуплоскость с полостью, заполненной металлом (соотношение ширины к высоте один к десяти)

Расчеты проведены при следующих исходных данных. Для области *ABCDEFGHI* : $H = \Delta x = \Delta y$; $\Delta t = 1{,}393 \cdot 10^{-6}$ 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. Для области BEDC : $H = \Delta x = \Delta y$; $\Delta t =$ $9{,}309 \cdot 10^{-7}$ с; $E =$ $2{,}06 \cdot 10^5$ МПа ($2{,}1 \cdot 10^6$ кгс/см^2); $\nu = 0{,}3$; $\rho = 0{,}784 \cdot 10^4$ кг/м^3 ($0{,}8 \cdot 10^{-5}$ кгс·с^2/см^4); $C_p =$ 5371 м/с; $C_s =$ 3177 м/с.

При расчетах принимается минимальный шаг по времени $\Delta t =$ $9{,}309 \cdot 10^{-7}$ с.

На границе материалов с разными свойствами приняты условия непрерывности перемещений.

Решается система уравнений из 8016008 неизвестных.

В качестве примера на рисунке 2 показано изменение упругого контурного напряжения $\overline{\sigma}_k$ ($\overline{\sigma}_k = \sigma_k / |\sigma_0|$) во времени *n* в точке *A*1 (рисунок 1), находящихся на свободной поверхности упругой полуплоскости: 1 – в задаче без полости; 2 – в задаче с полостью

заполненной металлом (соотношение ширины к высоте один к десяти).

Расстояние между точками: $A1$ и $A2$ равно H.

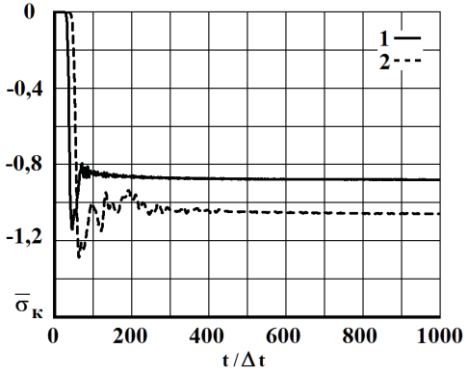


Рисунок 2 – Изменение упругого контурного напряжения $\overline{\sigma}_k$ во времени $t/\Delta t$ в точке $A1$: 1 – в задаче без полости; 2 – в задаче с полостью заполненной металлом (соотношение ширины к высоте один к десяти)

Выводы

1. Прогноз сейсмической безопасности объекта, с помощью численного моделирования, позволяет снизить последствия природной чрезвычайной ситуации.

2. Разработаны методика, алгоритм и комплекс программ для решения линейных двумерных (плоских) задач сложной формы при волновых воздействиях.

3. С помощью численного эксперимента получена устойчивая двумерная явная двухслойная схема.

4. Решена задача о математическом моделировании нестационарных упругих волн напряжений в полуплоскости с полостью заполненной металлом (соотношение ширины к высоте один к десяти) при сейсмическом воздействии. Решается система уравнений из 8016008 неизвестных. Полость (соотношением ширины к высоте один к десяти) заполненной металлом, увеличивает величину упругого контурного напряжения. Это связано с увеличением акустической жесткости полости.

Литература:

1. *Кольский Г.* Волны напряжений в твердых телах. – М.: Иностранная литература, 1955. – 192 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. *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.

5. *Мусаев В.К.* Математическое моделирование нестационарных упругих волн напряжений в консоли с основанием (полуплоскость) при фундаментальном сейсмическом воздействии // Строительная механика инженерных конструкций и сооружений. – 2019. – № 6. – С. 29-33.

6. *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.

Чернов К.В.

Зрение работника и безопасность техногенной деятельности

Аннотация: Приводится описание зрения как сциентного процесса и того, как успешное транскодирование сциенции обусловливает безопасность техногенной деятельности.

Ключевые слова: техногенная деятельность, безопасность, фотон, сциенция хромопротеина, транскодирование, техносциенция

Техногенная деятельность заключается в применении научных знаний к созданию и совершенствованию технетической продукции, в частности технических устройств, приложении научных знаний к выработке практических знаний для производства продукции, использовании практических знаний при ее производстве.

Воздействие вещества и энергии технетического компонента техногенной системы на антропный организм, сопровождающее техногенную деятельность работника или возникающее вследствие этой деятельности, представляет собой техногенное воздействие.

Опасности техногенной деятельности в зависимости от проприетарности воздействия разделяются на собственные техногенные воздействия послекритического уровня, а также химические и энергетические воздействия, возникающие реактивно. Реактивные техногенные опасности возникают при невыполненных необходимых или выполненных ошибочных антропотехнических воздействиях в процессе деятельности.

Деятельность человека как причина реактивных опасностей является опосредованным выражением функций нейросимперифорической и нейрогностической составляющих сциентной системы антропного организма.

Сциенция – слово, обобщающее собой в разных сочетаниях знание, умение, обладание реактивным действием (безусловным рефлексом) и системно характеризующее кодофлексные способности биоты. Сциенция есть аутоактантная совокупность вещественно-энергетических знаков, обладающих потенциалами, носителем которой является выполняющий определенную функцию компонент макромолекулярного, супрамолекулярного (или органоидного), клеточного и надклеточного уровня сопринадлежной организации биотической системы, способный посредством этих знаков к кодовой рефлексии. Кодовая рефлексия, или кодофлексия, – способность биоты имитировать существующее, представленное составляющими реальности, формообразованиями, их внешним окружением и взаимовлиянием, которая проявляется владением реактивным действием, умением действовать, знанием содержания, последствий и оснований действий. Биота эволюционирует вследствие эволюции сциенции, которая начинается с овладения биотой реактивным действием,

продолжается обладанием реактивным действием в сочетании с овладением умения действовать, и достигает стадии обладания реактивным действием в сочетании с обладанием умением действовать и овладением знанием последствий, содержания и оснований действий.

Аутоактантность компонентов нейросимперифорической и нейрогностической составляющих сциентной системы работника вызывается и сопровождается многократным транскодированием сциенции в нейроно-синапсной сети при переходе от одних фаз к другим.

Сциенция начальной фазы предстает вещественно-энергетическими знаками интеро- и экстерорецепции, в том числе знаками зрительной экстероцепции.

Работник до 80% сциентных вещественно-энергетических знаков от компонентов техногенной системы и внешней среды получает посредством зрения. При этом обеспечивается центральная, периферическая и объемная экстероцепция компонентов, а также рецепция их относительного перемещения в пространстве.

Транскодирование зрительной сциенции начинается с поступления квантов электромагнитной энергии видимого диапазона на фоторецепторные клетки сетчатки глаз. Совокупность рецептируемых фотонов создается светом неба, попадающим в производственное помещение через проемы в наружных ограждающих строительных конструкциях, искусственным светом электрических источников и светом, отраженным от поверхностей компонентов системы.

Показателями, характеризующими зрительную сциенцию в начале ее транскодирования, называемую техносциенцией, являются энергия фотонов и интенсивность переносимой ими электромагнитной энергии. Энергия фотонов определяется частотой электромагнитного излучения. Интенсивность, представляющая собой отношение потока энергии к единичной площади воспринимающей поверхности, определяется яркостью источника светового излучения. Знаки техносциенции предстают совокупностью фотонов с определенной частотой и их пространственной локализацией, обусловленной светящимися технетическими компонентами техногенной системы.

Фотон, поступивший через оптический аппарат глаза, воспринимается хромопротеином, встроенным в мембрану наружного сегмента фоторецепторной клетки сетчатки [1]. Хромопротеин состоит из белка, называемого опсином, и простетической хромофорной группы, ковалентно связанной с белком. Опсины колбочковых фоторецепторных клеток поддерживают фотопическое зрение. Опсин палочковых клеток способствует скотопическому зрению. Фотопсины восприимчивы к красной, зеленой и синей частям электромагнитного спектра, а также к фиолетовой и ультрафиолетовой. Хромопротеин палочек представляет собой родопсин, состоящий из палочкового опсина и ковалентно связанного с ним 11-*цис*-ретиналя. Поглощение фотона молекулой 11-*цис*-ретиналя переводит ее в возбужденное состояние. Энергия фотонного возбуждения приводит к изомеризации ретиналя в *транс*-конфигурацию и к активации опсина. Активация опсина ретиналем приводит в действие каскад реакций, преобразующих энергию фотонов в рецепторный потенциал.

Палочковый опсин – белок с полипептидной цепью из 348 аминокислотных остатков, расположенных в семи трансмембранных спиралях. Ретиналь соединен с аминокислотным остатком опсина лизином, находящимся в седьмой спирали. Трансмембранная часть родопсина образована пучком α-спиралей, имеющих изломы и уложенных по циклическому принципу. Внеклеточный домен родопсина образован *N*-концевым участком, а также тремя петлями, и содержит два сайта гликозилирования по остаткам аспарагина. *N*-конец белка и вторая внеклеточная петля содержат пары β-шпилек, некоторые из которых соединены консервативной дисульфидной связью со спиралью ТМ3, прикрывая сайт связывания ретиналя от внешнего влияния. Цитоплазматический домен белка образован петлями и *C*-концевым участком молекулы. В состав *C*-конца входит примембранная амфифильная спираль, зафиксированная в мембране остатками пальмитоиловой кислоты, присоединенными к остаткам цистеина в этой спирали. В *C*-конце также находятся остатки серина, по которым происходит фосфорилирование хромопротина, обусловливающее активацию опсина.

Супрамолекула хромопротеина при физиологических условиях имеет трехмерную конструкцию, которая зависит от связей

взаимодействия между ее частями, в том числе между радикалами аминокислот. Локализация сайтов связывания в ее конструкционном пространстве образуют энергетический ландшафт родопсина.

Связи взаимодействия в хромопротеине следующие: ковалентная связь; водородная связь, образующаяся между двумя полярными незаряженными радикалами или между незаряженным и заряженным радикалами; ионная связь, возникающая между противоположно заряженными радикалами; дисульфидная и гидрофобная связь.

Потенциалами вещественно-энергетических знаков, обусловливающими сциенцией родопсина, являются следующие:

1. Частичные положительные заряды атомов водорода, соединенных ковалентной связью с сильно электроотрицательными атомами (O, N), которые способствуют образованию водородных связей.

2. Местоположение на энергетическом ландшафте частичных положительных зарядов атомов водорода, соединенных ковалентной связью с сильно электроотрицательными атомами (O, N), которое обусловлено конструкцией радикала.

3. Ионные заряды полярных радикалов, которые способствуют образованию электростатических (ионных) связей.

4. Местоположение на энергетическом ландшафте ионных зарядов полярных радикалов, которые способствуют образованию электростатических (ионных) связей.

5. Заряды полярных серосодержащих радикалов, которые способствуют образованию ковалентных связей с другими серосодержащими радикалами.

6. Местоположение на энергетическом ландшафте зарядов полярных серосодержащих радикалов, которые способствуют образованию ковалентных связей с другими серосодержащими радикалами.

7. Частичные заряды сочетания ван-дер-ваальсовых сил и водородных связей, компенсирующиеся гидрофобным взаимодействием.

8. Местоположение на энергетическом ландшафте частичных зарядов сочетания ван-дер-ваальсовых сил и водородных связей, компенсирующихся гидрофобным взаимодействием.

9. Частичные заряды диполей, компенсирующиеся гидрофильным взаимодействием.

10. Местоположение на энергетическом ландшафте частичных зарядов диполей, компенсирующихся гидрофильным взаимодействием.

11. Кванты электромагнитной энергии, поглощаемые электронами хромофора и, возможно, поглощаемые или излучаемые электронами межзвенных орбиталей.

Вся совокупность вещественно-энергетических знаков родопсина предстает энграммной сциенцией, которая участвует в транскодировании куррентной сциенции, порожденной рецептируемыми квантами света и усиленной в фоторецепторных клетках. Сциенция фоторецепторов затем транскодируется многофазно вплоть до преобразования в сциенцию бихевиоральных темплатов, аутоактантность которых вызывает стереотипные действия организма работника, реализуемые в деятельности.

Реактивные опасности не возникают, если работник при сциентном взаимодействии с компонентами техногенной системы, в том числе посредством зрения, выполняет необходимые действия и не выполняет ошибочные.

Сциентное взаимодействие работника и технетического компонента может быть детерминированным и стохастическим. Детерминированное сциентное взаимодействие посредством зрения является целесообразным или сопутствующим. Термин «осмотр» в ФНиП [2] применяется 97 раз.

Главная особенность целесообразного сциентного взаимодействия состоит в том, что работник является инициатором и реципиентом взаимодействия, а технетический компонент – поставщиком вещественно-энергетических знаков, пригодных для последующего транскодирования.

Кванты световой энергии, отражаемой от технетических компонентов, создают зрительную техносциенцию, которая сообщает о конфигурации, размерах и цвете поверхностей, о положении указателей и показаниях приборов. Зрительная техносциенция создается также светящимися мониторами и при обращении к технической документации.

Энергия совокупности фотонов и их интенсивность обусловливают эффективность зрительной работы.

Вывод

Технетические компоненты должны быть приспособлены для сциентного взаимодействия посредством зрения. Частота электромагнитного излучения, определяющая энергию фотонов, и интенсивность переносимой ими энергии должны максимально способствовать успешному транскодированию техносциенции в сциенцию фоторецепторных клеток и сциенцию последующих фаз, вплоть до сциенции бихевиоральных темплатов, формируемых при обучении и вызывающих безопасные действия.

Литература:

1. *Островский М.А.* Фотобиологический парадокс зрения / Проблемы регуляции в биологических системах. Биофизические аспекты. – М.-Ижевск: НИЦ «Регулярная и хаотическая динамика», Институт компьютерных исследований, 2007. – С. 133-164.

2. Федеральные нормы и правила «Правила промышленной безопасности при использовании оборудования, работающего под избыточным давлением», утв. пр. Ростехнадзора от 15.12.20 №536. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId= 384352 (дата обращения 23.09.2021).

Чинакал В.О.

Повышение безопасности управления сложными объектами в условиях скрытых изменений параметров технологических процессов

Аннотация: Рассматриваются вопросы повышения безопасности управления сложными промышленными объектами в классе непрерывных производств на базе реализации методики раннего обнаружения скрытых изменений параметров технологических процессов. Обсуждаются возможности применения интеллектуальных методов анализа данных и методов моделирования для реализации методики в виде интеллектуальной подсистемы поддержки управления в перспективных системах усовершенствованного мониторинга и управления AMS&APC (AMS – Advanced Monitoring System, APC – Advanced Process Control).

Ключевые слова: безопасность управления, раннее обнаружение, скрытые изменения параметров, технологические процессы, непрерывное производство, AMS, APC

Введение

Одной из проблем повышения безопасности управления (БУ) сложными распределенными объектами в классе крупномасштабных непрерывных и непрерывно-дискретных технологических производств (ТП), таких как (нефтехимия, нефтепереработка, строительные материалы и др.) является проблема раннего обнаружения изменений части ключевых технологических параметров (КТП) продуктов и рабочих параметров агрегатов и установок из-за воздействия скрытых изменений (СИ) в характеристиках перерабатываемых потоков и параметров установок. При этом часть проблем БУ возникает из-за ряда неконтролируемых или редко контролируемых изменений параметров перерабатываемого сырья или промежуточных продуктов (это «скрытые» изменения СИ-1), а часть проблем из-за влияния скрытых изменений характеристик используемого оборудования технологических агрегатов и установок (СИ-2). Причина или комбинация нескольких возможных причин возникновения СИ-1 и/или СИ-2 могут быть различными, в частности, из-за наличия сложных перекрестных динамических связей в ТП, износа оборудования или его неправильной эксплуатации и др.

В ряде случаев такие неконтролируемые изменения с течением времени постепенно накапливаются и вызывают вполне значительные изменения уже в различных «измеримых» параметрах промежуточных или выходных продуктов, в режимных параметрах установки, либо в работе основного и вспомогательного технологического оборудования. В результате могут возникнуть серьезные нештатные и аварийные ситуации, приводящие к нарушениям технической и экологической безопасности и значительному ущербу для промышленного предприятия.

Решению различных проблем, связанных с обеспечением и повышением безопасности управления технологическими производствами, посвящено большое число научных работ и исследований, полный обзор которых практически невозможен.

Кратко, для данного типа производств основные проблемы БУ и некоторые современные подходы и методы их решения рассмотрены, например, в [1-4].

В [1] рассмотрены вопросы совершенствования контроля показателей качества продукции, а также применения усовершенствованных систем управления АРС в ТП, в [2,3] анализировались основные проблемы и подходы к повышению БУ ТП, включая применение систем усовершенствованного мониторинга AMS в ТП с использованием текущих измерений. В [4] рассмотрены вопросы наиболее частого применения AMS для off-line анализа измеряемых параметров КТП с использованием архивных данных и данных on-line-диагностики работы машинного оборудования (СП-2), в частности, применения методов оперативной вибродиагностики и других методов.

В данной работе рассматриваются возможности повышения БУ ТП с использованием методики повышения эффективности раннего обнаружения скрытых изменений параметров ТП (СИ-1) сложных промышленных объектов в перспективных интегрированных системах усовершенствованного мониторинга и управления AMS&APC [5]. Для реализации методики использованы интеллектуальные методы анализа данных и методы моделирования [6, 7], реализуемые в составе подсистемы интеллектуальной поддержки процессов управления (ИСПУ).

Учитывая большие единичные мощности промышленных установок, агрегатов и емкостей, а также пожаро-взрывоопасность ряда производств, разработка методики раннего обнаружения СИ в ИСПУ для таких классов производства является чрезвычайно актуальной задачей.

Методика раннего обнаружения СИ

Методика раннего обнаружения СИ предназначена для применения в интегрированных системах усовершенствованного мониторинга и управления ИСПУ [5] и используется в цикле работы AMS&APC.

Основные этапы цикла работы ИСПУ [5]:

– на основе циклического оперативного анализа данных на текущем и предыдущих рабочих интервалах определяется наличие возможных симптомов раннего обнаружения СИ параметров во всех КТП основных ТП;

– формируется множество оценок индикаторов симптомов с привязкой к наиболее вероятным интервалам времени;

– проводится интеллектуальных анализ выявленных оценок;

– формируется список возможных гипотез ситуаций;

– проводится проверка возможных гипотез;

– выделяются наиболее вероятные гипотезы;

– по каждой проверяемой вероятной гипотезе формируется расширенный вектор начальных значений индикаторов симптомов для полномасштабной системы имитационного моделирования (СИМ);

– выполняются сеансы моделирования СИМ, начиная с интервала времени наиболее раннего индикатора и заканчивая заданным интервалом прогноза;

– анализируются результаты работы СИМ по всем интервалам;

– выделяются критические СИ и формируются их типы и рейтинги;

– в зависимости от типов и рейтингов формируются сообщения соответствующим службам предприятия.

В реализуемой в ИСПУ методике раннего обнаружения СИ редко измеряемых параметров технологических потоков (СИ-1) и параметров самих технологических агрегатов (СИ-2) используются:

– доступные оперативные данных от штатных систем контроля и управления объектом (от поточных датчиков и анализаторов, данные измерений параметров технологических потоков, резервуаров и установок с использованием лабораторных анализов) [1];

– расчетные данные от LIMS-систем и виртуальных анализаторов (ВА), (АС или АСУТП) [1,2];

– дополнительная информация, получаемая в результате применения интеллектуальных методов обработки текущих данных реального времени, актуальных технологических данных и различных архивных данных [2,3,6];

– адаптивные модели виртуальных анализаторов, применяемые для оперативной оценки редко измеряемых параметров ТП с учетом их связи с другими, более часто измеряемыми параметрами ТП, а также оперативные корректировки

параметров соответствующих косвенных моделей ВА [1,6] с использованием различных измерений;

– интеллектуальные методы (ИМ) для формирования гипотез и их оценки при различных ситуациях возможного возникновения СИ ТП в прошлом и настоящем времени [5,6];

– методы и алгоритмы моделирования влияния возможных вариантов изменения параметров ТП, имитирующих возникновение СИ-1 и СИ-2, с последующими оценками развития ситуаций в будущем при разных гипотезах о вероятных причинах возникновении возможных СИ в ТП в различные интервалы времени контроля и управления ТП [3,5];

– методы и алгоритмы формирование индикаторов (симптомов) раннего обнаружения СИ-1 и СИ-2 по результатам обработки измерений [3,5];

– методика формирования распределенных баз знаний (БЗ) в виде продукционных правил и использование встраиваемых интеллектуальных компонентов (ВИК) для реализации логического вывода [7].

Для автоматического раннего обнаружения соответствующих признаков возникновения нештатных и аварийных ситуаций (симптомов) были использованы совместно методы моделирования на базе полномасштабной системы имитационного моделирования (СИМ) и интеллектуальные методы обработки текущих данных. Для проверки основных этапов методики и работы ИСПУ были построены варианты альтернативных моделей изменения качества сырья, выходных продуктов и анализа режимных параметров ТП на базе стандартного пакета статистической обработки реальных архивных данных крупной промышленной установки первичной переработки нефти. Это позволило сформировать для СИМ параметры «скрытых изменений» основных КТП, а затем выделить характерные симптомы на траекториях изменения КТП. Далее значения выделенных симптомов были использованы для формирования оценок индикаторов симптомов и настройки параметров правил в моделях представления знаний для последующего использования.

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.* Об одном подходе к мониторингу непрерывных технологических процессов. // Труды 17-ой международной конференции CAD/CAM/PDM – 2017 «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта» – М.: ИПУ РАН, 2017. – С. 438-440.

4. 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 01.08.2021).

5. *Чинакал В.О.* Применение интеллектуальных методов и моделирования в задачах анализа и прогноза состояния промышленных объектов // Труды 15-й Международной конференции CAD/CAM/PDM – 2015. – М.: ООО «Аналитик», 2015. – С. 74-76.

6. *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.

7. *Чинакал В.О.* Разработка и применение встраиваемых интеллектуальных компонентов, построенных с использованием матричных методов. // Труды 8-ой международной научно-практической конференции «Инженерные системы – 2015». – М.: РУДН, 2015. – Т. 1. – С. 145-150.

Кафидов В.В.

Миграционная политика и безопасность города

Аннотация: В работе рассматриваются модели развития города и модели миграционных процессов в городе, влияющие на его безопасность.

Ключевые слова: безопасность, город, жители, население, миграция, ассимиляция, диаспора

Ярким примером стратегически непродуманной миграционной политики является Москва. Каждые 25 лет Москва расширяет свою территорию. Но то, что происходит в последние годы – беспрецедентно.

В последние годы развернулось бурное строительство на новых территориях. Новые дома заселяются не москвичами, улучшающими свои жилищные условия, а новым населением, которое едет в Москву, т.к. не может реализоваться у себя на малой Родине. По данным исследования ЦИАН, «больше потенциальных мигрантов – из Подмосковья, Петербурга и Кубани. Самые дорогие квартиры в Москве ищут сахалинцы. Самое просторное жилье выбирают покупатели из Ингушетии» [1].

Кроме внутренней миграции, полным ходом осуществляется внешняя миграция. Причем миграция «диаспорная» [2], не предусматривающая ассимиляции мигрантов. В таком случае в полной мере проявляется модель развития города «город для людей» или, что то же самое, «жители для города» [2].

Рассматривая вопросы управления городом и различные подходы к пониманию системы управления городом, можно установить, что город, вид поселения, – это территория, организованная для проживания людей.

Город с количественной точки зрения может рассматриваться как скопление относительно большого количества людей, имеющих временное или постоянное жилище на определенной территории. Получается, что оседлость – фактор не обязательный, когда главенствует модель «жители для города». Количество людей, находящихся на территории города, связано с условиями и возможностями его развития.

С административно-политической позиции город представляет закрепленную за ним часть государственной территории с предоставлением полномочий по организации жизнедеятельности жителей и населения на данной территории.

С социальной точки зрения город, как поселение, представляет собой среду социализации проживающих и находящихся на территории города людей.

С экономической позиции город создает условия для производства товаров и услуг, обеспечивает эффективность производства и реализации товаров и услуг для обеспечения заданного уровня благосостояния и жизнеобеспечения жителей и населения, кооперации и конкуренции с другими поселениями.

Для города – экономические выгоды, своеобразная пирамида. С социальной точки зрения новое население не является жителями. Это, с одной стороны, люди, для которых этот город еще чужой и они не хотят соблюдать правила, не уважают жителей, которые зачастую менее успешные и богатые. С другой стороны, они хотят видеть себя хозяевами и входят в государственные органы и органы местного самоуправления, обучаются и преподают в учебных заведениях. Они не знают традиционной культуры, это революционеры.

В мегаполисе другие системы отношений. Москва – город с низким уровнем безработицы – всего 2,53% (за 2020 год), что меньше, чем в большинстве других мегаполисов мира [3]. Более того, есть еще люди третьего сорта – это мигранты. Считается, что именно они закроют невыгодные вакансии. В результате вместо внедрения техники и технологий, требующих квалифицированных кадров, используется неквалифицированный ручной труд.

Руководство города убеждено в том, что нам нужна рабочая сила мигрантов. При этом никто не задумывается, где и как живут эти люди. Они готовы работать за мизерные зарплаты. А если задуматься, то это элемент безопасности страны. Если по какой-то причине мигранты уедут домой или будут бастовать или примкнут к экстремистским силам, то возникнет чрезвычайная ситуация.

Безопасность поселения и обеспечение контроля над органами управления в значительной степени зависит от сложившейся культуры. Жители задают вектор развития города, которому должны следовать органы городского управления. Правда, нужно

иметь представление о том, что такое культура города и какими параметрами она определяется. Давно существовала гипотеза, требующая подтверждения, что изменение структуры населения более чем на 10 процентов приводит к необратимым процессам в культуре поселения города, страны. Вместе с тем, рост города или изменение структуры экономики приводят или к поглощению новых территорий с местным населением, не разделяющим культурные ценности города, или притоку мигрантов. Наличие значительного количества мигрантов может привести к тому, что в ближайшее время их следующие поколения будут претендовать на права горожан, не освоив культуру не только жителей, но и населения города. Это не может не отразиться на безопасности города.

А это возможно, т.к. в нашей стране сложилась диаспорная организация мигрантов.

Простая, «индивидуальная» ассимиляция успешно происходила в нашей стране. К примеру, москвичи это далеко не только русские – это татары, армяне, грузины, белорусы и др., но они проходили простую «индивидуальную» ассимиляцию, попали в котел столичной культуры и сварились в нем до состояния жителя Москвы. Теперь этот котел не работает, т.к. жителем может стать любой гражданин страны, имеющий собственное (или даже съемное) жилье и постоянную работу. Они никому ничем не обязаны. А кроме жителей в состав населения входят внутренние и внешние мигранты, которые еще более никому ничем не обязаны. «Сейчас мигранты живут замкнутыми диаспорами, женятся и выходят замуж за своих. Как показывает статистика, межнациональные браки встречаются все реже, и все больше и больше речь идет о закрытых сообществах внутри страны. Со временем это будут государства в государстве» [4].

Армянские, грузинские и другие диаспоры всегда существовали, но они не играли такую роль, какую играют современные диаспоры. Диаспоры, появившиеся, главным образом, в постсоветское время не способствуют усвоению местной городской культуры, уважению к коренным жителям. Городской культуры, потому, что наиболее привлекательными для мигрантов являются города в 7-8 регионах, представляющих 30% населения страны. Это связано с тем, что проявление городского образа жизни

в полной мере проявляется по разным оценкам в городах с числом жителей более 100 тыс. или даже 250 тыс. Но 75% городов, в которых проживает ровно треть городского населения, находятся за чертой такого городского стандарта [5].

В то же время от жителей города очень многое зависит. Только жители на генетическом уровне понимают значение и функции города.

«Диаспорная» миграция агрессивна, защищает культуру и интересы своей диаспоры. Москва с акцентом (магазины, кафе, спортивные клубы «для своих», закрытые вечеринки), газеты «Вестник Мигранта», «Мигранты сегодня» – это все последствия реализации «диаспорной» миграции и модели развития города «город для людей». Особенности этой модели уже описывались в предыдущих публикациях [2,5]. Разница в моделях «город для жителей» и «город для людей» в крупных и крупнейших городах заключается в том, что городские власти, далекие от жителей, формируют объект управления исходя из целесообразности экономического развития города и его успешной конкуренции во внешней среде.

Модель «город для жителей» ориентирована, прежде всего, на удовлетворение потребностей жителей данного города, которые определяют, нужно ли привлечение внешних трудовых ресурсов и какого качества, какие предприятия и организации полезны городу, а какие нет и т.п. Популярная модель «город для людей» на практике легко трансформируется в формулу «люди для города». В городе должно быть комфортно всем, т.е. приоритетно развитие города, как хозяйственной единицы.

«Диаспорные» мигранты первого поколения стараются быть незаметными, послушными и исполнительными, готовыми идти на любые лишения. Это инстинкт самосохранения, вызванный страхом потерять работу, место проживания, он опирается на земляческие механизмы, которые мы наблюдали в армейской дедовщине. Мигранты заинтересованы в расширении диаспоры. Но второе поколение претендует на полноправие в обществе, которое перерастает в доминирование. У коренного населения нет «диаспорной» культуры, оно построено на основе простой ассимиляции.

Последствия современной миграционной политики проявляются в снижении производительности труда, снижении качества продукции и выполнения работ, снижении заработной платы за работу, которую могли бы выполнять жители города, наполнение ученических классов агрессивно настроенными детьми мигрантов. Отдельные отрасли становятся полностью подчиненными мигрантам. Это торговля, городской транспорт, ЖКХ, строительство и ремонт и др. Внутренняя миграция создает отток кадров из городов и сел России.

В этой ситуации решения о судьбе крупного города могут принимать в определенных условиях люди, с этим городом не связанные исторически и культурно.

Важной темой для исследования является разработка методов стратегического выбора: развивать город за счет нового населения или создавать условия для развития городских трудовых ресурсов, выстраивать политику и разрабатывать механизмы влияния на предпринимателей по вопросам создания и заполнения рабочих мест.

Для оценки происходящих процессов требуется разработать модели и методы оценки скорости ассимиляции и критических параметров потока миграции. Исследованию подлежит и нелинейная зависимость между общей численностью населения и долей нового населения. Видимо это зависит еще и от типа города, его внешней и внутренней миссии, его размеров.

В законодательстве не защищаются права жителей. Некоторые исследователи отмечают, что к моменту распада СССР городские жители в большинстве своем были горожанами в первом-втором поколении, это наиболее агрессивные поколения и последствия этого отразились в распаде страны. В настоящее время данное положение усугубляется внешней миграцией неквалифицированных и малообразованных выходцев из стран бывшего СССР. Их дети становятся жителями без этой генетической памяти.

Процесс постепенного вытеснения из города менее технологичных секторов экономики более технологичными секторами сопровождается освобождением территории, улучшением экологии и потребностью в более квалифицированной рабочей силе. Если это не делать на плановой основе, то сложится ситуация, при которой новые высокотехнологичные рабочие места придется заполнять за счет притока мигрантов или создавать такие

рабочие места, на которых выгоднее использовать дешевую рабочую силу опять же мигрантов. Уже сейчас в системе ЖКХ, строительстве, торговле, на транспорте работают преимущественно приезжие. А с расширением позиций «цифровой экономики» еще больше рабочих мест, требующих квалификации, будет сокращаться.

Любое поселение – это среда социализации. И здесь наблюдаются два возможных процесса: социальная среда формирует органы городского управления, а второй путь – органы городского управления формируют социальную среду, способствующую сохранению таких органов городского управления. Экономика города превалирует над развитием социальной организации. В результате происходит изменение социальной организации.

В такой ситуации проще манипулировать, а не осуществлять государственное и муниципальное управление. У города появляются бесполезные, преимущественно коренные, жители в «возрасте доживания».

Коренное изменение складывающейся ситуации связано с отказом от диаспорной миграционной политики, сокращением рабочих мест, не требующих определенной высокой квалификации и увеличением размера оплаты труда.

Литература:

1. Кто переезжал в Москву до коронакризиса и после? – URL: https://www.cian.ru/stati-kto-pereezzhal-v-moskvu-do-koronakrizisa-i-posle-318111/ (дата обращения 03.10.2021).

2. *Кафидов В.В.* Современные методологические подходы к стратегическому управлению и развитию городов различных типов. – М.: Издательский дом «Дело» РАНХиГС, 2015. – 246 с.

3. Москва в цифрах. – URL: https://investmoscow.ru/ (дата обращения 03.10.2021).

4. *Михеев Сергей*. Власти диаспор в России быть не должно. Демография демографии рознь. – URL: https://zen.yandex.ru/2rub/ (дата обращения 03.10.2021).

5. *Кафидов В.В.* Экономика и социология безопасности. – М.: Креативная экономика, 2019. – 254 с.

VI. Методы моделирования и принятия решений при управлении безопасностью сложных систем

Дашков Р.Ю., Комков Н.И., Сивокоз В.Н., Тисленко А.В.

Проблемы управления обоснованием и реализацией крупномасштабных проектов

Аннотация: Рассматриваются проблемы формирования и управления крупномасштабными проектами. Отмечается поступательное увеличение числа таких проектов на протяжении второй половины прошлого века и в начале текущего столетия. Рост масштабности и увеличение сложности проектов потребовали разработки инструментария управления современными проектами, где значительное внимание уделяется информационной системе, средствам мониторинга и контроля за ходом реализации проектов. Рассматриваются особенности управления крупным проектом производства сжиженного природного газа (СПГ) компанией «Сахалин Энерджи».

Ключевые слова: проект, технологии, социально-технологическое развитие, программа, сжиженный природный газ

Роль и значение крупномасштабных проектов в социально-экономическом развитии промышленных и развивающихся стран на протяжении второй половины XX века – в начале XXI века были высокими, что повлияло на рост объемов мировой экономики (в среднем более чем на 3% ежегодно). Значительные производственные мощности в добывающих, перерабатывающих и машиностроительных отраслях, включая оборонную промышленность, были созданы в США, странах ЕС, а также в бывшем СССР и странах юго-восточной Азии, Японии, Китае, Индии, Индонезии и др. Создание этих мощностей в свою очередь базировалось на разработке и использовании сотен тысяч новых

технологий и огромного количества взаимосвязанных промышленных объектов, объединенных в производственно-транспортные сети цепочек поставок, распределенных на значительной территории и охватывающие десятки стран. Обоснование целесообразности и перспективной возможности создания такого значительного объема производственных мощностей базируется на социально-экономических и научно-технологических прогнозах, включая оценку возможности привлечения инвестиций и рыночную целесообразность дополнительно производимых продуктов [1].

Основным инструментом воплощения перспективных целей, инновационных решений, технологий, ресурсов и инвестиций в практически целесообразные мощности по созданию новых продуктов являются проекты. Проектное управление, как прикладная область знаний, развивается с середины XX века и благодаря усилиям многих зарубежных: Р. Арчибальд, Э. Голдратт, Т. ДеМарко, Р. Инглунд, Э. Йескомб, Г. Керцнер, Л. Лоуренс, Д. Милошевич, Р. Ньютон, К. Хелдман, Б. Фливбьорг и российских ученых: С. Никанорова, П. Кузнецова, А. Лернера, А. Маликонова, В. Буракова, превратилось в эффективное средство управления большим количеством работ (сотни тысяч), значительными объемами инвестиций (миллиарды долларов), огромным числом исполнителей (десятки тысяч) и созданием большого количества объектов.

Одновременно с изменением базовых характеристик проектов, включая рост числа работ (операций), увеличение структурной и параметрической неопределенности работ и проектов в целом, нарастанием рисков срыва сроков и превышения бюджетов проектов и др., постепенно совершенствовались методы и инструменты управления проектами. Если в 60-х-70-х годах прошлого века основные усилия по совершенствованию инструментов управления проектами предпринимались в направлении создания моделей баз данных математиками и специалистами по исследованию операций, то уже в начале XXI века возможности решения сложных практических задач стали доступны благодаря успехам в программировании и использовании персональных ЭВМ, средств передачи, хранения и обработки больших объемов информации.

Существенная практика отбора крупномасштабных проектов, которые назывались в СССР народнохозяйственными программами, не отличались креативностью, а предложения по их составу, как правило, формировались на партийных собраниях КПСС и принимались на съездах народных депутатов. Несмотря на очевидность проблемных ситуаций в социально-экономическом развитии страны, принятие народнохозяйственных программ осуществлялось с большим опозданием. Так, обозначившиеся еще в конце 70-х годов трудности со снабжением населения продовольствием только в конце 80-х годов сформировали «Продовольственную программу СССР». Жилищные проблемы (нехватка жилья, избыточное ветхое жилье и др.) также только в 80-х годах было решено отразить в народнохозяйственной Программе «Жилье». Выпуск малоэффективных и ресурсноизбыточных машин предполагалось технологически и организационно изменить в Программе развития машиностроительного комплекса. Этим крупномасштабных проектам, к сожалению, не удалось достичь намеченных в них целей и целевых нормативов [1]. К числу главных причин неудач в достижении обозначенных в народнохозяйственных программах целей относится отставание в развитии технологической базы в СССР, завышенные целевые нормативы и чрезмерно высокие объемы ресурсов (металла, электроэнергии, топлива и др.). Народнохозяйственные программы, наряду с крупномасштабными проектами в СССР, формировались на основе учета политических и социальных факторов, а экономические и инновационно-технологические составляющие развития обычно рассматривались как второстепенные.

В условиях рыночной экономики России, помимо масштабности и значимости целей проектов на верхнем уровне руководства экономикой страны, прежде всего, следует учитывать социально-экономическую значимость проектов, рыночную целесообразность продуктов, производимых создаваемыми в рамках крупномасштабных проектов производственными мощностями, а при подготовке таких проектов необходимо учитывать возможность привлечения инвестиций, доступность для генерального подрядчика технологий, способных обеспечить конкурентоспособность производимых товаров, необходимое качество и квалификацию привлекаемого персонала.

Перечисленные выше особенности формируемых в настоящее время крупномасштабных проектов требуют от управляющей проектом компании сочетания высокого технологического уровня знаний, необходимых персоналу и менеджменту, эффективной интеграции стратегической и операционной деятельности и умения управлять сложными процессами с учетом неопределенностей внешней и внутренней среды проектов и рисков.

В соответствии с концепцией целевого управления проектам (ЦУП) методология ЦУП предполагает в качестве инструмента пошагового планирования, контроля и оценки достижения сроков и частных результатов отдельных видов работ, представляет собой пакеты задач и итогов, необходимых для согласования оценок более высокого уровня управления [1].

В соответствии с порядком формирования ЦУП, центром является проект, вокруг которого определяются и выстраиваются взаимоотношения остальных участников. ЦУП определяет и обеспечивает непрерывную цепочку реализации проектов, более низкого уровня, включающую действия участников в соответствии с распоряжением центра.

Исполнители проекта шаг за шагом добиваются ожидаемого значения индикаторов целей проекта в обозначенных графиком намеченными промежуточными результатами и установленным бюджетом. Неизбежные отклонения при использовании нововведений, должны своевременно диагностироваться и корректироваться в процессе выполнения проекта.

В общем виде методология ЦУП включает следующие элементы:

– концепция Проекта;
– базовую цель Проекта;
– количественный индикатор достижения цели;
– технико-экономическое обоснование проектов;
– пакеты задач с подцелями, стратегиями и индикаторами достижения подцелей;
– описание работ из пакета задач, ожидаемые результаты, исполнители и сроки;
– календарный график выполнения работ;
– бюджет проекта с привязкой расходов к отдельным работам и срокам их выполнения;

– бизнес-план;

– договоры (соглашения) между заинтересованными сторонами проекта;

– публичная отчетность о результатах выполнения проекта.

В качестве примера успешной реализации методологии ЦУП может считаться проект «Сахалин-2», реализуемый компанией «Сахалин-Энерджи» [2].

При формировании крупномасштабных проектов убежденности властных структур в их целесообразности и эффективности на макроуровне, не всегда достаточно для их успешной реализации. Права владения материальными и нематериальными ресурсами в условиях рыночной двухсекторной экономики в определенной доле принадлежат собственникам и государству. Поэтому при обосновании целей и состава крупномасштабных проектов необходимо в максимальной степени учитывать всесторонние интересы, как участников (заказчиков) проектов, так и перспективы пространственного развития конкретной социально-экономической системы (СЭС). Для этого следует учитывать перспективы развития такого пространства с учетом целевого характера проектов и возможности увеличения синергии при объединении разных компонент проектов. При этом наиболее предпочтительной может считаться следующая последовательность определения содержания основных компонент целевого проекта: прогнозы --- тенденция развития --- узкие места--- точки роста --- способы их устранения --- технологии --- цели проектов развития --- соответствие целям национального развития --- обеспеченность проектов ресурсами --- договор на выполнение проекта.

Порядок формирования целей и содержания проектов может быть представлен в виде последовательности матриц, где, начиная с первой матрицы, построенной с учетом тенденций и узких мест, формируются точки роста, которые затем служат основой формирования второй матрицы и т.д. вплоть до ресурсного обеспечения потенциально эффективных проектов.

На наш взгляд, именно на основе методологии ЦУП можно придти к принятию Окончательного инвестиционного решения о строительстве 3-й производственной линии завода СПГ, когда в качестве поставщиков сырьевого газа могут быть привлечены

другие компании и должны учитываться перспективы пространственного развития Сахалина как целостной СЭС.

При реализации проекта «Сахалин-2» [2-5] у традиционных методов мониторинга и контроля выявлялись существенные недостатки:

– во-первых, не учитывается важность и ценность отдельных работ, влияющих на жизнеспособность всего проекта, то есть не учитывается изменяющийся во времени характер ценности работ;

– во-вторых, не проводится различие между работами, которые отличаются по трудоемкости и производительности, одинаковое предпочтение уделяется обоим. Можно иметь хороший прогресс по вспомогательным работам, не лежащим на критическом пути, тогда как наиболее важные работы будут иметь неудовлетворительный статус;

– в-третьих, не учитываются предпочтения заинтересованных сторон, ценность новой информации о результатах проведенных работ и корректирующие мероприятия, что затрудняет коммуникации и координацию подрядных организаций и структурных подразделений компании;

– в-четвертых, крайне сложно проводить интеграцию структуры разбиения работ со структурой разбиения рисков, сопровождающих проект в виде неопределенности, вариативности и непредсказуемости.

Все эти недостатки обусловили необходимость совершенствования методологии мониторинга и контроля проектов, основные результаты которой изложены в работах [1-5].

Несмотря на многочисленные исследования по проблемам проектного управления, специалисты-практики по управлению проектами постоянно сталкиваются с трудностями в применении традиционных методов мониторинга и контроля для объективного прогнозирования будущей эффективности проектов. При управлении проектом «Сахалин-2» ключевым недостатком управления освоенным объемом, освоенным графиком и освоенной длительностью, выявилась неспособность предсказывать объем затрат и изменения в расписании процесса создаваемых объектов проекта, а также неготовность определять корректирующие действия на стадии реализации по видам деятельности – рабочему

проектированию, комплектации и строительству создаваемых объектов.

Важным отличием проекта «Сахалин-2» является совмещение в одном общем проекте стратегической и операционной деятельности компании. Это, с одной стороны, требует четкой согласованности проектной и операционной деятельности, а с другой стороны, позволяет максимально быстро осваивать уже завершенную часть проекта.

Существенное отличие, предлагаемых авторами методов управления освоенным объемом и освоенной длительностью по фазам проекта от традиционных методов мониторинга и контроля с постоянным шагом оценки состояния, заключается в отказе от регулярного предоставления отчетности по исполнению, привязанного к концу календарного периода (месяца, квартала), и замене ее отчетностью, дата которой привязана к моменту исполнения крупного пакета работ с измеримым результатом, имеющим отношение только к конкретной фазе, либо к создаваемому производственному объекту, или к различным видам деятельности, без которых невозможен прогресс проекта. В этом случае повышается достоверность контроля и снижаются затраты на мониторинг проекта.

Многопараметричность характеристик проекта и многосвязанность процессов освоения запасов углеводородов достигается на основе мониторинга с переменным шагом контроля, что позволяет снижать неопределенность по мере приближения к завершению проекта.

В управлении освоенным объемом и освоенной длительностью по фазам проекта структурированные фазы являются ключевым элементом агрегированного контроля содержания, сроков и стоимости. Фазы являются логическими компонентами всего проекта. Они естественным образом разделяют отдельные работы по проекту на агрегированные блоки деятельности, которые группируются по значимым основным и вспомогательным объектам проекта. В конце фазы менеджер проекта может осуществлять мониторинг основных, либо вспомогательных объектов проекта с точки зрения понесенных затрат и затраченного времени, независимо от того выполняются фазы параллельно, либо последовательно. В традиционных методах мониторинга и контроля

оценка исполнения всех пакетов работ осуществляется в конце каждого периода, но не проводится различие между работами, завершенными в данной фазе, и работами, завершаемыми в других фазах.

Используемый при реализации проекта «Сахалин-2» способ разбиения на фазы, которые привязываются к проектируемым и реализуемым объектам, позволяет эффективно координировать рабочее проектирование, комплектацию и строительство, которые выполняются различными субподрядными организациями. Сопоставление структуры разбиения фаз с организационной структурой компании позволяет отслеживать иерархический статус проекта и в соответствии с ним принимать управленческие решения по минимизации перерасхода средств и задержек, включая инспекцию создаваемых объектов на строительной площадке.

Эффективный контроль по фазам проекта в компании Сахалин Энерджи начинается на ранних стадиях планирования проекта, сопровождаясь формированием реестра рисков и его обновлением в ходе рабочего проектирования, комплектации и строительства объектов. Эти меры позволяют проектному офису компании в целом иметь эффективную систему отчетности по проекту по видам деятельности в разрезе технических и нетехнических фаз, связанных с неопределенностью и рисками. С помощью таких методов мониторинга и контроля проектный офис и руководство компании приобретают возможность отслеживать прогресс крупномасштабных проектов в условиях неопределенности внешней и внутренней среды, используя гибкие и адаптивные инструменты управления.

Заключение

1. Управление крупномасштабными проектами совершенствуется в направлении увеличения числа учитываемых параметров за счет совершенствования средств мониторинга и контроля.

2. Прогнозные оценки реализуемости таких проектов с точки зрения сроков и затрат являются важными, но не решающими, принимая во внимание рыночную стоимость извлекаемых запасов углеводородов и финансовую устойчивость компании. Во многом успех крупномасштабного проекта зависит от возможностей и

выгод комплексного управления портфелем проектов различных заинтересованных сторон в рамках пространственного развития единой СЭС.

3. Из-за сложности и неопределенности крупномасштабных нефтегазовых проектов системы мониторинга и контроля должны включать иерархические структуры разбиения проектов на фазы, интегрируемые со структурами разбиения рисков, а в корпоративном управлении необходима координация проектной и операционной деятельности в структурных подразделениях компании.

Литература:

1. *Комков Н.И.* Проблемы управления развитием крупномасштабных социально-экономических систем. – М.: Издательский дом «Наука», 2020. – 152 с.

2. *Дашков Р.Ю.* Приоритезация и ранжирование фаз в управлении проектом строительства производственной линии завода сжиженного природного газа // МИР (Модернизация. Инновация. Развитие). – Т. 8. № 1. – С. 88-95.

3. *Дашков Р.Ю.* Система стратегического мониторинга и контроля нефтегазовых проектов: Цели-Фазы-Метрика+Стратегии // Проблемы экономики и управления нефтегазовым комплексом. – 2017. – №9. – С. 12-19.

4. *Дашков Р.Ю., Тисленко А.В.* Система мониторинга и контроля деятельности заинтересованных сторон проекта на основе метода Управления освоенной длительностью // МИР (Модернизация. Инновации. Развитие). – 2018. – Т. 9. № 1. – С. 86-97.

5. *Дашков Р.Ю., Тисленко А.В.* Система стратегического контроля и мониторинга проекта строительства производственной линии завода СПГ: интеграция модели Цели-Фазы-Метрика+Стратегии с управлением рисками // Проблемы экономики и управления нефтегазовым комплексом. – 2017. – №11. – С. 17-23.

Прус М.Ю.

Стохастическое моделирование каскадных сценариев развития аварий и катастроф

Аннотация: Построена общая стохастическая модель, описывающая динамику возникновения и развития аварий и катастроф техногенного и природного происхождения по каскадному сценарию с ветвящейся структурой. Приведены нестационарные решения уравнений Колмогорова-Чепмена, с заданием интенсивностей переходов трехпараметрическим распределением Вейбулла.

Ключевые слова: моделирование техногенных аварий, каскадное развитие аварии, распределение Вейбулла

Возникновение и развитие аварий и катастроф как техногенного, так и природного происхождения, наиболее часто происходит по определенным типам каскадных сценариев, в которых аварии и/или отказы одних элементов порождают отказы и/или аварии других элементов в рамках одной системы, либо нескольких взаимодействующих систем [1-4]. Возможные неблагоприятные сценарии развития ситуации по так называемому «принципу домино» обусловлены реализацией поэтапных переходов к критическим состояниям с нарастанием степени потенциальной опасности, либо сопровождаются усилением неблагоприятных факторов и явлений.

В ходе развития реальных аварийных либо опасных природных процессов, как правило, возникают и исчезают так называемые «окна возможностей» – временные интервалы, в течение которых может быть оказано существенное влияние на динамику событий и общий исход в результате комплекса своевременных целенаправленных воздействий. Основные цели исследования динамики различных аварий и катастроф состоят в выявлении закономерностей, способствующих определению характера и момента наиболее эффективного воздействия на объекты и процессы со стороны имеющихся систем обеспечения безопасности.

При своевременном реагировании оперативных и аварийно-спасательных подразделений служб экстренного реагирования

появляется возможность торможения процессов развития событий по неблагоприятному сценарию и дальнейшего снижения степени опасности вплоть до ликвидации угроз и негативных последствий инцидента. Поэтому перспективным направлением развития систем информационно-аналитического обеспечения и поддержки управления оперативным реагированием на инциденты представляется построение превентивных и рискориентированных алгоритмов реагирования, генерируемых на основе математического моделирования динамики наиболее вероятных сценариев при производственных авариях, катастрофах и стихийных бедствиях.

Математические модели и алгоритмы, предназначенные для информационно-аналитического обеспечения и решения задач поддержки управления при оперативном реагировании на инциденты и аварии, должны обладать свойствами адекватности и адаптивности, понимаемыми соответственно как совпадение модели и моделируемой системы в отношении цели моделирования, а также как способности модели изменять структуру и параметры в соответствии с изменением состояния системы.

Приведем основные гипотезы, допущения и ограничения, принимаемые при построении предлагаемой стохастической модели техногенных аварий и катастроф.

Первая гипотеза, которая лежит в основе моделирования, заключается в предположении о каскадном характере развития инцидентов, заключающемся в возможности реализации ряда неблагоприятных сценариев вследствие возникновения инициирующего события (аварийной ситуации). При этом возможно разделение любой реализующейся последовательности событий по этапам, характеризующимся определенной длительностью развития, степенями текущей опасности состояний системы и возможностями дальнейшего перехода к критическим состояниям последующих уровней с возрастанием степени опасности и/или усилением проявления неблагоприятных факторов.

В общем случае на развитие инцидентов влияет вся предыстория событий, т.е. переходы между состояниями могут зависеть не только от предыдущего, но и от ряда предшествующих состояний, и формально описываются моделью, относящейся к классу немарковских случайных процессов. Вместе с тем, при

моделировании многие немарковские процессы удается трансформировать за счет расширения числа состояний в марковские случайные процессы. Основное допущение связано с возможностью описания наблюдаемой динамики реальных систем в рамках модели марковских процессов с дискретными состояниями и непрерывным временем на основе уравнений Колмогорова-Чепмена.

Вторая гипотеза связана с предположением о древовидной структуре наблюдаемой последовательности событий с ветвлением при переходах на последующие уровни. Соответствующие возможные реализации последовательности элементарных событий отражаются как совокупности переходов между состояниями моделируемой системы, представленных множеством вершин размеченного стратифицированного графа. Представление отображает иерархическую структуру состояний, разграничивая этапы последовательности событий в соответствии с динамикой развития аварийной ситуации и выделением страт различных уровней, включающих наборы близких по степени опасности состояний.

В основе третьей гипотезы лежит эмпирически оправданное предположение о значительных отличиях в наблюдаемой динамике на различных этапах развития аварийной ситуации. По мере развития событий и возрастании угроз на последующих уровнях происходит качественное изменение динамики переходов между принадлежащими к смежным стратам возможными состояниями системы.

Еще одно предположение связано с подбором подходящих законов для адекватного описания временной зависимости интенсивности переходов между состояниями, с учетом определенных этапов развития аварийной ситуации. Представляется обоснованным использование трехпараметрических распределений Вейбулла, позволяющих быстро и легко из анализа статистических данных либо с помощью экспертных методов осуществлять подбор необходимых параметров, при которых достигается достаточно точное соответствие изменения интенсивностей переходов между состояниями и наблюдаемой динамикой развития аварийных ситуаций и катастроф.

В качестве иллюстративного примера далее рассмотрим систему «потенциально опасный объект – инциденты» (ПОО-И), представленную размеченным стратифицированным графом на рисунке 1. Каждый из возможных сценариев после возникновения инцидента рассматривается как композиция последовательности произошедших событий, относящихся к стратам: N-нормальное состояние (Normal); A – авария (accident) (включает некоторые события C, O, а также их комбинации); F – пожар (Fire); E – взрыв (Explosion).

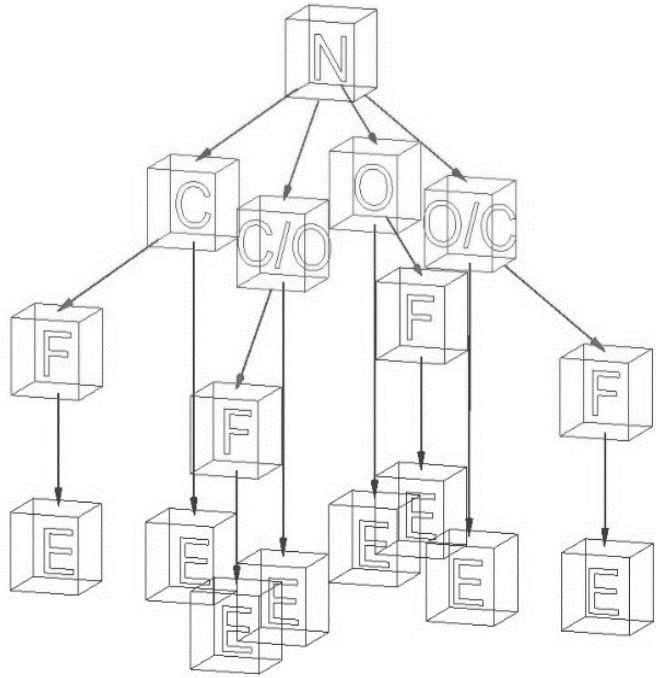


Рисунок 1 – Стратифицированный граф состояний системы «потенциально опасный объект – инциденты»

Моделирование переходов между возможными состояниями при возникновении инцидентов проводится на основе решения системы дифференциальных уравнений Колмогорова-Чепмена:

$$
\begin{cases}
\frac{dP_N}{dt} = -P_N(\lambda_C + \lambda_O + \lambda_{CO} + \lambda_{OC}) \\
\frac{dP_O}{dt} = P_N\,\lambda_C - P_C(\lambda_{F/C} + \lambda_{E/C}) \\
\frac{dP_O}{dt} = P_N\,\lambda_O - P_O(\lambda_{F/O} + \lambda_{E/O}) \\
\frac{dP_{CO}}{dt} = P_N\lambda_{CO} - P_{CO}(\lambda_{F/CO} + \lambda_{E/CO}) \\
\frac{dP_{OC}}{dt} = P_N\lambda_{OC} - P_{OC}(\lambda_{F/OC} + \lambda_{E/OC}) \\
\frac{dP_{F/C}}{dt} = P_C\lambda_{F/C} - P_{F/C}\lambda_{E/F/C} \\
\frac{dP_{F/O}}{dt} = P_O\lambda_{F/O} - P_{F/O}\lambda_{E/F/O} \\
\frac{dP_{F/CO}}{dt} = P_{CO}\lambda_{F/CO} - P_{F/CO}\lambda_{E/F/CO} \\
\frac{dP_{F/OC}}{dt} = P_{OC}\lambda_{F/OC} - P_{F/OC}\lambda_{E/F/OC} \\
\frac{dP_E}{dt} = \frac{dP_{E/C}}{dt} + \frac{dP_{E/O}}{dt} + \frac{dP_{E/CO}}{dt} + \frac{dP_{E/OC}}{dt} + \\
+ \frac{dP_{E/F/C}}{dt} + \frac{dP_{E/F/O}}{dt} + \frac{dP_{E/F/CO}}{dt} + \frac{dP_{E/F/OC}}{dt} = \\
= P_C\lambda_{E/C} + P_O\lambda_{E/O} + P_O\lambda_{E/CO} + P_{OC}\lambda_{E/OC} + \\
+ P_{F/C}\lambda_{E/F/C} + P_{F/O}\lambda_{E/F/O} + P_{F/CO}\lambda_{E/F/CO} + P_{F/OC}\lambda_{E/F/OC}
\end{cases}
\tag{1}
$$

Для задания временной зависимости интенсивности переходов между состояниями системы применяется трехпараметрическое распределение Вейбулла. Интенсивности переходов между состояниями, принадлежащим смежным уровням, описываются соответствующими распределениями, полностью задаваемыми коэффициентами масштаба, формы и сдвига:

$$
\begin{cases}
\lambda_C = \dfrac{1}{\eta_C}, \quad \lambda_O = \dfrac{1}{\eta_O}, \quad \lambda_{CO} = \dfrac{1}{\eta_{CO}}, \quad \lambda_{OC} = \dfrac{1}{\eta_{OC}}, \\
\lambda_{F/C} = \beta_{F/C} \dfrac{\left(t - \theta_{F/C}\right)^{\beta_{F/C}-1}}{\eta_{F/C}^{\beta_{F/C}}}, \\
\lambda_{F/O} = \beta_{F/O} \dfrac{\left(t - \theta_{F/O}\right)^{\beta_{F/O}-1}}{\eta_{F/O}^{\beta_{F/O}}}, \\
\lambda_{F/CO} = \beta_{F/CO} \dfrac{\left(t - \theta_{F/CO}\right)^{\beta_{F/CO}-1}}{\eta_{F/CO}^{\beta_{F/CO}}}, \\
\lambda_{F/OC} = \beta_{F/OC} \dfrac{\left(t - \theta_{F/OC}\right)^{\beta_{F/OC}-1}}{\eta_{F/OC}^{\beta_{F/OC}}}, \\
\lambda_{E/C} = \beta_{E/C} \dfrac{\left(t - \theta_{E/C}\right)^{\beta_{E/C}-1}}{\eta_{E/C}^{\beta_{E/C}}}, \\
\lambda_{E/O} = \beta_{E/O} \dfrac{\left(t - \theta_{E/O}\right)^{\beta_{E/O}-1}}{\eta_{E/O}^{\beta_{E/O}}}, \\
\lambda_{E/CO} = \beta_{E/CO} \dfrac{\left(t - \theta_{E/CO}\right)^{\beta_{E/CO}-1}}{\eta_{E/CO}^{\beta_{E/CO}}}, \\
\lambda_{E/OC} = \beta_{E/OC} \dfrac{\left(t - \theta_{E/OC}\right)^{\beta_{E/OC}-1}}{\eta_{E/OC}^{\beta_{E/OC}}}, \\
\lambda_{E/F/C} = \beta_{E/F/C} \dfrac{\left(t - \theta_{E/F/C}\right)^{\beta_{E/F/C}-1}}{\eta_{E/F/C}^{\beta_{E/F/C}}}, \\
\lambda_{E/F/O} = \beta_{E/F/O} \dfrac{\left(t - \theta_{E/F/O}\right)^{\beta_{E/F/O}-1}}{\eta_{E/F/O}^{\beta_{E/F/O}}}, \\
\lambda_{E/F/CO} = \beta_{E/F/CO} \dfrac{\left(t - \theta_{E/F/CO}\right)^{\beta_{E/F/CO}-1}}{\eta_{E/F/CO}^{\beta_{E/F/CO}}}, \\
\lambda_{E/F/OC} = \beta_{E/F/OC} \dfrac{\left(t - \theta_{E/F/OC}\right)^{\beta_{E/F/OC}-1}}{\eta_{E/F/OC}^{\beta_{E/F/OC}}}
\end{cases}
\tag{2}
$$

$$
\begin{cases}
\lambda_C = \dfrac{1}{\eta_C}, \quad \lambda_O = \dfrac{1}{\eta_O}, \quad \lambda_{CO} = \dfrac{1}{\eta_{CO}}, \quad \lambda_{OC} = \dfrac{1}{\eta_{OC}}, \\
\lambda_{F/C} = \beta_{F/C} \dfrac{\left(t - \theta_{F/C}\right)^{\beta_{F/C}-1}}{\eta_{F/C}^{\beta_{F/C}}}, \\
\lambda_{F/O} = \beta_{F/O} \dfrac{\left(t - \theta_{F/O}\right)^{\beta_{F/O}-1}}{\eta_{F/O}^{\beta_{F/O}}}, \\
\lambda_{F/CO} = \beta_{F/CO} \dfrac{\left(t - \theta_{F/CO}\right)^{\beta_{F/CO}-1}}{\eta_{F/CO}^{\beta_{F/CO}}}, \\
\lambda_{F/OC} = \beta_{F/OC} \dfrac{\left(t - \theta_{F/OC}\right)^{\beta_{F/OC}-1}}{\eta_{F/OC}^{\beta_{F/OC}}}, \\
\lambda_{E/C} = \beta_{E/C} \dfrac{\left(t - \theta_{E/C}\right)^{\beta_{E/C}-1}}{\eta_{E/C}^{\beta_{E/C}}}, \\
\lambda_{E/O} = \beta_{E/O} \dfrac{\left(t - \theta_{E/O}\right)^{\beta_{E/O}-1}}{\eta_{E/O}^{\beta_{E/O}}}, \\
\lambda_{E/CO} = \beta_{E/CO} \dfrac{\left(t - \theta_{E/CO}\right)^{\beta_{E/CO}-1}}{\eta_{E/CO}^{\beta_{E/CO}}}, \\
\lambda_{E/OC} = \beta_{E/OC} \dfrac{\left(t - \theta_{E/OC}\right)^{\beta_{E/OC}-1}}{\eta_{E/OC}^{\beta_{E/OC}}}, \\
\lambda_{E/F/C} = \beta_{E/F/C} \dfrac{\left(t - \theta_{E/F/C}\right)^{\beta_{E/F/C}-1}}{\eta_{E/F/C}^{\beta_{E/F/C}}}, \\
\lambda_{E/F/O} = \beta_{E/F/O} \dfrac{\left(t - \theta_{E/F/O}\right)^{\beta_{E/F/O}-1}}{\eta_{E/F/O}^{\beta_{E/F/O}}}, \\
\lambda_{E/F/CO} = \beta_{E/F/CO} \dfrac{\left(t - \theta_{E/F/CO}\right)^{\beta_{E/F/CO}-1}}{\eta_{E/F/CO}^{\beta_{E/F/CO}}}, \\
\lambda_{E/F/OC} = \beta_{E/F/OC} \dfrac{\left(t - \theta_{E/F/OC}\right)^{\beta_{E/F/OC}-1}}{\eta_{E/F/OC}^{\beta_{E/F/OC}}}
\end{cases}
$$

где коэффициенты: $\eta_*, \theta_*, \beta_*$ определяют масштаб, сдвиг и форму распределений изменения интенсивности λ_* переходов между состояниями (обозначены нижними индексами).

Рассмотрим основные этапы развития аварий и катастроф в рамках предлагаемой каскадной модели. Первый этап обусловлен переходом в результате возникновения инцидента из состояния «норма» в одно из состояний, соответствующих агрегированному состоянию «авария». Спонтанное формирование некоторого потенциально опасного аварийного состояния системы достаточно точно может быть описано в приближении однородного пуассоновского процесса.

Дальнейшее развитие событий в соответствии с одним из неблагоприятных сценариев связано со вторым этапом, представляющим обусловленный нарушением нормального функционирования системы переход из потенциально опасного аварийного состояния к одному из критических состояний следующего уровня. Возможен некоторый временной сдвиг при перераспределении элементов системы либо трансформации запасенной энергии. При этом формируются предпосылки возникновения с нарастающей по времени интенсивностью переходов к последующим критическим состояниям следующего уровня опасности, для которого характерны процессы неконтролируемой диссипации запасенной энергии.

Переход к третьему этапу может произойти в ходе дальнейшей трансформации системы и связан с возникновением критического события, характеризующегося резким выделением значительной доли запасенной энергии, приводящим к разрушению основных элементов системы, а также воздействию опасных факторов на находящихся в зоне поражения людей и иные объекты. Также возможен некоторый временной сдвиг, обусловленный изменением элементов системы и дальнейшей трансформацией энергии системы.

В качестве четвертого этапа развития событий в системе рассматриваются последующие состояния, связанные с возникновением и дальнейшим развитием чрезвычайной ситуации соответствующего масштаба.

Опыт моделирования динамики развития опасных событий при инцидентах, основанных на получении отдельных локальных

решений системы дифференциальных уравнений Колмогорова-Чепмена (1) с заданными распределениями Вейбулла (2), описывающих переходы между принадлежащим к смежными этапам состояниями системы позволяет сделать следующие выводы:

1. Марковская модель с представлением набора возможных элементарных состояний в виде стратифицированного графа позволяет выделять возможные сценарии развития последовательности событий при возникновении различных инцидентов.

2. Применение трехпараметрического распределения Вейбулла достаточно адекватно описывает динамику интенсивностей переходов между элементарными состояниями.

3. Полученные для избранного сценария локальные решения систем уравнений Колмогорова-Чепмена позволяют проводить численное моделирование и анализ динамики рисков возникновения и развития аварийных и критических состояний.

4. Своевременное реагирование оперативных и аварийно-спасательных подразделений служб экстренного реагирования в течение определенного «окна возможностей» приводит к торможению процессов развития событий по неблагоприятному сценарию и дальнейшему снижению степени опасности вплоть до устранения угроз и ликвидации негативных последствий инцидента.

Литература:

1. *Синицын В.В., Татаринов В.В., Прус Ю.В., Кирсанов А.А.* Совершенствование процессов управления в системе обеспечения безопасности автомобильных перевозок опасных грузов // Технологии техносферной безопасности. – 2019. – № 1(83). – С. 50-60.

2. *Синицын В.В., Татаринов В.В., Прус Ю.В., Кирсанов А.А.* Моделирование системы поддержки принятия управленческих решений при ликвидации автомобильных аварий с опасным грузом // Технологии техносферной безопасности. – 2019. – № 2 (84). – С. 84-90.

3. *Кирсанов А.А., Прус М.Ю., Туниеков Д.С.* Системы информирования об автомобильной аварии с опасным грузом / Материалы XXVII международной конференции «Проблемы

управления безопасностью сложных систем» (ПУБСС-2019) (18 декабря 2019 г. Москва). – М.: ИПУ РАН, 2019. – С. 372-377.

4. *Kirsanov A.A., Tatarinov V.V., Prus Y.V.* Decision support software for chemical accident elimination management // AIP Conference Proceedings. – AIP Publishing LLC, 2019. – V. 2195. № 1. – P. 020076.

Мистров Л.Е., Головченко Е.В.

Основы моделирования мероприятий информационной безопасности для обеспечения конфликтной устойчивости функционирования социально-экономических организаций

Аннотация: Предлагаются основы математического моделирования мероприятий информационной безопасности для обеспечения конфликтной устойчивости авиационных социально-экономических организаций на основе критерия «эффективность-стоимость». Основы базируются на методах теорий многоуровневых иерархических систем, теории игр, гомотопическом методе исследования нелинейных оптимизационных задач с экстремальными переменными и методе Гаусса-Зейделя.

Ключевые слова: социально-экономическая организация, конкуренция, конфликтная устойчивость, многошаговая биматричная игра, математическое моделирование

Авиационные перевозки являются одним из самых развивающихся отраслей экономики. Функционирование авиационных предприятий гражданской авиации характеризуется широкой географией, значительным спектром предоставляемых услуг и одновременно жесткими требованиями по обеспечению авиационной безопасности. Все это существенно ужесточается в условиях конкуренции. В связи с чем, проблемным вопросом является необходимость обеспечения конфликтной устойчивости (КУ) функционирования таких авиационных социально-экономических организаций (СЭО), каковыми и являются авиационные предприятия (АП). При этом особую актуальность приобретают вопросы математического моделирования технико-экономического обоснования мероприятий информационной

безопасности (ИБ), направленных на обеспечение КУ функционирования СЭО.

В общем случае АП осуществляет свою деятельность в условиях конкурентного взаимодействия с большим количеством СЭО. Обозначим авиационную СЭО множеством $\{A\}$, а все взаимодействующие с ней СЭО – $\{B\}$. Предположим, что КУ функционирования АП достигается реализацией совокупности мероприятий ИБ. В результате чего процесс конкурентного взаимодействия сторон $\{A\}$ и $\{B\}$ можно представить в виде многошаговой биматричной игры на выживание с ненулевой суммой:

$$\max_{\{p_i\}} \min_{\{g_j\}} \left\{ \frac{\sum_{i,j} a_{ij} p_i g_j}{\sum_{i,j} b_{ij} p_i g_j} \right\} = \min_{\{g_j\}} \max_{\{p_i\}} \left\{ \frac{\sum_{i,j} a_{ij} p_i g_j}{\sum_{i,j} b_{ij} p_i g_j} \right\}, \qquad (1)$$

где i – возможные стратегии стороны $\{A\}$, содержащие определенную совокупность мероприятий индивидуальной (БИ), групповой (БГ) и общей (ОБ) ИБ; j – возможные стратегии стороны $\{B\}$; $\|a_{ij}\|$, $\|b_{ij}\|$ – платежные матрицы сторон $\{A\}$ и $\{B\}$, элементы которых характеризуют их выигрыш (проигрыш) и равны: $a_{ij} = Э_{ij}^A / C_i^A$, $b_{ij} = Э_{ij}^B / C_j^B$; $Э_{ij}^A$, $Э_{ij}^B$ – эффективность функционирования сторон; C_i^A, C_j^B – стоимость реализации i -ых и j -ых мероприятий (стратегий в терминах теории игр) ИБ сторон $\{A\}$ и $\{B\}$, соответственно. Результатом конфликтного взаимодействия является средняя (в смысле математического ожидания) цена n -шаговой конкурентной борьбы (игры) $Ц^*$ в условиях оптимальной (равновесной) или рациональной (смешанной) стратегии сторон (соответственно $R_{i^*j^*}$ или $\overline{R}^*$).

Следует отметить, что поскольку биматричные игры решаются приближенным методом последовательного исключения «доминируемых» стратегий, сводя их к игре типа «2х2» и выбору из них одной (или двух) стратегий стороны $\{A\}$ – $i_1^* = 1$ (или $i_2^* = 2$), то конечное решение является условным, которое подлежит последующему анализу с использованием дополнительных критериев.

Инвариантное моделирование оценки эффективности используется и при решении задач нижних уровней СЭО с использованием методов Гаусса-Зейделя и гомотопического метода решения оптимизационных нелинейных многоуровневых задач с экстремальными ограничениями [1]: на уровне функциональной СЭО – обоснование целесообразного варианта комплекса мероприятий БО, БГ и БИ для каждой i -ой стратегии стороны $\{A\}$ (или, что то же самое для каждого j -го варианта стороны $\{B\}$); на уровне составных ОТС – комплекса ИБ, включающих мероприятия БО, БГ и БИ; на уровне отдельных технических систем – комплекса ИБ, включающих мероприятия БГ и БИ; на уровне комплексов – комплекса ИБ, включающих мероприятия БИ.

Для определенности рассмотрим одну из инвариантных задач математического моделирования технико-экономического обоснования КУ СЭО для обоснования оптимального варианта мероприятий ИБ с позиции критерия «эффективность-стоимость» в условиях ограниченного использования обеспечивающего ресурса, то есть ограничений. Данная задача решается с использованием теоретико-игрового метода [1], но применительно к частным внешним условиям игры сторон $\{A\}$ и $\{B\}$ и к каждому i -му начальному варианту (далее для упрощения записи индекс i будем опускать).

В рамках теоретико-игрового метода необходимо определение масштабных численных оценок, которые в относительных величинах позволяют сформировать значения элементов платежных матриц $\|a_{ij}\|$, $\|b_{ij}\|$ конкурирующих сторон. Для оценки оптимальности (целесообразности) генерируемых вариантов мероприятий ИБ введем понятие коэффициента технико-экономической целесообразности любого r -го, $r = \overline{1,R}$ варианта мероприятий ИБ применительно к любому j -му $j = \overline{1,J}$ варианту мероприятий ИБ стороны $\{B\}$ в виде:

$$K_r^A = \frac{C_0^A(1-\alpha_r)\sum\limits_{i=1}^{I}\gamma_i^r\left(\min\limits_{j\in\{J\}}\left[\overline{P}_{rj}^{\,i}(\alpha_r)\right]\right)}{C_0^A\sum\limits_{i=1}^{I}\gamma_i^{r=0}\left(\min\limits_{j\in\{J\}}\left[\overline{P}_{rj}^{\,i}(\alpha_r=0)\right]\right)}, \qquad (2)$$

где C_0^A – суммарная стоимость элементов стороны $\{A\}$ $(i=\overline{1,I})$, обеспечиваемых мероприятиями БИ, БГ и БО, конкретная совокупность которых (вариант) определяется при решении данной задачи; $\alpha_r = C_r^A / C_0^A$ – относительная стоимость *r*-го варианта мероприятий ИБ; $\gamma_i^r = C_i^A / C_0^A$ – относительная стоимость совокупности элементов *i*-го типа, обеспечиваемых *r* -ым вариантом мероприятий ИБ; $\overline{P}_{rj}^i(\alpha_r)$ – математическое ожидание вероятности (среднее значение в серии испытаний) достижения целей *r* -го варианта мероприятий ИБ в отношении элементов *i* -го типа системы $\{A\}$ при *j* -ом воздействии системы $\{B\}$. Например, это может быть среднее количество элементов *i* -го типа, сохранивших свою эффективность функционирования; $\overline{P}_{rj}^i(\alpha_r = 0)$ – математическое ожидание вероятности сохранения эффективности функционирования элементов *i* -го типа системы $\{A\}$ при *j* -ом воздействии системы $\{B\}$ в отсутствии мероприятий ИБ (в этом случае относительная стоимость мероприятий ИБ равна нулю).

С учетом вышеизложенного, под коэффициентом технико-экономической целесообразности K_r^A понимается отношение стоимости элементов стороны $\{A\}$, сохранивших свою эффективность при реализации *r* -го варианта мероприятий ИБ в условиях конкурентных отношений со стороной $\{B\}$ к стоимости элементов стороны $\{A\}$ без применения *r*-го варианта.

При выборе оптимального варианта мероприятий ИБ используется, как правило, максиминный критерий вида [1]

$$\begin{gathered} \grave{A}rg\,\alpha^* \to \max_{\{\alpha_r\}}\left(K_r^A = (1-\alpha_r)\frac{1}{f_0}\sum_{i=1}^{I}\gamma_i^r\left(\min_{j\in\{J\}}\left(\overline{P}_{rj}^i(\alpha_r)\right)\right)\right), \\ f_0 = \sum_{i=1}^{I}\gamma_i^{r=0}\cdot\left(\min_{j\in\{J\}}\left(\overline{P}_{rj}^i(\alpha_r=0)\right)\right),\ \alpha_r = \alpha_1+\alpha_2+\alpha_3, \end{gathered} \tag{3}$$

где α_1, α_2, α_3 – относительная стоимость *r*-го варианта мероприятий БИ, БГ, БО, отличающиеся целями, средствами, составом и способами применения. Их значения задаются (определяются на нижних уровнях) при следующих ограничениях:

$$P_r = \sum_{i=1}^{I} \gamma_i^r \cdot \left(\min_{j \in \{J\}} \left(\overline{P}_{rj}^{\,i}(\alpha_r) \right) \right) \geq P_{зад} \;\; K_r^A \geq 1; \quad C_0^A = const; \qquad (4)$$

$$0 \leq \alpha_r < 1 \text{ для всех } r \in \{R\}.$$

Из выражения (3) следует, что поиск оптимального варианта мероприятий ИБ представляется в виде максиминной дискретной стохастической оптимизационной задачи. Для ее решения возможно применить последовательный поэтапный итерационный алгоритм, включающий следующие этапы.

На первом этапе формируют конкретные варианты мероприятий ИБ, используя полученные решения на нижних уровнях, относительно возможных (условных) оптимизационных решений при обосновании целей, средств, составов и способов применения мероприятий БИ, БГ, БО, то есть условно-оптимальных значений множества (α_1, α_2, α_3) на основе их сочетаний. Все сформированные варианты нумеруются по возрастанию номеров r и для всех вариантов рассчитываются значения относительной их стоимости α_r. Варианты, для которых значения α_r не удовлетворяют ограничительным условиям (4) отбрасываются.

На втором этапе для каждого r-го варианта мероприятий ИБ рассчитываются значения $\overline{P}_{rj}^{\,i}(\alpha_r)$. При этом используются математические модели процессов функционирования СЭО, способные учитывать все стратегии $j = \overline{1,J}$ поведения стороны $\{B\}$. С использованием методов кусочно-линейной аппроксимации и вычисленным дискретным значениям формируется непрерывная функция $\widetilde{P}(\alpha) \approx P(\alpha)$.

На третьем этапе осуществляется определение оптимального значения α^* из условия: $\max_{\alpha} \left(\widetilde{K}'(\alpha) = K(\alpha) \cdot f_0 = (1-\alpha) \cdot \widetilde{P}(\alpha) \right)$ при ограничениях $0 \leq \alpha_r < 1$ и $f_0 < \widetilde{P}(\alpha) \leq 1$ и определяются оптимальные значения $\widetilde{K}(\alpha = \alpha^{opt})$ и $\widetilde{P}(\alpha = \alpha^{opt})$. Далее осуществляется проверка условия $\widetilde{P}(\alpha = \alpha^{opt}) \geq P_{зад}$. Если условие выполняется, то является достаточным исключить из дальнейшего рассмотрения все варианты, для которых $\alpha < \alpha^{opt}$ до значения α', при котором $\widetilde{P}(\alpha') \geq P(\alpha)$. В случае когда условия не выполняются, требуется проведение анализа дальнейших решений.

На четвертом этапе осуществляется этап поиска окончательного решения. Поскольку решается частная (по условию) задача на основе гомотопического метода исследования оптимизационных нелинейных задач, то для сужения области поиска оптимального решения осуществляется последующий переход от абсолютных значений критериальной функции $\alpha = \alpha^{opt}$ к поиску рационального решения по технико-экономическим показателям на основе принципа оптимальности Парето.

Решение оптимальности по Парето позволяет выделить и сузить область возможного компромисса на основе ослабления исходных требований к критерию «эффективность-стоимость» (в случае $\alpha^{opt} \neq \Delta\alpha^{\Pi}$), где $\Delta\alpha^{\Pi}$ есть некоторый заданный предел (например: 5% от $\widetilde{P}(\alpha = \alpha^{opt})$) в условиях ($\Delta\left|\alpha^{\Pi}\right| \to 0$). Введение принципа оптимизации по Парето при обосновании рациональных (уже не оптимальных) вариантов является существенным, поскольку может значительно улучшить решение на вышестоящем уровне иерархии исследований, снизить требования к формируемым вариантам за счет совместного использования в их составе разнотипных мероприятий ИБ, а также приблизиться к модели (принципам предпочтительности) оптимальности заказчика.

В этом случае целесообразным вариантом мероприятий ИБ является тот, который обеспечивает минимальное значение ($\alpha^{opt} - \Delta\alpha^{\Pi}$), то есть стоимости. Следует отметить, что математические модели для решения оптимизационных задач нижних уровней рассматриваемых мероприятий могут быть поставлены и решены аналогичным образом.

Таким образом, предложенные основы математического моделирования мероприятий по ИБ позволяют обосновать по критерию «эффективность-стоимость» целесообразный вариант комплекса мероприятий для обеспечения КУ функционирования СЭО.

Литература:

1. *Мистров Л.Е.* Синтез конфликтно-устойчивых функциональных радиоэлектронных систем / Математическое моделирование информационных и технологических систем: Сборник научных трудов. – Воронеж: ВГТА, 2003. – Вып. №6. – С. 193-199.

Сидоренко И.А., Дудариков О.Н., Ходырева Н.Е.

Средства информационной поддержки принятия решений по оценке возможностей видовых технических разведок

Аннотация: Анализ возможностей технических разведок иностранных государств по добывания и вскрытия охраняемых сведений о Вооруженных Сил Российской Федерации показывает, что ведущие страны мира активно наращивают возможности технических средств разведки. В настоящее время для оценки эффективности противодействия данным разведкам используется методический аппарат, разработанный ФСТЭК России. Опыт его практического применения показывает низкую достоверность получаемых оценок, а также громоздкость проводимых вычислительных процедур, что требует достаточно большого резерва времени, который на практике отсутствует. В связи с этим, возникает необходимость автоматизации оценки возможностей сигнальных технических разведок и разработки специализированного программного обеспечения, решающего данные задачи. В результате проведенного анализа возможностей технических средств и применяемого методического аппарата разработаны два алгоритма для оперативной оценки возможностей радио- и радиотехнической разведки противника, отвечающие основным требованиям войсковой практики: простота реализации, минимальное количество исходных данных, минимальное время на проведение, наглядность, приемлемая достоверность, возможность автоматизации расчетов.

Ключевые слова: оптико-электронная разведка, инфракрасная разведка, методика оценки вероятностей вскрытия и обнаружения

Введение

Анализ возможностей технических разведок иностранных государств по добывания и вскрытия сведений военного и военно-технического характера о состоянии, деятельности и развитии

Вооруженных Сил Российской Федерации показывает, что ведущие страны мира продолжают модернизировать свои разведывательные службы, совершенствуют техническую разведку, наращивают ее возможности. Современные комплексы и системы с широким спектром разведывательных возможностей действуют против России постоянно на всей территории нашей страны. Кроме того, ведение разведки вероятным противником в последнее время характеризуется высокой чувствительностью разведывательной аппаратуры и оперативностью доставки, обработки и анализу разведывательных сведений. Вышеперечисленные факторы требуют организации качественного противодействия техническим средствам разведки иностранных государств, что невозможно без своевременной оценки их возможностей, вскрытию технических каналов утечки информации и оперативному принятию эффективных мер по их закрытию (ослаблению). В настоящее время для оценки возможностей радио- и радиотехнических разведок используется методический аппарат, разработанный ФСТЭК России. Опыт его практического применения показывает низкую достоверность получаемых оценок, а также громоздкость проводимых вычислительных процедур, что требует достаточно большого резерва времени, который на практике отсутствует. В связи с этим, возникает необходимость автоматизации оценки возможностей видовых технических разведок и разработки специализированного программного обеспечения, решающего данные задачи.

Обосновывая необходимость разработки программного обеспечения, по оперативной оценке, возможностей технических средств разведки следует обратить внимание на следующее обстоятельство. При передислокации объектов и подразделений возникает потребность в прогностических функциях оценки разведобстановки в предполагаемом районе их развертывания с целью планирования и выполнения мер противодействия техническим средствам разведки. Поэтому задача прогнозирования разведдоступности и соответствующих мер противодействия техническим средствам разведки в условиях повышения маневренности объектов защиты, динамики современных вооруженных конфликтов и объективной неполноты исходных данных делает актуальной разработку соответствующих методик

оперативной оценки возможностей технических средств разведки. Очевидно, что данная методика должна применяться на всех уровнях иерархии управления войсками и оружием, начиная от самого объекта.

Исходя из указанных требований следует, что число показателей количественной оценки разведдоступности должно быть минимальным, физически понятным и содержать пространственные параметры. Реализация любой математической модели оценки предполагает выбор показателя оценки, методики проведения расчетов и выработку рекомендаций. Прежде всего, следует определить требования к выбору показателей оценки. В качестве показателей для оценки возможностей разведки устанавливают вероятность обнаружения W_o, вероятность распознавания W_p.

При комплексном решении задачи противодействия техническим средствам разведки важным показателем для видовой разведки становится вероятность распознавания. Реализация методики предполагает использование исходных данных по объекту защиты, средству разведки и условиям ведения разведки. Результатом оценки является численное значение выбранного показателя и сравнение его с нормативным.

Таким образом, в качестве главного условия применения методики оценки примем условие ее реализуемости в войсковой практике. В этом случае можно предъявить следующие требования к подобной методике: простота реализации, минимальное количество исходных данных, минимальное время на проведение, наглядность, приемлемая достоверность, возможность автоматизации расчетов.

Для разработки алгоритма рассматриваемой методики, проведен анализ оценок разведдоступности объектов комплексного технического контроля средствами визуальной разведки, в результате которого составлены два алгоритма решения данной задачи – графоаналитический и автоматизированный.

Графоаналитический алгоритм автоматизации методики оценки вероятностей обнаружения, представленный на рисунке 1, основывается на обобщении данных по средствам разведки, условиям разведки и результатам измерительного контроля с

дальнейшим представлением полученных данных в виде графических зависимостей, которые используются для получения численных значений оценки возможностей визуальной разведки.

Данный алгоритм предполагает наличие указанных графиков и проведение элементарных расчетов, для которых не обязательны средства вычислительной техники, что позволяет с необходимой оперативностью вычислить вероятность обнаружения.

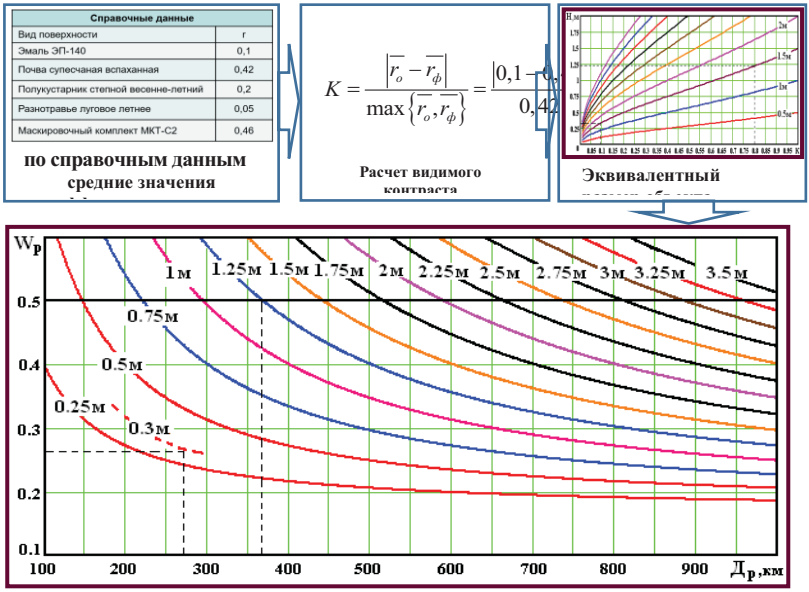


Рисунок 1 – Содержание графоаналитического алгоритма оперативной оценки возможностей ТВР и эффективности мер ПД

Автоматизированный алгоритм (рисунок 2) основывается на файловых данных, которые оформляются в виде программно-алгоритмической реализации. Этот алгоритм предполагает наличие вычислительных средств с заранее установленной программой оценки.

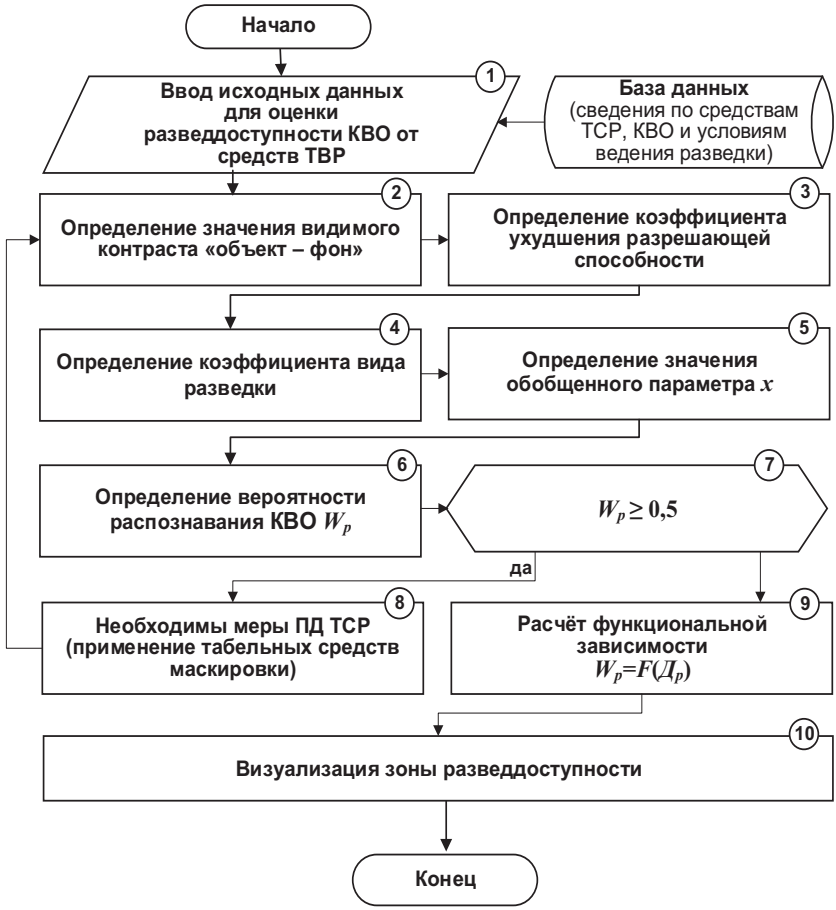


Рисунок 2 – Графоаналитический алгоритм оценки возможностей визуальной разведки

Представленный методический подход позволяет оперативно оценивать возможности технических разведок при недостатке исходных данных. Кроме того, предложенные решения могут быть автоматизированы в виде комплекса специальных программных средств оценки разведдоступности объектов защиты, тем самым перейдя на автоматизированный алгоритм.

Литература:

1. *Меньшаков Ю.К.* Теоретические основы технических разведок: Учеб. пособие / Под ред. Ю.Н. Лаврухина. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.

2. *Хорев А.А.* Теоретические основы оценки возможностей средств видовой разведки. – М.: Минобороны России, 2000. – 255 с.

3. *Хорев А.А.* Оценка возможностей средств оптико-электронной разведки // Специальная техника. – 2009. – № 3. – С.55-61.

4. *Кравцов Е.В.* Методический подход к комплексной оперативной оценке возможностей выявления сведений об объектах защиты // Телекоммуникации. – 2020. – № 9. – С. 33-41.

5. *Леньшин А.В., Кравцов Е.В.* Методика адаптивного распределения сил и средств комплексного технического контроля по объектам защиты в различных физических полях разнесенного приема // Радиотехнические и телекоммуникационные системы. – 2020. – № 4. – С. 15-22.

6. *Леньшин А.В., Кравцов Е.В., Рюмшин Р.И., Сенюков Г.А.* Оценка возможностей радиотехнической разведки по результатам контроля радиоэлектронных средств комплексом радиотехнического контроля // Динамика сложных систем – XXI век. – 2015. – № 3. – С. 29-35.

7. *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.

Plotnikov N.I.

Psychological modeling of air traffic control communications in protection against mid-air collisions and near misses of aircraft in air navigation

Abstract: In this paper, mid-air collisions and near misses of aircraft are investigated in the aspect of communication between the flight crew and the air navigation service. A statistical review of the observations and the analysis reveals that the most important solution to blocking the danger are the parameters of the "air traffic controller - pilot" communication in the interaction of the crew and the service. It has been

established that the essential parameters of the interaction between controllers and pilots are the structure, context and channels of voice communications, which have a much more complex structural content that is absent in modern standards. In practical terms, the work is aimed at developing collision protection recommendations by optimizing the standards of the regulatory framework.

Keywords: air navigation, collisions, near misses, aircraft, flight safety, air traffic controller, pilot, communications

Introduction

Mid-Air Collision (MAC) is an air accident (AA) in which two aircraft collide in flight. Air collisions almost always lead to two crashes of the colliding aircraft. Near misses (NM), airmisses, near collisions) are prerequisites for collisions: runway, on taxiing with parked aircraft, with obstacles on the ground - controlled flight into terrain (CFIT) of the world civil aviation (CA). The reasons for the MAC and NM are assessed not in favor of the aircraft crew in a ratio of 1:4 [1]. In this paper, MAC and NM events are investigated in the aspect of communications between the aircraft crew and the ATC service. A statistical review observation was performed. The analysis reveals that the most important solution to blocking the danger is the parameters of the "controller-pilot" communication in the interaction of the aircraft crew and the ATC service. It has been established that the essential parameters of interaction between air traffic controllers and pilots are the structure, context and channels of voice communications, which have a much more complex structural content that is absent in modern ATC standards. In practical terms, the work is aimed at developing recommendations for FS by optimizing the standards of the regulatory framework.

Problem Overview

The existing methods for calculating the MAC and NM are extremely complex. That is approximately considered as movement (NM) at distances (S) equal to or less than half the interval of the normalized flight level (FL) (1):

$$\mathrm{NM}: S_{\mathrm{NM}} \leq S_{\mathrm{FL}}/2. \quad (1)$$

The regulatory framework for the regulation of air traffic is dispersed in numerous documents and requires a clearer subject identification of terms and definitions. The connection between MAC and NM should be recognized as stochastic. The presented statistics are fragmentary, can be recognized as examples of accounting and do not allow for a full analysis of air traffic services (ATS). The general problem is the uncertainty as to how established and justified the relationship between the accident and the quality of communications "controller-pilot". Communication takes place on the audio channel. The controller can "self-confirm" visually by the locator, that is, "see what heard". Meanwhile, this very moment appears in the accident investigations, when the pilot misunderstood the instruction [2]. The most vulnerable points are the points of "blooper" (lapsus linguae) and "mishearing" messages. The biggest problem is the hear back problem [3, 4].

Method and Task

The method of resource modeling in this work is considered by the author as a scientific approach to the study of complex and weakly structured scientific problems, the solution of which by known theories and methods is not possible and is not achieved over long periods of time. The method is installed in the sequence of performing statistical analysis of events, information modeling. Due to the lack of acceptable mathematical methods, symbolic formalizations are used to formulate and solve the problem of this work [5]. The aim of the study is to find and establish new theoretical approaches to modeling events, suitable for calculation and computing. The operational reliability of the interaction requires modern technical means, depends on professional training, experience and operational WL. The safety conditions in the simplest form can be written as the ratio of the actual workload (AWL) and the normative workload (NWL) of pilot (P) and controller (C), corresponding to the standardized risks (2):

$$\left\{\begin{matrix}\mathrm{AWL_P} \le \mathrm{NWL_P} \\ \mathrm{AWL_C} \le \mathrm{NWL_C}\end{matrix}\right\} \le \mathrm{F}_{AA}\left\{\begin{matrix}1 \cdot 10^{-7}\ \frac{1}{\text{час}}, MAC \\ 5 \cdot 10^{-4}\ \frac{1}{\text{час}}, \mathrm{NM}\end{matrix}\right\}, \qquad (2)$$

where F – function of solving the problem of blocking danger of AA.

Psychological Modeling of ATC Communications

This paper briefly examines the subject of message formation from the standpoint of the mathematical theory of communication, qualitative information theory [6, 7], psycholinguistics theory of communication [7]. The evaluation of these theories is carried out to establish the possibilities of their application. Communication channels in psychology are studied as ways of transmitting and receiving messages through the senses: A - auditory (hearing), V - visual (vision), K - kinesthetic (tactile). There is also a digital (discrete) channel, which is also considered part of the A-channel. The totality of the AVK-channels of an individual in the transmission and reception of messages forms the representative system (RS) of a person. If any channel in a person predominates in nature and experience, then this is called the leading system (LS). In psychology, it has been established that regardless of the LS, the communication channels of people differ in the completeness of the volume and the accuracy of the content. The most accurate in terms of content is the A-channel. The most complete in terms of volume is the K-channel. The simplest model for assessing the reliability of communications in this work is presented as follows (table 1).

Table 1 – AVK Communication model

	Communication		Reliability	
Channel	Transmitter	Receiver	Completeness	Accuracy
A	speaks	listens	minimum	high
B	shows	looks	average	average
K	moves	feels	high	minimum

Since each person's RS is unique, this leads to a fundamental obstacle - **the problem of understanding**. It has been established that there are ways to re-encode messages between channels. The receiver subject is able to recode, for example, an A-message into a B-message, or "see what was said." Just draw what you were told. Similar transcoding is possible between other channels. Let's compose a more complex communication model as a two-dimensional matrix. Since such developments are unknown in the studies known to the author, this model is presented as an original one, having a theoretical value and a

basis for further research. Fragments of the model, which are pseudo-channels of communication, are italicized. For their interpretation, there is still not enough theoretical knowledge and experiments. The demonstration of this model shows that the "controller-pilot" communication standardized in modern technologies is carried out mainly according to one of all possible options (cell "AA" of the таble 2).

Table 2 – AVK Communication Matrix

Subjects → / Transmitting message ↓		Receiving message: }B seen	Receiving message: }A heard	Receiving message: }K simulated
Transmitting message	B→ shown	}BB→ seen shown B→}B shown for vision	*}AB→ heard shown* *B→}A shown to hear*	}KB→ simulated shown B→}K shown for imitations
Transmitting message	A→ said	}BA→ seen what said A→}B said for vision	**}AA→ heard what said** **A→}A said to hear**	}KA→ simulated what said A→}K said for imitation
Transmitting message	K→ movement	}BK→ movement seen K→}B movement for vision	*}AK→ heard movement* *K→}A movement to hear*	}KK→ simulated movement K→}K movement for imitation

The solution to the problem is to find a way to include all theoretically identified channels to achieve reliable communications. However, even standard ATC communications have structural complexity that distorts messages and poses a threat to flight safety. An example of modelling is presented below.

Experimental Model of Distortion of Standard ATC Communications. Communication is carried out on the A-channel "speaking-listening". A call to communication can be carried out by the controller of the ATC and the crew of the aircraft. Let a standardized communication session (CS) contain communication procedures (CP), consisting of three pairs or six communication operations (CO). The six operations are called in this work the Operational Directive Loop (OPL) for ATC purposes. Other CP are called the ATC off-line circuit, for example, such as mutual informing of the controller and the crew about the meteorological conditions of the flight.

Demonstration of the failure of communication technology can occur in the following scenario. In the controller message 1A [b], the pilot misheard and repeats the numbers by mistake 1P [a]. The controller does not hear or listen to the content of 2P [v]. His attention is focused only on the very fact that his instruction is being repeated. The controller gives 3A [b] confirmation of the pilot's incorrect answer or does not give any confirmation. The communication chain generates distortion of each CO and the OPL collapses (3).

$$1\mathrm{C}[\mathrm{в}] \stackrel{\text{def}}{=\!=} \rightarrow \{1\mathrm{P}[\tilde{\mathrm{а}}] \rightarrow 2\mathrm{P}[\tilde{\mathrm{в}}] \ \rightarrow 3\mathrm{C}[\tilde{\mathrm{в}} \rightarrow 3\mathrm{P}[\tilde{\mathrm{а}}]\} \neq \stackrel{\text{def}}{=\!=} 1\mathrm{A}[\mathrm{в}]. \qquad (3)$$

The pilot in operation 3P [a] does not seek confirmation of the connection, since he has no doubts about the content of the air traffic control message 1C [b] (!). This excludes the last opportunity to correct a mistake, possibly tragic. These examples demonstrate many prerequisites for disruption of communications even in standardized ATC communications.

MAC and NM prevention task The event (E) of blocking the air traffic control system is defined as the formulation and solution of the problem of air navigation, flight operation in the "controller-pilot" communication. Air navigation (A), flight operation (P) and their parameters constitute a complex for performing a safe flight {A-P}. The observation base (M) and many of its manifestations are a methodological solver of the problem. The general condition of the problem is written (4):

$$\text{MAC (NM)}: \begin{Bmatrix} M\{\mathrm{A.P}\} \rightarrow f(\mathrm{E}\ ), \text{the event occur} \\ M\{\mathrm{A.P}\} \rightarrow f'(\bar{\mathrm{E}}\ ), \text{the event does not occur} \end{Bmatrix}, \qquad (4)$$

where f and f' are functions of the initial and ultimate protection in solving the problem.

Let, for each $M_i \in M$ there is an environment $A_i \in A$ and conditions $P_i \in P$, when any event $E_i > 0$ in the phase space $\{E; \overline{E}\}$ is impossible if the function of the limit protection solver and hazard blocking $M_i \rightarrow \max f'$. Particular tasks for observation parameters can be formulated in a similar way. In accordance with the projected content of the subject area, observation tasks for objects in natural language (NL) are formed with a subsequent formalized description. Parameter names can be taken as object names, one of which is determined by the observation base.

Conclusion

This work has a search character with the aim of researching new, previously unexplored aspects of air navigation. It is postulated that air traffic controller-pilot communications are the main component of ATS safety management and MAC (NM) events prevention. Reliability of communications between the controller and the pilot is the resultant parameter of air traffic safety surveillance. The development and design of a flight safety complex was carried out, the identification of the main object: communications "controller-pilot" and threat events. The subject of the interaction between the pilot and the controller requires interdisciplinary research and development. Fundamental solutions may be the introduction of visual and kinesthetic channels into communication for communication through technological advances.

References:

1. Process for Conducting Joint Implementation Measurement And Data Analysis Teams (JIMDATs) DRAFT. – June 2004 Draft.

2. *Kleeman J.* ATC training: realism and training effectiveness // The Controller. – 1986. – V. 24. № 3. – P. 13-18.

3. *Kreamer T.* Listen-Read back-Comply // Air Line Pilot. – 1986. – V. 55. № 7. – P. 41-43.

4. *Pope J.A.* The hear back problem // FSF Accident Prevention Bull. – 1986. – V. 43. № 10 (3).

5. *Plotnikov N.I.* 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, 2021. – P. 116-130.

6. *Mazur M.* Qualitative theory of information. – M.: Mir, 1974. – 239 p. (in Russian).

7. *Plotnikov N.I.* Information intelligence: how closed information is created from open sources. Monograph. – Novosibirsk: SB RAS, 1998. – 131 p. (in Russian). – URL: http://aviam.org/index.php/layout/library (дата обращения 1.09.2021).

Степанцов М.Е.

Об одной особенности моделирования первого этапа распространения инфекции COVID-19

Аннотация: В работе рассмотрен ход моделирования распространения инфекции на первом этапе пандемии, выявлены несоответствия между результатами моделирования при помощи непрерывных функций и на основе дискретных моделей класса клеточных автоматов. По результатам анализа этих несоответствий указано на возможную ошибку при использовании непрерывных моделей в данном случае и даны рекомендации по ее избеганию.

Ключевые слова: распространение инфекции, математическое моделирование, дискретные модели, клеточные автоматы

Безусловно, главной проблемой безопасности на данном этапе развития человечества стала пандемия новой коронавирусной инфекции и последствия как самого заболевания, так и ограничительных мер, призванных сдержать ее распространение. Математическое моделирование динамики этих процессов представляет собой не просто задачу с рядом неопределенных параметров – оно является задачей, в которой не определено, какие параметры и в какой степени являются неопределенными.

Так, в этот период постоянно менялись данные о различиях в характере распространения разных штаммов вируса, взятие анализов на наличие вируса в разных странах производилось у разных групп населения, использовались тесты разного качества с

неизвестной долей ложноположительных и ложноотрицательных результатов, в ряде регионов в статистику заболевших были включены пациентов с любыми проявлениями ОРВИ или, напротив, исключались лица без симптомов заболевания. Что касается статистики смертности от коронавируса, подходы к тому, что считать причиной смерти также разнились по странам и регионам [1]. Наконец, имеют право на существование подозрения в том, что из политических или иных соображений в некоторых случаях показатели заболеваемости и смертности сознательно искажались в ту или иную сторону. Благодаря такой неопределенности также не представляется возможным учесть прямое влияние ограничительных мер на распространение заболевания, если твердо придерживаться принципа «после – не обязательно означает вследствие».

В этих условиях, тем не менее, проводилось много исследований с использованием классических непрерывных моделей динамики распространения инфекции, например, [2-3]. В большинстве случаев они основывались на том, что при исследовании начального этапа пандемии может быть рассмотрен лишь один объективный показатель: официально заявленное число зараженных людей.

Представлялось интересным попытаться построить дискретные модели распространения инфекции, например, на основе клеточных автоматов, и сравнить порождаемую ими динамику с непрерывными вариантами моделей. Исходя из вышеприведенных рассуждений о неопределенностях, рассматривалось только количество «официально» заразившихся людей и было сделано предположение, что в каждой отдельной стране или на обособленной территории динамика этого показателя определяется двумя факторами: способностью вируса к распространению и неким обобщенным сдерживающим фактором.

Таким образом, можно предположить, что определяется в отсутствии сдерживающего фактора количество зараженных описывается простейшим дифференциальным уравнением

$$\frac{dN}{dt} = kN, \tag{1}$$

а при его наличии – уравнением Ферхюльста [4]

$$\frac{dN}{dt} = kN\left(1 - \frac{N}{M}\right) \quad (2)$$

Решениями этих уравнений являются экспоненциальная функция

$$N(t) = Ae^{kt} \quad (3)$$

при рассмотрении начального роста, и логистическая кривая

$$N(t) = \frac{B}{1 + Ce^{-kt}} \quad (4)$$

после начала действия сдерживающего фактора соответственно.

Далее в ходе исследования эта динамику была описана при помощи простого дискретного отображения, а также математических моделей, представлявших собой одномерный и многомерные клеточные автоматы с различными типами окрестностей. Следует указать, что в рамках этого исследования не удалось получить оригинальных результатов, принципиально отличающихся от полученных в рамках непрерывной модели.

Однако в ходе моделирования обнаружилась одна любопытная особенность. Первым значимым событием в развитии эпидемии в стране или регионе можно считать момент, когда рост числа заболевших начинает отставать от экспоненциального – в этот момент можно утверждать, что сдерживающий фактор (чем бы он ни был) начал действовать, а также имеет смысл заменять регрессию к экспоненциальной функции (3) регрессией к логистической кривой (4).

В ходе вычислительных экспериментов момент замедления роста заболеваемости определялся как день, после которого реальное количество заболевших становилось меньшим 99% предсказанного при моделировании неограниченного роста. При использовании дискретных моделей любого типа этот момент наступал на несколько дней позже, чем при использовании непрерывных моделей.

Причина этого, как удалось выяснить, состоит в том, что регрессия к экспоненциальной кривой обычно производится путем линеаризации исходной модели, то есть логарифмирования выражения (1)

$$\ln N = \ln A + kt \quad (5)$$

и применения линейной регрессии к полученной зависимости. При этом фактически минимизируется относительное, а не абсолютное расхождение между экспериментальными и теоретическими значениями. При использовании же дискретной модели ее коэффициенты подбираются исходя из минимизации евклидова расстояния между результатами вычислительного эксперимента и наблюдаемыми данными. В рассматриваемом случае это приводит к тому, что коэффициент прироста, рассчитываемый на основании непрерывной модели, оказывается выше, и, как следствие – начало отставания реального роста заболеваемости от экспоненциального (назовем его моментом А) опережает момент В – начало его же отставание от неограниченного роста, рассчитываемого при помощи дискретной модели.

В таблице 1 приведены результаты моделирования динамики числа зараженных на первом этапе пандемии по пяти странам. Статистические данные о количестве зараженных в этих странах были взяты из [5].

Таблица 1 – Результаты моделирования динамики численности зараженных

Страна	Коэффициент прироста k			Время между моментами А и В
	Линеаризация непрерывной модели	Дискретная модель	Уравнение Ферхюльста	
Китай	0,26	0,19	0,20	4 дня
Италия	0,24	0,18	0,15	3 дня
США	0,24	0,18	0,18	5 дней
Россия	0,20	0,15	0,16	10 дней
Швеция	0,18	0,10	0,11	9 дней

Различие в полученных этими двумя способами темпов прироста числа заболевших на первом этапе распространения вируса являются весьма существенными. Полагаю, что в рамках рассматриваемой проблемы аппроксимация динамики числа заболевших, исходя из минимизации абсолютных значений разницы

между наблюдаемым и теоретическим количествами зараженных, является более адекватной, поскольку речь идет не о некоей обобщенной или усредненной величине, а о соответствии между интегральными результатами отдельных случайных событий в модели и в реальности. Подтверждением этого является и близость значений коэффициента прироста по результатам моделирования второго этапа развития пандемии именно к коэффициентам, полученным при помощи дискретных моделей.

Таким образом, применение регрессии к линеаризованной модели в данном случае может привести к тому, что замедление распространения инфекции может быть зафиксировано преждевременно. Во избежание такой ошибки в данной задаче может быть либо применено дискретное моделирование, либо же нелинейная регрессия должна осуществляться путем минимизации расстояния между исходной функцией, к которой проводится регрессия и наблюдаемыми величинами.

Литература:

1. *Ильин С.* Коронавирусная инфекция: моделирование и прогноз // Коммерсантъ, 15.04.2020. – URL: https://www.kommersant.ru/doc/4322667 (дата обращения 18.05.2020).

2. *Томчин Д.А. Ситчихина М.С., Фрадков А.Л.* Прогнозирование распространения вируса covid-19 в россии на основе математической модели SIR / Национальная (Всероссийская) конференция по естественным и гуманитарным наукам «Наука СПбГУ – 2020». – Санкт-Петербург: СПбГУ, 2020. – С. 529-531.

3. *Куркина Е.С., Кольцова Е.М.* Математическое моделирование и прогнозирование распространения эпидемии коронавируса COVID-19 / Проектирование будущего. Проблемы цифровой реальности: труды 4-й Международной конференции (4-5 февраля 2021 г. Москва). – М.: ИПМ им. М.В.Келдыша, 2021. – С. 178-192. – URL: https://keldysh.ru/future/2021/17.pdf (дата обращения 18.09.2021).

4. *Verhulst P.F.* Recherches Mathématiques sur La Loi D'Accroissement de la Population // Nouveaux Mémoires de l'Académie

Royale des Sciences et Belles-Lettres de Bruxelles. – 1845. – 18, Art. 1. – P. 1-45.

5. Our World in Data. Statistics and Research. Coronavirus Pandemic (COVID-19). – URL: https://ourworldindata.org/coronavirus# (дата обращения 10.10.2021).

Гучук В.В.

Прикладная формализация корректировки экспертной кластеризации многопараметрических объектов

Аннотация: Рассматривается формализация процедуры корректировки экспертных оценок, используемой в качестве механизма повышения надежности и адекватности применения экспертных оценок. Интерактивная процедура основана на простейших предположениях о свойствах объектов, которые позволяют улучшать качество кластеризации по экспертным оценкам слабо формализуемых многопараметрических объектов.

Ключевые слова: экспертные оценки, кластеризация, объективизация, алгоритмизация, нечеткие множества, фаззификация, диндекс

Использование экспертных оценок актуально при разработке новых сложных научно-технических изделий, в медицинской диагностике, при анализе сложно-структурированных объектов, которые плохо поддаются полной или даже частичной формализации. Для повышения надежности этих оценок автором в [1] предлагается использовать процедуру, позволяющую на основе анализа измеряемых параметров улучшать качество экспертной кластеризации объектов – процедуру объективизация экспертных оценок. В качестве одного из механизмов дополнительной поддержки надежности и адекватности применения экспертных оценок может служить формализация таких процедур.

Сложность формализации процедуры объективизации экспертной кластеризации определяется, как правило, отсутствием математических моделей реальных объектов.

Для фаззификации (интерпретации содержания процедуры объективизации в терминах теории нечетких множеств [2]) $\{\vec{V}\}_i$ (множество векторов i-го класса) определим как нечеткое множество F_i, а именно как совокупность пар $F_i=\{(v,\mu_i(v))|v\in U\}$, где v – вектор, принадлежащий универсуму U, т.е. множеству всех векторов, $\mu_i(v)$: $U \rightarrow [0,1]$ – функция (степень) принадлежности вектора v к нечеткому множеству F_i (выше определенная как кластерный коэффициент принадлежности вектора к классу). В качестве порогового значения степени принадлежности обычно используют значение т.н. точки перехода нечеткого множества, а именно 0,5, которое можно использовать в качестве начального ориентира. Носителем нечеткого множества F_i будет подмножество $\widetilde{F}_i$ векторов, обладающих явными признаками класса, т.е. степень принадлежности $\mu_i(v)$ которых весьма высока.

Поскольку в нашем случае объективизация априори производится для достаточно представительных выборок, то высота нечеткого множества $\sup\limits_{F_i} \mu_i\ (v) = 1$, т. е. нечеткое множество F_i нормально. По этой же причине нечеткое множество F_i не унимодально, т.е. степень принадлежности (коэффициент принадлежности вектора к классу) достигает единичного значения как минимум для нескольких векторов. Фильтрация векторов с использованием максимальных пороговых значений $K^* = \alpha$ ($K^{**} = \alpha$) для коэффициентов принадлежности порождает α-срез нечеткого множества F_i, т.е. подмножество, называемое четким множеством $A_{i,\alpha}$ и определяемое характеристической функцией $\chi A_{i,\alpha}$, согласно формуле (1):

$$((\mu_i < \alpha) \rightarrow (\chi A_{i,\alpha}=0))\&((\mu_i \geq \alpha) \rightarrow (\chi A_{i,\alpha}=1)). \qquad (1)$$

Для α-срезов нечеткого множества F_i справедлива взаимная импликация $\alpha_1<\alpha_2 \leftrightarrow A_{i,\alpha 1} \supset \supset A_{i,\alpha 2}$, отражающая тот факт, что фильтрация векторов с использованием большего порогового значения порождает множества меньшей мощности чем фильтрация с меньшим пороговым значением.

Что касается такого важного понятия, как выпуклость множества, то к реальным экспериментальным данным в большинстве случаев оно не применимо. Следует сказать, что гипотетически в оценочном плане вышеупомянутое нечеткое

множество F_i может быть выпуклым из-за простоты построения границ множеств в пространстве измеряемых параметров. В дальнейшем нарушить условия выпуклости может переклассификация векторов, отнесенных экспертным оцениванием к F_i и лежащих внутри области F_i, но в результате объективизации включенных в другое множество.

Для уже объективизированной кластеризации можно применять и более развернутый инструментарий теории нечетких множеств, в частности, основанный на максиминных, алгебраических и ограниченных операциях, и использующий *t*-норму и *t*-конорму. Так, если для практических целей объединяются два нечетких множества, получается объединение множеств $F_i \vee F_j$ – наименьшее нечеткое множество $F_{i \cup j}$, содержащее одновременно F_i и F_j, для которого $\mu_{i \cup j}(v) = \max(\mu_i(v), \mu_j(v))$, т.е. в качестве ориентира берется наибольшая по величине степень принадлежности (кластерный коэффициент принадлежности) к первому (например, *i*-му) или второму (соответственно, *j*-му) классу. Для уточнения $\mu_{i \cup j}$ необходимо снова произвести в два подэтапа ранжирование векторов объединенного множества $F_{i \cup j}$. Если необходимо вычленить подмножество векторов, имеющих ненулевые степени принадлежности к двум нечетким множествам, определяется пересечение множеств $F_i \wedge F_j$ – наибольшее нечеткое множество $F_{i \cap j}$, содержащееся одновременно в F_i и F_j, для которого $\mu_{i \cap j}(v) = \min(\mu_i(v), \mu_j(v))$, т.е. в качестве степени принадлежности берется наименьшая по величине степень принадлежности (кластерный коэффициент принадлежности) к *i*-му или *j*-му классу.

Отметим, что алгоритм переклассификации использует более сложные конструкции, в частности, применяется логический анализ абсолютных значений степеней принадлежности и соотношения значений степеней принадлежности к разным классам одного и того же вектора. В результате такого логического анализа можно, в частности, произвести корректировку вышеупомянутого пересечения множеств $F_i \wedge F_j$.

При фаззификации еще не объективизированной экспертной кластеризации более релевантными являются нечеткие (размытые) оценки степени принадлежности. Это вызвано тем, что на этом этапе невозможно получить достаточно точные и окончательные оценки. В процессе объективизации состав множества F_i, а также

подмножества $\widetilde{F}_i$, может претерпеть существенные изменения, влияющие на параметрическое формирование степеней принадлежности. Дополнительно можно ввести понятие степени размытости оценок и понятие уверенности (надежности) этих оценок [3], или использовать вероятностные характеристики для степени принадлежности. Что касается нечеткой классификации, то это понятие в общепринятом понимании сложно применить к параметрической классификации, выполняемой с использованием алгоритмов распознавания (алгоритмов классификации). В определенном смысле задачу нечеткой классификации решает эксперт при субъективной оценке степени сходства вектора v с формируемым им же эталоном класса F_i, т.е. используя попарные сравнения и заранее не определенное число классов.

Задача нечеткого упорядочивания при данном подходе вообще не ставится – используется ранжирование векторов по вычисляемым кластерным коэффициентам принадлежности. Показатель размытости нечеткого множества, понимаемый как мера внутренней неопределенности, можно использовать и для характеристики компактности класса в параметрическом пространстве, и для оценки идентифицируемости векторов *i*-го класса в общей массе векторов. Вообще, аппарат теории нечетких множеств предназначен, прежде всего, для описания и анализа статической ситуации, когда имеется некоторое зафиксированное на определенный момент состояние анализируемых множеств и оценочного конгломерата.

Для полноценной формализации процедуры объективизации необходимо изначально вводить динамические конструкции. В качестве первого шага можно использовать введение такого понятия, как *неустоявшееся* множество (*динамическое* множество), которое в процессе своего развития меняет состав, мощность и т.п. Дополнительно к известной атрибутике здесь добавляется *диндекс* (динамический индекс) множества, для простоты имеющий дискретный характер, и отражающий шаг или итерацию в динамическом процессе корректировки множества, в данном случае итерацию в процедуре объективизации кластеризации многопараметрических объектов по экспертным оценкам.

При фиксации значения диндекса, т.е. при рассмотрении зафиксированного состояния на определенном этапе

объективизации, ситуация входит в общепринятое русло, для которого имеется развитый матаппарат. Известны прецеденты использования диндекса, например, в методах генетической оптимизации, развивающих идеи Дж. Холланда [2]. Его присутствие прослеживается также в концепции итеративных множеств [4], являющихся частным случаем неустоявшихся (динамических) множеств. Для описания и анализа процедуры объективизации в данном случае необходимо вводить такие понятия как обусловленность множества, вырождение множества, стабильность присутствия элементов на множестве и т.п. Возможно также использовать такую аналитику, как сходимость итеративных процедур, например, стремление мощности множества в процессе его корректировки к определенному значению, устойчивость множества относительно номенклатуры элементов и ряд других понятий. Естественным образом к неустоявшимся (динамическим) множествам, в контексте формализации процедуры объективизации, применима определенная часть инструментария теории множеств, а также аппарат нечетких множеств.

В заключение отметим, что работы по объективизации экспертных оценок проводились и ранее [5]. Процедуры разрабатывались для уточнения выставленных в ранговых шкалах экспертных оценок качества одной группы объектов. Объективизации экспертных оценок служат и стандартные, для экспертного оценивания, процедуры обработки оценок, например, привлечение достаточно большой группы экспертов, проведение отбора наиболее компетентных экспертов и т.п. Разработанная процедура объективизации была использована при создании алгоритмов медицинской диагностики по пульсовым сигналам на основе субъективной кластеризации формы пульсовых сигналов [6].

Литература:

1. *Guchuk V.V.* Application of algorithms of objectifying expert clustering of Multiparameter objects in the analysis of big arrays of information // Advances in Systems Science and Applications. – 2018. – № 1. – P. 102-109.

2. *Гэри В., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. – М.: Мир, 1982. – 416 с.

3. *Гучук В.В.* Технология объективизации экспертной кластеризации слабо формализуемых объектов // Вестник УГАТУ. – 2014. – №5. – С. 149-154.

4. *Maddy P.* Second philosophy: a naturalistic method. – Oxford: Oxford University Press, 2007. – 448 p.

5. *Kuznetsov M.P., Strijov V.V.* Methods of expert estimations concordance for integral quality estimation // Expert Systems with Applications. – 2014. – Vol. 4. – P. 1988-1996.

6. *Гучук В.В., Покровская И.В., Дорофеюк А.А., Десова А.А.* Интеллектуальный анализ квазипериодических биосигналов в задачах медицинской диагностики (на примере пульсового сигнала) // Автоматика и телемеханика. – 2018. – №11. – С. 3-15.

Хабибулин Р.Ш., Кадиев Ш.К.

Онтологический подход к выявлению проблем в области реагирования на чрезвычайные ситуации

Аннотация: Показана необходимость разработки и внедрения информационных моделей в предметную область реагирования на чрезвычайные ситуации (ЧС). Представлены функциональная модель деятельности центра управления в кризисных ситуациях (ЦУКС) при получении сообщения о ЧС и графическое изображение онтологической модели одноименной предметной области. Вместе с тем, отмечена необходимость разработки теоретической базы информационного моделирования процессов реагирования на ЧС с точки зрения определения необходимых сил и средств для их ликвидации.

Ключевые слова: онтологическая модель, чрезвычайная ситуация, функциональное моделирование, антикризисное управление, машинное обучение

Реагирование и ликвидация ЧС – это сложный, многозадачный процесс. Выбор из множества решений, сбор, накопление и хранение знаний опытных руководителей, оптимизация полученной информации, оперативное реагирование – лишь некоторые из большого числа задач лиц принимающих решения (ЛПР).

Тренд на цифровую трансформацию организационно-функциональных структур, направлен и на эффективное решение задач в области ликвидации ЧС.

Ликвидацию ЧС укрупненно можно поделить на 3 этапа:

1) реагирование на ЧС (получение и обработка сообщения о ЧС, отправка сил и средств пожарно-спасательных подразделений к месту вызова, межведомственное информационное взаимодействие);

2) ликвидация ЧС (проведение аварийно-спасательных и других неотложных работ);

3) ликвидация последствий и подведение итогов.

Таким образом, жизненный цикл ликвидации ЧС графически можно отобразить следующим образом (рисунок 1).

Рисунок 1 – Жизненный цикл ликвидации ЧС

Для формализации внутренних процессов на всех этапах жизненного цикла было предложено использование функциональной и семантической моделей. Предметная область исследования сосредоточена на этапе реагирования на ЧС. В этой сфере в работе [1] представлена функциональная модель стандарта *IDEF0* «Деятельность ЦУКС при получении сообщения о ЧС» (рисунок 2).

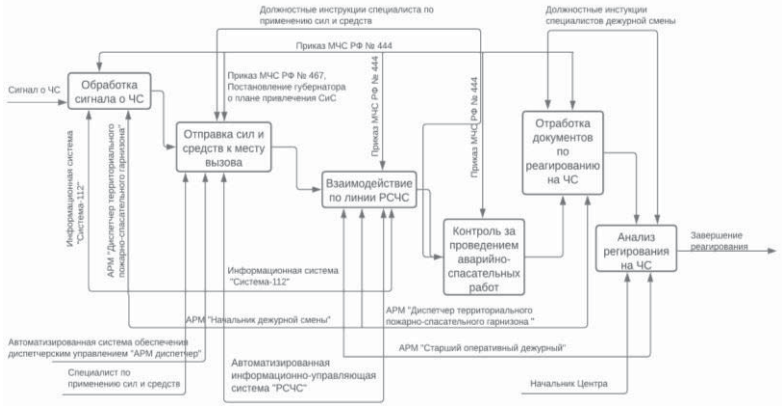


Рисунок 2 – Функциональная модель деятельности ЦУКС при получении сообщения о ЧС

Данная модель служит предварительным этапом к разработке онтологической модели предметной области, для этого из функциональной модели извлечены основные экземпляры, составлены классы для каждого экземпляра, обозначены свойства-связи для потока информации. В работах [2-4] представлены преимущества составления онтологий в инструментальной среде *Protégé (https://protege.stanford.edu/)*. Анализ публикаций показал, что составление онтологий в *Protege* соответствует основным требованиям:

– консистентность – требование не содержит конфликтов с другими требованиями

– полнота – требования не нуждаются в дальнейших пояснениях

– верифицируемость – требования можно проверить, чтобы доказать, что система удовлетворяет требованиям.

Для составления онтологии были заданы основные классы, к каждому классу были отнесены экземпляры модели (рисунок 3).

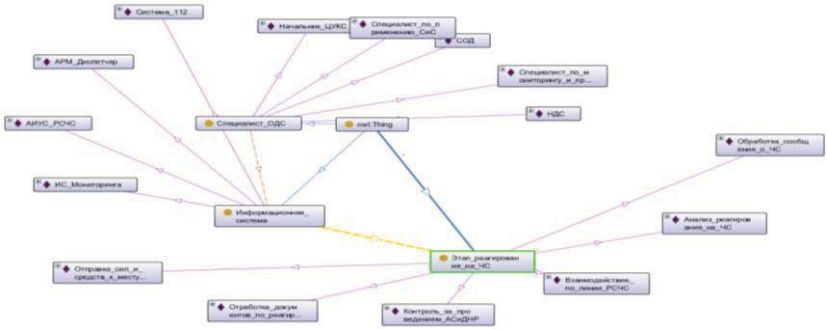


Рисунок 3 – Фрагмент онтологии в редакторе *Protege*

После определения экземпляров и классов, были составлены свойства-связи между экземплярами. Были заданы два свойства для всех типов экземпляров: *выполняет функцию, использует.*

Для отображения связей между классами «Специалист ОДС» (domains) и «Информационная система» (ranges) определено свойство *использует*, между классами «Информационная система» (domains) и «Этап реагирования на ЧС» (ranges) – *выполняет функцию.*

По итогам описания экземпляров и их классов, основных свойств-связей с помощью плагина *OntoGraf* представлена разработанная модель в графическом виде (рисунок 4).

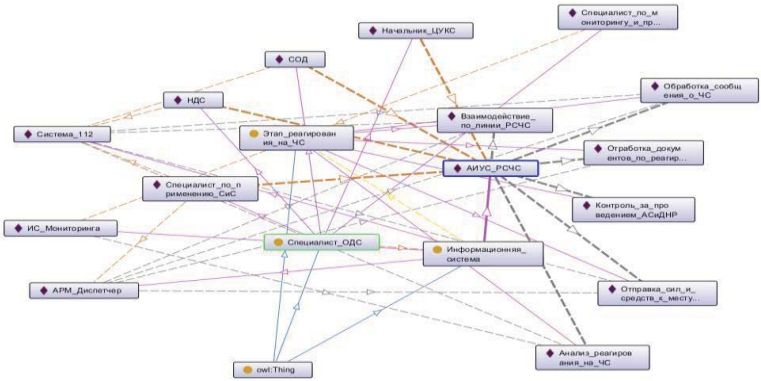


Рисунок 4 – Онтология предметной области

С помощью формализации процессов антикризисного управления в области реагирования на ЧС была выявлена проблема формализации определения сил и средств к месту вызова. Для решения этой проблемы планируется разработка специального программного обеспечения по классификации ЧС с использованием методов машинного обучения.

Литература:

1. *Кадиев Ш.К.* Функциональная модель деятельности центров управления в кризисных ситуациях при получении сообщения о ЧС / Материалы X-ой Международной научно-практической конференции молодых ученых и специалистов «Проблемы техносферной безопасности – 2021». – М.: Академия ГПС МЧС России, 2021. – С. 219-223.

2. *Муртазина М.Ш., Авдеенко Т.В.* Выявление конфликтов в спецификации требований на основе онтологической модели и системы продукционных правил / Информационные технологии и нанотехнологии (ИТНТ): V междунар. конф. и молодеж. шк. – Самара: Новая техника, 2019. – С. 592-600.

3. *Муртазина М.Ш., Авдеенко Т.В.* Онтологический подход к поддержке процесса инженерии требований в Scrum / Сборник трудов IV международной конференции и молодежной школы «Информационные технологии и нанотехнологии» (ИТНТ-2018). – Самара: Новая техника, 2018. – С. 2610-2620.

4. *Атнабаева А.Р., Вагапова З.Н.* Аналитическая поддержка принятия решений при управлении рисками как инструмент эффективного использования человеческих знаний // Известия Самарского научного центра Российской академии наук. – 2019. – Т. 21. №. 5. – С. 130-135.

Фомичев А.Н.

Методика расчета экономического ущерба от распространения наркомании

Аннотация: В работе предложена методика количественной оценки экономического ущерба от распространения наркомании и обоснована необходимость

применения указанной методики в современных социально-экономических условиях.

Ключевые слова: экономический ущерб, наркомания, криминогенные дисфункции

В современных условиях на специфику развития российской экономики все большее влияние оказывают так называемые криминогенные дисфункции.

Под криминогенными дисфункциями в наиболее общем виде можно понимать дисфункции, возникновение которых обусловлено противоправной деятельностью недобросовестных юридических лиц и граждан.

Уровень криминогенных дисфункций в первую очередь зависит от степени криминализации общества.

Степень криминализации региона может характеризоваться различными показателями, основными из которых являются: уровень преступности, раскрываемость выявляемых преступлений, доля населения, склонного к осуществлению противоправной деятельности, уровень наркотизации населения и др.

Уровень преступности определяется как отношение количества преступлений, зарегистрированных на территории конкретного региона в отчетном периоде, к общей численности населения данного региона. Как правило, уровень преступности отражает количество совершенных в отчетном периоде преступлений, приходящихся на каждые на 100 тыс. чел. населения региона.

Для расчета уровня преступности используется следующая формула

$$Упрест = Кпрест / Чнасел \quad (1)$$

где Упрест – уровень преступности;

Кпрест – количество преступлений, выявленных на территории региона в течение отчетного периода;

Чнасел – численность населения региона.

С показателем уровня преступности тесным образом связана раскрываемость, которая характеризует долю раскрытых преступлений в общем количестве выявленных преступлений на территории конкретного региона в течение отчетного периода.

Раскрываемость преступлений рассчитывается по следующей формуле

$$Рпрест = Кпрест.раск / Кпрест.выявл \quad (2)$$

где Рпрест – раскрываемость преступлений;

Кпрест. выявл – количество преступлений, выявленных на территории региона в течение отчетного периода;

Кпрест.раск – количество преступлений, раскрытых на территории региона в течение отчетного периода.

Доля населения, склонного к осуществлению противоправной деятельности, исчисляется в процентах к общей численности населения изучаемого региона и включает в себя лиц, ранее привлекавшихся к уголовной ответственности либо ведущих асоциальный образ жизни.

Для расчета указанного параметра используется следующая формула

$$Нпрот = Чпрот/Чнасел \quad (3)$$

где Нпрот – доля населения, склонного к осуществлению противоправной деятельности;

Чпрот – численность населения, склонного к осуществлению противоправной деятельности;

Чнасел – численность населения региона.

Уровень наркотизации населения определяется как отношение числа лиц, допускающих немедицинское потребление наркотических средств и психотропных веществ, к общей численности населения

$$Унарк = Чнарк/Чнасел \quad (4)$$

где Унарк – уровень наркотизации населения;

Чнарк – число лиц, допускающих немедицинское потребление наркотических средств и психотропных веществ;

Чнасел – численность населения региона.

Наиболее важную роль в системе управления криминогенными рисками играет определение экономического ущерба, наносимого в результате противоправной деятельности.

Определение ущерба, наносимого преступлениями экономического характера, как правило, проблем не вызывает и рассчитывается, исходя из общей стоимости похищенного или выведенного из строя имущества, размера неполученных доходов, суммы неуплаченных налогов, пошлин и сборов.

Более подробно целесообразно остановиться на экономическом ущербе от преступлений, носящих асоциальный характер, например, от преступлений, связанных с незаконным оборотом наркотиков.

Наркотизация населения и распространение наркомании являются одной из основных проблем, стоящих перед нашей страной и мировым сообществом в целом. Увеличение объемов незаконного оборота наркотиков и большое число числа наркозависимых лиц не только подрывают здоровье нации, вызывают резкое обострение криминогенной обстановки, создают предпосылки для дестабилизации социальной, демографической и политической ситуации, но и негативным образом сказываются на динамике развития национальной экономики.

Оценку ущерба от распространения наркомании представляется целесообразным производить на основе стоимостной оценки. Данный показатель можно определить по двум основным сферам: демографической и бюджетно-финансовой.

1. Ущерб в демографической сфере как сумма ущерба от смертности в результате потребления наркотических средств и психотропных веществ и ущерба от заболеваемости наркоманией.

Ущерб от смертности в результате потребления наркотических средств и психотропных веществ можно рассчитать по следующей формуле

$$Усм = Чум.нарк \times Сжиз \quad (5)$$

где Чум.нарк – число умерших от потребления наркотиков, чел.;

Сжиз – стоимость человеческой жизни, руб./чел.

Для определения стоимости человеческой жизни предлагается использовать следующую формулу

$$Сжиз = ВРПср.душ/(Креф/100) \quad (6)$$

где ВРПср.душ – среднедушевой валовый региональный продукт города К.;

Креф – ставка рефинансирования Центрального банка РФ (13%).

Ущерб от заболеваемости наркоманией можно определить по следующей формуле

$$Узаб = Члеч.нарк \bullet Слеч \quad (7)$$

где Члеч. нарк – число наркозависимых, проходивших лечение в государственных медицинских учреждениях, чел.;

Слеч – средняя стоимость лечения одного больного наркоманией, тыс. руб./чел.

2. Ущерб от распространения наркомании в бюджетно-финансовой сфере (Уф.б) складывается из четырех основных составляющих:

1) ущерб от расходования бюджетных средств на борьбу с наркоманией (Зб.н);

2) ущерб от содержания заключенных, осужденных за преступления, связанные с незаконным оборотом наркотиков (Зн.п);

3) ущерб от содержания заключенных, которые на момент совершения преступления являлись наркозависимыми (Зн.з);

4) ущерб от расходования бюджетных средств на содержание аппарата по профилактике и борьбе с распространением наркотиков (Зн.к).

$$Уф.б = Зб.н + Зн.п + Зн.з + Зн.к \quad (8)$$

7

Последующий сравнительный анализ рассмотренных выше показателей применительно к различным регионам страны позволяет выявлять территории с более или менее острой криминогенной обстановкой, что может иметь существенное значение при принятии управленческих решений, касающихся размещения долгосрочных капиталовложений или открытия дочерних предприятий в ходе диверсификации бизнеса.

Литература:

1. Уголовный кодекс Российской Федерации. – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 30.09.2021).

2. *Фомичев А.Н.* Оптимизация методики управления криминогенными дисфункциями // Вестник Екатерининского института. – 2016. – № 2(34). – С. 93-97.

3. *Фомичев А.Н.* Разработка методики количественной оценки уровня криминогенных дисфункций // Вестник Екатерининского института. – 2013. – № 2(22). – С. 85-89.

4. *Фомичев А.Н.* Наркомания: экономический ущерб региона в цифрах // Российское предпринимательство. – 2011. – № 2(2). – С. 181-184.

5. Министерство внутренних дел Российской Федерации. – URL: http://мвд.рф/ (дата обращения 30.09.2021).

Гончар Д.Р.

Балансировка вычислительной нагрузки при параллельной реализации решения минимаксной задачи составления расписания методом ветвей и границ

Аннотация: Рассматривается минимаксная задача построения расписания наименьшей длины без прерываний для многопроцессорной системы. Для решения данной задачи предложен параллельный алгоритм на основе метода ветвей и границ. Исследуются возможности повышения скорости расчетов при балансировке загрузки используемых процессоров.

Ключевые слова: многопроцессорная система, работы без прерываний, расписание наименьшей длины

Введение

Задачи по построению оптимальных расписаний часто встречаются при планировании производства, управлении энергетикой, подготовке и проведении испытаний сложных технических систем, работе различных систем экологического, медицинского, промышленного мониторинга и в ряде других случаях. Одним из способов ускорения расчетов при решении подобных задач является разработка параллельных алгоритмов планирования. Для алгоритмов на основе метода ветвей и границ этот вопрос весьма актуален в связи с достаточно высокой вычислительной сложностью метода.

В данной работе приведено как описание самого алгоритма, так и подходы к балансированию вычислительной нагрузки при расчетах с использованием разного числа процессоров на Межведомственном суперкомпьютерном центре РАН.

1. Постановка задачи

Пусть имеется множество работ $N = \{1, 2, \ldots, n\}$, которое необходимо выполнить с помощью m процессоров, составляющих вычислительную систему для их обработки. Длительность выполнения работы i на процессоре j равно t_{ij} ($i = 1, 2, \ldots, n$; $j = 1, 2, \ldots, m$). В каждый момент времени каждая работа может выполняться не более чем одним процессором, а каждый процессор может выполнять не более одной работы. Переключения с одного процессора на другой и прерывания при выполнении работ не допускаются.

Расписание выполнения работ N определим как разбиение множества N на m непересекающихся подмножеств $N_1, N_2, \ldots, N_m$ ($N = \bigcup_{j=1}^{m} N_j$; $N_{j_1} \bigcap N_{j_2} = \varnothing$ при $j_1 \neq j_2$). Работы из множества N_j приписываются процессору j и выполняются на нем одна за другой в произвольном порядке. Под загруженностью процессора j ($j = 1, 2, \ldots, m$) будем понимать величину $Q_j = \sum_{i \in N_j} t_{ij}$, а $\max_{j=1, 2, \ldots, m} Q_j$ – это длина расписания. Задача заключается в построении оптимального по быстродействию расписания, т.е. расписания минимальной длины.

При решении подобных задач применяются методы случайного и исчерпывающего поиска, методы математического программирования [1], метод ветвей и границ [2], муравьиные алгоритмы, поиск с запретами, вероятностные алгоритмы, генетические алгоритмы [3], метод имитации отжига, различные эвристические алгоритмы [4, 5], алгоритмы агрегирования и др.

2. Метод ветвей и границ

Для решения вышеприведенной задачи предлагается метод ветвей и границ, основанный на результатах работы [2]. Этот метод подразумевает последовательное разбиение исходного множества решений на подмножества (ветви дерева решений) и применение оценочных процедур для определения перспективности исследования очередной ветви дерева решений. На каждом следующем шаге новые подмножества образуются в итоге разбиения некоторых подмножеств, полученных на предыдущих

шагах, пока для подмножеств, соответствующих концевым вершинам дерева, решение задачи уже не требует разбиения.

В итоге указанного разбиения мы получаем множество подзадач, которые могут обрабатываться совмещено по времени.

2.1. Дерево решений

Опишем множество всех расписаний (их число равно m^n) в виде дерева решений. Корень дерева находится на нулевом уровне и соответствует множеству всех расписаний. На первом уровне находится m вершин, каждая из которых соответствует множеству всех расписаний, в которых первая работа назначена на определенный процессор. На втором уровне дерева находится m^2 вершин, каждая из которых соответствует множеству всех расписаний, в которых первые две работы назначены на один или два определенных процессора. На n-м уровне дерева расписаний находится m^n листьев, каждый из которых соответствует некоторому расписанию выполнения множества работ N.

Пусть x_k – некоторый узел уровня k дерева расписаний, $R(x_k)$ – множество всех расписаний, соответствующих этому узлу (т.е. множество расписаний, в которых работы 1, 2, …, k назначены на определенные процессоры), x_{k+1}^j – узел уровня $k+1$ ($k < n$), связанный с узлом x_k ребром, соответствующим процессору j. Наша цель – вычисление нижней и верхней оценок минимальной длины расписания на множестве $R(x_k)$. Имея эти оценки, можно применить стандартную схему метода ветвей и границ [2].

2.2. Вычисление нижней оценки

Пусть T_j (j = 1, …, m) – загруженность процессора j после назначения первых k работ (т.е. T_j – это суммарная длительность работ из числа 1, 2, …, k, назначенных на процессор j). Нижнюю оценку $L(x_k)$ минимальной длины расписания на множестве $R(x_k)$ будем вычислять следующим образом:

$L(x_k) = \max(L_1(x_k), L_2(x_k), L_3(x_k))$, где $L_1(x_k)$, $L_2(x_k)$, $L_3(x_k)$ – это нижние оценки, вычисленные тремя различными способами.

Величина $L_1(x_k)$ вычисляется как следующий максимум: $L_1(x_k) = \max\limits_{j=1,2,...,m} T_j$. При хранении величины T_1, T_2, …, T_m в виде обычного массива сложность вычисления $L_1(x_k)$ составляет $\theta(m)$.

Величина $L_2(x_k)$ вычисляется как следующий максимум:

$$L_2(x_k) = \max_{i=k+1,\ldots,n} \min_{j=1,\ldots,m} (T_j + t_{ij}) \quad (1)$$

При использовании для этого двумерного массива A с элементами $a_{ij} = T_j + t_{ij}$, $i = k+1, \ldots, n$; $j = 1, 2, \ldots, m$ сложность вычисления величины $L_2(x_k)$ составляет $\theta(mn)$.

Величина $L_3(x_k)$ вычисляется по формуле

$$L_3(x_k) = \frac{1}{m}\left(\sum_{j=1}^{m} T_j + \sum_{i=k+1}^{n} \min_{j=1,\ldots,m} t_{ij}\right) \quad (2)$$

Величину $\min\limits_{j=1,\ldots,m} t_{ij}$ вычислим для всех $i = 1, 2, \ldots, n$ сразу до начала вычисления нижних оценок. Тогда сложность вычисления величины $L_3(x_k)$ составляет $O(n + m)$. Перейдем в дереве расписаний от узла x_k к узлу $x_{k+1}^{j_0}$, $k < n$ (т.е. будем считать, что работа $k+1$ назначена на процессор j_0).

Тогда

$$L_3(x_{k+1}^{j_0}) = \frac{1}{m}\left(\sum_{j=1}^{m} T_j + t_{k+1,j_0} + \sum_{i=k+1}^{n} \min_{j=1,\ldots,m} t_{ij}\right) \quad (3)$$

Вычислим разность

$$L_3(x_{k+1}^{j_0}) - L_3(x_k) = \frac{1}{m}\left(t_{k+1,j_0} - \min_{j=1,\ldots,m} t_{k+1,j}\right) \quad (4)$$

Таким образом,

$$L_3(x_{k+1}^{j_0}) = L_3(x_k) + \frac{1}{m}\left(t_{k+1,j_0} - \min_{j=1,\ldots,m} t_{k+1,j}\right) \quad (5)$$

и с помощью данного рекуррентного соотношения, используя $L_3(x_k)$, величина $L_3(x_{k+1}^{j_0})$ вычисляется за время $O(1)$.

2.3. Вычисление верхней оценки

В качестве верхней оценки $H(x_k)$ минимальной длины расписания на множестве $R(x_k)$ возьмем длину расписания, в котором работы 1, 2, …, k в соответствии с вершиной x_k дерева расписаний распределены на процессоры, а работы $k+1, \ldots, n$ распределяются по следующему «жадному» алгоритму. Пусть уже

распределены работы 1, 2, …, p ($k \le p < n$), T_j – загруженность процессора j ($j = 1, 2, \ldots, m$) и $\min(T_1 + t_{p+1,1}, \ldots, T_m + t_{p+1,m}) = T_{j_0} + t_{p+1,j_0}$. Тогда работа p+1 назначается на процессор j_0.

Указанные действия повторяются для $p = k, k + 1, \ldots, n - 1$. Сложность процедуры вычисления величины $H(x_k)$ равна $O(mn)$.

2.4. Ветвление

Последовательное разбиение множества допустимых решений на подмножества происходит следующим образом: на каждом последующем шаге новые подмножества получаются в результате разбиения некоторых подмножеств, полученных на предыдущих шагах. Так образуется выше упоминавшееся дерево решения исходной задачи. Такое разбиение продолжается до тех пор, пока для подмножеств, соответствующих концевым вершинам дерева, решение задачи уже не требует разбиения.

В итоге разбиения начальная задача распадается на ряд подзадач, которые могут решаться в заметной степени вне зависимости друг от друга.

При этом представляется целесообразным поддерживать определенные связи между порожденными подзадачами, что связано с тем, что дерево решения может оказаться не вполне хорошо уравновешенным, что приводит к тому, что какая-то часть процессоров вычислительной системы оказывается загруженными неравномерно. Другая причина в том, что возникающие при попытке уравновешивания нагрузки зависимости по данным между подзадачами, связанные с передачей оценок, наилучших значений оптимизируемого функционала и других подобных сведений, могут приводить к большим накладным расходам на взаимодействие процессов, препятствующих повышению параллельной эффективности.

Для преодоления перечисленных причин снижения эффективности распараллеливания решения задачи применяется распределение обменов по вычислительному пространству, методы оптимизации загрузки процессов и минимизации обменов данными [6, 7].

Для реализации метода ветвей и границ в данной работе автором был выбран вариант метода назначаемых деревьев.

Литература:

1. *Алексеев О.Г.* Комплексное применение методов дискретной оптимизации. – М.: Наука, 1987. – 248 с.

2. *Фуругян М.Г.* Некоторые алгоритмы решения минимаксной задачи составления многопроцессорного расписания // Известия Российской академии наук. Теория и системы управления. – 2014. – № 2. – С. 50-56.

3. *Костенко В.А., Смелянский Р.Л., Трекин А.Г.* Синтез структур вычислительных систем реального времени с использованием генетических алгоритмов // Программирование. – 2000. – № 5. – С. 63-72.

4. *Brucker P.* Scheduling Algorithms. – Heidelberg: Springer, 2001. – 365 p.

5. *Гончар Д.Р.* Параллельная реализация мультиоценочного алгоритма составления многопроцессорного расписания без прерываний // Некоторые алгоритмы планирования вычислений и методы многокритериальной оптимизации для многопроцессорных систем. – М.: ВЦ РАН, 2014. – С. 21-31.

6. *Тимошевская Н.Е.* Параллельные методы обхода дерева // Математическое моделирование. – 2004. – Т. 16. № 1. – С. 105-114.

7. *Посыпкин М.А., Сигал И.Х., Галимьянова Н.Н.* Алгоритмы параллельных вычислений для решения некоторых классов задач дискретной оптимизации. – М.: ВЦ РАН, 2005. – 43 с.

Волгина О.А.

Выборочный анализ методов обработки качественной информации в количественном прогнозе

Аннотация: В работе рассматриваются выборочные методы использования качественной информации для решения широкого круга задач долгосрочного прогнозирования и анализа. Описываются свойства качественных характеристик, позволяющие им эффективно дополнять количественные методы. Особое внимание обращается на способы выделения и подготовки данных к машинной обработке.

Ключевые слова: долгосрочное прогнозирование, количественные и качественные параметры, экспертная оценка

При формировании долгосрочного прогноза основная проблема, которую сложно решить, заключается в том, что все доступные данные обычно относятся к прошлому или настоящему, а точной и надежной информации для прогнозирования не хватает. Наблюдается следующая особенность: чем больше горизонт прогноза, тем объем информации о будущем состоянии не только уменьшается, но и изменяется его структура. При изменении интервалов между точками формирования количественные методы теряют свою эффективность. Таким образом, если вся информация будет представлена в количественном виде, прогнозирование не будет иметь никакой ценности. Повышение качества долгосрочного прогноза возможно только за счет комбинации качественных и количественных методов.

Характеристики, на основе которых производятся прогнозы в основном, описываются разными «языками»: как правило, для количественных характеристик мы используем обычные числа, которые называются физическими величинами характеристики; для качественных это слова естественного язык, которые называются лингвистическими ценностями. Лингвистические значения могут быть определены также для количественных характеристик; однако для качественных характеристик физические величины не могут быть определены.

На данный момент самым распространенным методом качественного прогнозирования является экспертные оценки. Экспертное заключение часто необходимо при прогнозировании задач из-за отсутствия соответствующей или доступной информация для использования статистических процедур.

Во многих практических приложениях прогнозированию статистические методы могут оказаться неприменимыми, а экспертная оценка, как метод качественного анализа, может служить единственной основой для прогноза [1].

По сравнению с другими методами прогнозирования, у экспертных систем есть разумные перспективы для распространения, но некоторые препятствия очевидны. Психологические риски создают препятствия для экспертных

систем из-за неразрешимых проблем с верификацией результатов. Поскольку проблемы со сложностью заслуживают внимания, первоначальные попытки создания экспертных систем были простыми, даже если это влекло за собой некоторую потерю предсказательной способности [2].

В статье [3] исследуется использование экспертных систем и искусственного интеллекта (в частности, применение нейронных сетей) к прогнозированию недвижимости. В результате авторы пришли к выводу, что более сложные методы не могут дать лучшего результата простых. В статье описывается использование искуственной нейронной сети самого простого уровня. Нейронная сеть используется как вспомогательный элемент для экспертов.

Для проведения качественного анализа после выбора массива статей (документов) требуется предварительная обработка текстовых данных. Цель состоит в том, чтобы извлечь соответствующую информацию из набора новостей и подготовить ее к машинному обучению. Слова и фразы, которые сигнализируют об изменение цены необходимо верно извлечь.

В [4] предложено разделить текстовую предварительную обработку в три основных этапа: извлечение, выбор и представление функций. Шаг извлечения признаков относится к процессу создания списка признаков, которые являются словами или фразами, извлеченными из документов, в достаточной степени описывающие документы.

Это можно сделать разными способами. Метод семантического анализа «мешок слов» самый популярный [5]. Каждый документ или текст выглядит как неупорядоченный набор слов без сведений о связях между ними. Его можно представить в виде матрицы, каждая строка в которой соответствует отдельному документу или тексту, а каждый столбец – определенному слову. Ячейка на пересечении строки и столбца содержит количество вхождений слова в соответствующий документ, либо иное значение, связанное с «весом» – важностью конкретного термина в конкретном документе. Далее семантически пустые термины удаляются, а методы определения корней слов применяются к каждому слову для обработки различных формы слова как единого признака. Документы часто делятся на две (отрицательные и положительные)

или три (отрицательная, нейтральная и положительная) категории, классы в зависимости от их содержания.

Некоторые исследователи используют метод выявления событий на основе заранее составленных терминов предметной области. В статье [6] прогнозируют фондовые рынки, используя информацию, содержащуюся в статьях, опубликованных в Интернете. В качестве исходных данных используются в основном текстовые статьи, появляющиеся в ведущих и наиболее влиятельных финансовых газетах. Текстовые заявления содержат не только эффект (например, падение акций), но и возможные причины события (например, падение запасов из-за ослабления доллара и, как следствие, ослабления казначейских облигаций). Таким образом, использование текстовой информации повышает качество вводимых данных, из которых выбираются значимые позиции.

Еще одним эффективным методом является использование статистической информации в виде частоты упоминаний. В статье [4] показано, как текст из новостных статей может быть использован для прогнозирования внутридневных движений цен финансовых активов с использованием машин опорных векторов. Авторы используют частотный новостной анализ для создания блока данных, используемых впоследствии как основу прогнозирования. Полученные данные показывают, что отслеживание частоты упоминания информации в пресс-релизах может предоставить дополнительную информацию, которая может быть использована для прогнозирования тенденций цен на акции.

После завершения этапов предварительной обработки текста статьи выравниваются по цене и времени, и готовы в машинной обработке.

Таким образом, методы количественного прогнозирования хорошо показывают результат на задаче краткосрочного прогноза, но для среднесрочного и долгосрочного прогнозирования параметров не дают должного результата. При формировании такого рода прогноза необходимо также проводить анализ качественной информации по теме. Существует несколько методов извлечения информации из текстов и документов, подготавливающие данные для машинной обработки. Выбор метода

во многом зависит от стиля представления информации и прогнозируемой величины.

Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011

Литература:

1. *Rowe G., Wright G.* Expert opinions in forecasting: the role of the Delphi technique / Principles of forecasting. – Springer: Boston, MA, 2001. – P. 125-144.

2. *Armstrong J.S., Yokum J.T.* Potential diffusion of expert systems in forecasting // Technological Forecasting and Social Change. – 2001. – Volume 67. Issue 1. – P. 93-103.

3. *Rossini P.* Using expert systems and artificial intelligence for real estate forecasting / Sixth Annual Pacific-Rim Real Estate Society Conference (24-27 January 2000 Sydney, Australia). – URL: https://www.researchgate.net/publication/255480942_Using_Expert_Systems_and_Artificial_Intelligence_For_Real_Estate_Forecasting (дата обращения 10.10.2021).

4. *Mittermayer M.A.* Forecasting intraday stock price trends with text mining techniques / 37th Annual Hawaii International Conference on System Sciences (5-8 January 2004 Big Island, HI, USA). – URL: https://ieeexplore.ieee.org/document/1265201 (дата обращения 10.10.2021).

5. *San Kim T., Sohn S.Y.* Machine-learning-based deep semantic analysis approach for forecasting new technology convergence // Technological Forecasting and Social Change. – 2020. – Volume 157. – P. 120095.

6. *B. Wüthrich, D. Permunetilleke, S. Leung, V. Cho, J. Zhang, W. Lam*. Daily prediction of major stock indices from textual www data // Hkie transactions. – 1998. – Volume 5. Issue 3. – P. 151-156.

VII. Автоматизированные системы и средства обеспечения безопасности сложных систем

Сиротюк В.О., Богатырева Л.В., Потапова О.А.

Построение системы защиты цифровых фондов интеллектуальной собственности

Аннотация: В работе рассмотрены особенности формирования и использования цифровых информационных фондов интеллектуальной собственности (ЦФИС). Рассмотрены требования к базам данных (БД) интеллектуальной собственности и ЦФИС. Предложены постановка задачи, формализованные модели и методы построения оптимальных по различным критериям эффективности систем защиты БД ЦФИС от несанкционированного доступа. Предложенные модели и методы использовались при разработке системы управления информационной безопасностью БД евразийского патентно-информационного пространства.

Ключевые слова: база данных интеллектуальной собственности, цифровой информационный фонд интеллектуальной собственности, конфиденциальность данных, неизменность данных, доступность данных, система защиты данных

Введение

Системы управления интеллектуальной собственностью (ИС) играют важную роль при проведении хозяйствующими субъектами патентных и научных исследований с целью принятия обоснованных решений в различных областях науки и техники. Используемая при этом патентная и научно-техническая информация обладает значительными преимуществами перед другими видами информации [1].

В совокупности информационные фонды ИС, хранимые в соответствующих базах данных интеллектуальной собственности (БД ИС), информационные технологии сбора, хранения, обработки и передачи данных, информационно-телекоммуникационные и сетевые инфраструктуры образуют цифровой фонд интеллектуальной собственности (ЦФИС), который формируется для эффективного выполнения научно-исследовательскими институтами, организациями и предприятиями различных отраслей экономики поставленных перед ними задач.

Формирование, хранение и развитие данных ЦФИС включает операции, связанные с получением документов, комплектованием и организацией хранения документов фондов, переводом их в цифровую форму и загрузкой в БД ИС, представленных БД патентной информации (ПБД) и БД научно-технической информации (БД НТИ) [1,2].

Создание БД ИС по материалам первоисточников является весьма мощным средством активизации национальных информационных ресурсов за счет перевода значительной их части в цифровую форму и последующего многоаспектного использования в процессе исследований и разработок.

Современный ЦФИС имеет распределенную информационно-управляющую структуру и предоставляет доступ к локальным и внешним удаленным ПБД и БД НТИ, поиск информации и ее использование через единый пользовательский интерфейс [1,2]. Это обусловливает необходимость логической интеграции (или консолидации) данных локальных и внешних ПБД и БД НТИ.

Большие объемы хранимой в БД ИС информации, относимых к классу сверхбольших баз данных (VLDB), обусловливают необходимость не только разработки методов и средств оптимизации их проектирования, организации и использования, но и создания эффективных методов, средств и технологий защиты БД, информационной и обеспечивающей инфраструктуры ЦФИС [1,3].

В работе рассмотрены требования к БД ИС и ЦФИС, предложены формализованные модели и методы построения оптимальных по различным критериям эффективности систем защиты данных ЦФИС от преднамеренного или непреднамеренного несанкционированного доступа, модификации или разрушения данных.

Требования к БД ИС, обеспечивающей и информационной инфраструктуре ЦФИС

ПБД и БД НТИ (БД ИС) ЦФИС хранят информацию о патентных документах и научно-технической литературе. 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 [1-3]. Сложность их создания и эксплуатации увеличиваются в связи с тем, что в них загружаются и хранятся очень большие объемы информации (от сотен гигабайт до десятков терабайт). Эти особенности обусловливают повышенные требования к качеству и безопасности информационной и обеспечивающей инфраструктуры ЦФИС.

Оценка эффективности построения ЦФИС проводится с использованием критериев максимума обеспечиваемых уровней полноты, достоверности, гарантированной защиты ПБД и БД НТИ от несанкционированного доступа, непреднамеренных искажений, разрушения и других неблагоприятных факторов.

С учетом распределенной структуры доступа к данным ЦФИС представляется в виде виртуального информационного хранилища. Инфраструктура ЦФИС должна удовлетворять следующим основным требованиям:

1. Обеспечивать защиту данных БД ИС от несанкционированного доступа, преднамеренного или непреднамеренного искажения, разрушения и модификации информации.

2. Обеспечивать доступность данных по схеме 24часа*365дней.

3. Для обеспечения высокого уровня сохранности данных ПБД и БД НТИ должны обладать свойством «самообслуживания», предполагающим возможность самостоятельного восстановления работоспособности БД. Например, технологии ORACLE обеспечивают такую возможность на основе концепции создания т.н. автономных БД [4].

4. Предоставлять удобный интерфейс доступа к локальным и внешним удаленным ПБД и БД НТИ, базирующийся на принципе «одного окна» и средств метапоиска [1,2].

5. Серверное оборудование ЦФИС должно быть легко масштабируемым по объему хранимой информации. Подключение

дополнительных модулей хранения, расширяющих объем хранилища, должно осуществляться автоматически, и при этом должна обеспечиваться интеграция с существующими компонентами хранилища без перестройки уже развернутого информационного хранилища.

6. Обладать современными средствами поддержания готовности данных, обеспечивающими полное резервирование, упреждающий мониторинг, обнаружение и исправление ошибок.

7. Обладать развитой системой диагностики и автоматического информирования о произошедших неполадках.

С учетом сформулированных требований ЦФИС в современных условиях должен создаваться на основе специализированной системы аппаратно и программно конфигурируемой и масштабируемой платформы хранения, например, на основе платформы Oracle Exadata Cloud&Customer [4].

Формализованные методы построения оптимальной системы защиты данных ЦФИС

Как известно, множество существующих методов защиты данных БД включают в себя организационные, процедурные, структурные, аппаратные и программные методы [3,5].

Организационные методы защиты используются для ограничения числа лиц, которые получают право доступа в помещение центра обработки данных (ЦОД).

Процедурные методы защиты делают возможным доступ к данным и передачу их только тем пользователям, которые имеют соответствующие разрешения.

Структурные методы защиты применяются на этапах проектирования структур БД (канонической, логической и физической) и системы защиты данных ЦФИС. Они должны обеспечивать такую структуризацию и организацию данных, которая позволяет повысить уровень защищенности хранимых данных.

Аппаратные средства защиты информации представляют собой различные электронные устройства, встраиваемые в состав технических средств вычислительной системы или сопрягаемые с ними с помощью стандартного интерфейса.

Программные методы защиты реализуются путем включения специализированных программных средств в состав используемых операционных систем и СУБД, либо выделения их в самостоятельные приложения, которые инициируются перед началом процесса обслуживания запросов пользователей.

Различные методы защиты информации характеризуются определенными технико-экономическими показателями, к которым относятся затраты на их разработку и эксплуатацию, безопасное время раскрытия методов защиты и др. [3,5].

Рассмотрим постановку задачи и модели синтеза оптимальной системы защиты данных ЦФИС [3,5].

При синтезе системы защиты данных ЦФИС требуется сформировать структуры файлов БД ИС и их распределение между устройствами памяти, выбрать варианты взаимодействия пользователей с ЦФИС при которых обеспечивался бы заданный критерий эффективности функционирования системы защиты, возможность выполнения ею функций защиты информационных ресурсов ПБД и БД НТИ в условиях заданных ограничений.

Синтез оптимальной системы защиты ЦФИС включает решение следующих задач:

1. Формирование структуры файлов БД ИС с учетом степеней секретности логических записей и характеристик запросов.
2. Распределение файлов БД ИС между устройствами памяти.
3. Выбор варианта закрепления пользователей за терминалами.
4. Выбор варианта сопряжения терминалов с устройствами памяти.
5. Распределение методов защиты между объектами защиты.

Исходной информацией при решении задач синтеза оптимальной системы защиты БД ИС являются описания механизмов защиты канонической и логической структур ПБД и БД НТИ, представляемые отображениями $\{(u_k, db_i, as_j)\} \xrightarrow{\theta} \{0,1\}$, где «1» соответствует правомочности доступа пользователя $u_k \in U$ к элементам (объектам, данным) БД $db_i \in DB$ и/или приложениям $as_j \in AS$, а «0» – запрету на такой доступ [3].

Формально механизмы защиты канонической и логической структуры *v–й* БД ИС $M(G_к)$ и $M(G_л)$ описываются, соответственно,

матрицами смежности канонической структуры *v-й* БД ИС $W_v = \left\| w^v_{\varepsilon\varepsilon'} \right\|$, матрицей степеней секретности объектов данных $F_v = \left\| f^v_{\varepsilon i} \right\|$ и матрицей полномочий пользователей $P = \left\| p_{ki} \right\|$ канонической структуры; матрицей описания логической структуры БД ИС $B = \left\| b_{jj'} \right\|$, матрицей степеней секретности $\hat{F} = \left\| \hat{f}_{lj} \right\|$, а также матрицей полномочий пользователей $P = \left\| p_{ki} \right\|$ логической структуры данных. Методы и алгоритмы их построения приводятся в [3,4].

Система защиты $S^3 = \{m_s : \mathrm{s} = \overline{1, \mathrm{S}}\}$ представляет собой взаимосвязанную совокупность методов защиты, где m_s есть s-й метод, а S – общее число методов. Под оптимальной системой защиты данных ЦФИС понимается такая совокупность (подмножество) методов защиты $S_{opt} \subset S^3$, которые в совокупности обеспечивают экстремальное значение некоторого заданного критерия эффективности разработки и/или эксплуатации системы защиты БД ЦФИС при условии соблюдения требований к функционированию БД ИС, выполнению структурных и функциональных ограничений, накладываемых ЦФИС, СУБД и пользователями.

В качестве исходных данных, помимо формального описания механизмов защиты канонической и логической структур БД ИС, используются также характеристики логической структуры БД ИС, запросов пользователей и транзакций, ограничения на возможность доступа пользователей к отдельным типам логических записей, параметры методов защиты информации от несанкционированного доступа и технических средств хранения информации и взаимодействия пользователей с БД.

Для формализации задачи синтеза оптимальной системы защиты вводятся следующие переменные [3,5]:

– переменные, определяющие требования пользователей на доступ к файлам ПБД и БД НТИ;

– переменные, идентифицирующие правомочность доступа пользователей к файлам БД ИС;

– переменные о размещении файлов на внешних устройствах памяти;

– переменные прикрепления пользователей к терминалам;

– переменные выбора метода защиты для объектов БД ИС;

– производные переменные.

Критериями эффективности при решении задач синтеза оптимальной системы защиты данных ЦФИС являются максимум информационной независимости пользователей БД ИС, минимум суммарных потерь от несанкционированного доступа к конфиденциальной информации БД ИС и др. В качестве ограничений выступают ограничения на уровень защищенности информационных ресурсов БД ИС, на стоимость разработки и эксплуатации системы защиты, ограничения, определяемые требованиями к эффективности использования ресурсов вычислительной системы и др. [3].

Поставленные задачи синтеза относятся к классу задач нелинейного целочисленного программирования с булевыми переменными. Методы и алгоритмы решения данных задач приводятся в [5].

В результате решения поставленных задач формируется оптимальная по заданному критерию эффективности, коррелированному с требованиями информационной безопасности, система защиты БД ЦФИС, обеспечивающая:

– распределение логических записей по файлам ПБД и БД НТИ с учетом степеней секретности логических записей и характеристик запросов пользователей;

– распределение файлов ПБД и БД НТИ между устройствами памяти в соответствии с требованиями безопасности данных и эффективности доступа к ним;

– закрепление пользователей ЦФИС за терминалами;

– сопряжение множества терминалов с множеством внешних носителей;

– закрепление методов непосредственной защиты за объектами защиты различных структурных уровней.

Заключение

В работе рассмотрены особенности построения ЦФИС, характеристики и требования к БД ИС, обеспечивающей и

информационной инфраструктуре ЦФИС. Рассмотрены постановка задачи, модели и методы построения оптимальной системы защиты данных ЦФИС. Полученные результаты использовались при построении оптимальной системы защиты БД ЦФИС евразийского патентного информационного пространства [1,2].

Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011

Литература:

1. *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.

2. *Фаязов Х.Ф., Сиротюк В.О., Овчинников А.В., Бурцев А.Б.* Формирование и развитие евразийского патентно-информационного пространства. – М.: ИНИЦ «Патент», 2010. – 124 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. Материалы сайта ORACLE. – URL: https://www.oracle.com/ (дата обращения 14.10.2021).

5. *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.

Грузман В.А.

Исследование проблемы обеспечения комплексной безопасности Арктической зоны РФ методами сценарного анализа

Аннотация: Выполнено исследование проблем обеспечения комплексной безопасности железнодорожного транспорта в Арктической Зоне РФ; разработана базовая интегрированная многофакторная модель, проведен сценарный анализ эффективности управления реализацией государственной политики РФ в Арктике. Предложенный подход обеспечивает значительное повышение обоснованности генерируемых сценариев развития ситуации, точности формируемых на их основе прогнозов, а также достоверности оценки эффективности принимаемых управленческих решений.

Ключевые слова: анализ, синтез, сценарии развития, экономические и технические системы, управляемость, безопасность

Сценарный анализ развития сложных систем

Одним из методов представления информации о возможных изменениях сложных социально-экономических систем и выработки эффективных управленческих решений является сценарный анализ [1]. Понятие сценария в настоящее время используется уже достаточно широко, особенно при анализе стратегических управленческих решений в организационном управлении [2]. Сценарный подход относится к классу объектно-ориентированных методов представления информации о внутренней обстановке и состоянии внешней среды и выработке ответных действий (в первую очередь, в качестве реакции на внутренние и внешние деструктивные воздействия и связанные с ними риски различной природы).

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

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

Подход к решению задачи

Одним из важнейших стратегических направлений освоения Арктической зоны РФ (АЗРФ) является рациональное, экономически обоснованное комплексное развитие транспортной инфраструктуры, включающее развитие транспортных сетей, средств и систем, имеющих высокую пропускную способность и способных надежно и эффективно функционировать в сложных природно-климатических условиях.

Основой арктической транспортной системы является эффективная эксплуатация, впрочем, как и социально-экономическое развитие АЗРФ в целом, которые невозможны без устойчиво и эффективно функционирующей сети железнодорожного транспорта. При этом, как показывает практика, интегральная эффективность работы железных дорог в значительной мере определяется обеспечиваемым уровнем безопасности в самом широком толковании данного понятия.

В силу наличия проблем подготовки, принятия, реализации и оценки эффективности управленческих решений существенно возрастает роль этапа моделирования и опережающего сценарного анализа ключевых тенденций развития ситуации в АЗРФ, а также оценки возможных последствий принимаемых решений в краткосрочной и долгосрочной перспективе.

Практическое решение рассмотренных задач обеспечения безопасности должно осуществляться на трех базовых уровнях: стратегическом, тактическом, оперативном.

Базовые типы стратегий обеспечения безопасности:

- ориентированные на ликвидацию источников уязвимости или в случае невозможности – на ослабление действия внешних и внутренних источников угроз;

- ориентированные на устранение существующих или предотвращение возникновения вероятных угроз безопасности (в случае невозможности воздействия на источники уязвимости);

- нацеленные на предотвращение или снижение интенсивности деструктивного воздействия существующих или вероятных угроз безопасности рассматриваемых типов;

- направленные на максимально возможное снижение тяжести последствий реализации угроз и компенсацию нанесенного ущерба, а также ликвидацию негативных последствий.

Тактический уровень предполагает решение задач, связанных с ликвидацией (блокированием) угроз или предотвращением их негативного воздействия на объект управления.

Внутренние угрозы реализации государственной политики России в Арктике определяются, прежде всего, имеющимися комплексными проблемами в развитии социально-экономической сферы как на региональном, так и на федеральном уровнях [3].

К основным их источникам можно отнести:

– неравномерность распределения ресурсов;

– моноспециализацию хозяйства и моноструктурный характер экономики в целом;

– невысокую производительность труда;

– усугубление отрицательных демографических процессов;

– неприспособленность региональных экономик к возможным глобальным климатическим изменениям;

– низкую энергоэффективность региональных экономик, высокую энергоемкость, а также себестоимость генерации и транспортировки электроэнергии;

– значительный уровень риска для инвесторов и др.

В качестве потенциальных негативных результатов воздействия рассматриваемых внутренних угроз могут рассматриваться:

– увеличение пространственной асимметрии в развитии между отдельными приарктическими территориями;

– отток высококвалифицированных кадров из приарктических районов в другие регионы и за рубеж, сужение социальной базы экономического развития;

– рост уязвимости стратегических секторов экономики;

– создание внутренних источников уязвимости формируемыми мощными финансово-технологическими агломерациями на приграничных территориях других государств, а также их союзов;

– возможные негативные последствия глобальных климатических процессов и др.

Несмотря на то, что Россия располагает значительными морскими запасами углеводородов, помимо упомянутых выше существует еще целый ряд внутренних угроз успешному освоению природных ресурсов Арктики.

Исследование базовой модели развития транспортной инфраструктуры АЗРФ

Для решения рассматриваемого комплекса задач разработана базовая интегрированная многофакторная модель развития транспортной инфраструктуры АЗРФ, состоящая из трех взаимосвязанных моделей:

– «Анализ перспектив и рисков социально-экономического развития АЗРФ»;

– «Анализ развития системы портов СМП»;

– «Анализ проблем обеспечения комплексной безопасности железнодорожного транспорта».

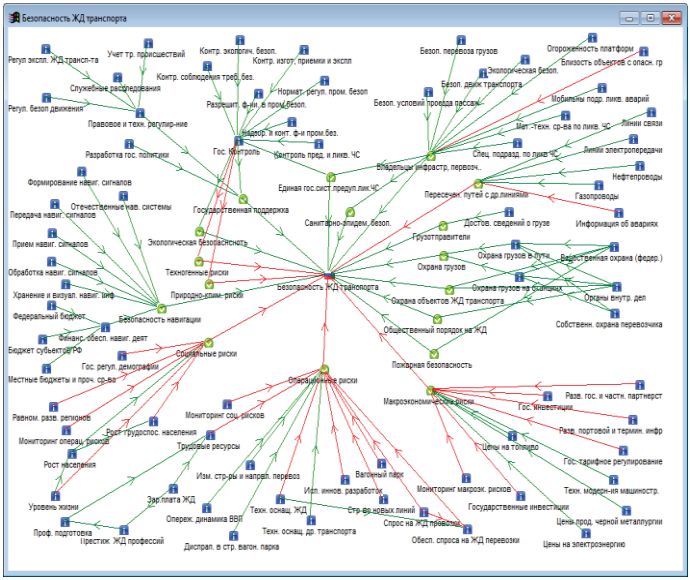


Рисунок 1 – Структура взаимосвязей модели

Исследование данного показателя (в широкой его трактовке) предполагает анализ наиболее существенных и, в первую очередь, стратегических факторов риска развития железнодорожного транспорта, связанных с различными аспектами безопасности. Структура взаимосвязей выделенных факторов представлена на рисунке 1. Основные стратегические факторы безопасности железнодорожного транспорта:

– операционные риски;
– макроэкономические риски;
– социальные риски;
– государственная поддержка;
– единая государственная система предупреждения и ликвидации ЧС на транспорте;
– природно-климатические риски;
– техногенные риски;
– экологическая безопасность и др.

Результаты моделирования

Объединение построенных моделей в единую структуру предполагает создание в ней трех слоев и проведение межслойных взаимосвязей между отдельными факторами. На первом этапе моделирования исследовался сценарий развития порта Архангельск. Для этого в модели были деактивированы факторы «Развитие порта Индига» и «Развитие порта в бухте Хабарова». На втором этапе моделирования исследовался сценарий развития портов Индига и бухты Хабарова. Для этого в модели был деактивирован фактор «Развитие порта Архангельск». Долевые характеристики сценария представлены на рисунке 2.

Стратегические факторы риска железнодорожного транспорта	Растет	Уменьшается	Постоянно	Устойчиво	Нестабильно	Стабилизируется
Глобальная конкурентоспособность АЗРФ	95%	0%	5%	0%	0%	0%
Развитие портов СМП	95%	0%	5%	0%	0%	0%
Макроэкономические риски	5%	95%	5%	0%	0%	0%
Безопасность железнодорожного транспорта	90%	5%	5%	0%	0%	0%

Рисунок 2 – Долевые характеристики сценария

Результаты моделирования демонстрируют благоприятный сценарий развития ситуации. Развитие портов положительно (95%), падение наблюдается лишь на начальном периоде, который связан с затратами на строительство и соответствующими макроэкономическими рисками, которые в начале показывают кратковременный рост (5%), затем устойчивое непрерывное снижение. Наблюдается также рост безопасности железнодорожного транспорта. Положительные тенденции основных факторов модели благоприятно отражаются на росте конкурентоспособности АЗРФ.

Таким образом, выполненное исследование убедительно показывает, что сценарный анализ обеспечивает возможность комплексного подхода к решению задач безопасности, анализа взаимосвязанных, но принципиально различных по своей природе явлений и процессов, а также исследования имитационных моделей с использованием количественных оценок и абсолютных шкал в реальном масштабе времени.

Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011

Литература:

1. 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.

2. *Архипова Н.И., Кульба В.В., Косяченко С.А., Чанхиева Ф.Ю., Шелков А.Б.* Организационное управление. – М.: Изд-во РГГУ, 2007. – 733 с.

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://www.garant.ru/products/ipo/prime/doc/74710556/ (дата обращения 14.10.2021).

Фуругян М.Г.

Алгоритмы оптимизации контроля в вычислительных системах реального времени

Аннотация: Рассматривается задача оптимального расположения модулей контроля в вычислительной системе реального времени. Данная задача формулируется в виде минимаксной задачи. Исследуются следующие структуры графа частичного порядка выполнения прикладных модулей: последовательная цепочка, несколько независимых последовательных цепочек. Разработаны алгоритмы построения оптимальной расстановки модулей контроля.

Ключевые слова: система реального времени, оптимальная расстановка модулей контроля

Введение

При разработке и функционировании вычислительных систем реального времени необходимо учитывать возможность возникновения сбоев и ошибок, возникающих при выполнении прикладных модулей. Для контроля правильности вычислений, обнаружения сбоев и повышения безопасности функционирования сложных технических объектов в систему помимо прикладных модулей вводят специальные программы – модули контроля. Эти модули помимо отслеживания сбоев и ошибок в системе сохраняют промежуточную информацию, что позволяет при рестарте системы воспользоваться сохраненными в них данными, а не выполнять все вычисления заново. Таким образом, наличие модулей контроля может существенно улучшить надежность работы системы и уменьшить временные издержки, вызванные возникновением сбоев и ошибок, что крайне важно для систем жесткого реального времени.

Задачи оптимизации расположения модулей контроля исследовалась ранее рядом авторов и при их решении разрабатывались, в основном, вероятностные модели [1-3]. В [4] предполагается, что модули контроля уже расставлены некоторым образом. Для этого случая разработан алгоритм построения зоны

рестарта, т.е. минимальной совокупности прикладных модулей, подлежащей перезапуску после обнаружения ошибки некоторым модулем контроля. В [5] разработан алгоритм, позволяющий определить такое расположение модулей контроля, при котором математическое ожидание суммарного времени, затраченное на выполнение всех модулей, минимально.

В настоящей работе предполагается, что программное обеспечение вычислительной системы реального времени состоит из прикладных модулей, на множестве которых задано отношение частичного порядка в виде независимых ориентированных цепочек. Количество модулей контроля фиксировано. Каждый модуль контроля располагается непосредственно после некоторого прикладного модуля. При обнаружении ошибки каким-либо модулем контроля определяется цепочка повторного выполнения прикладных модулей. Требуется таким образом расположить модули контроля, чтобы максимально возможная длина такой цепочки была минимальной.

1. Постановка задачи

Задан набор прикладных модулей $W = \{w_1, w_2, \cdots, w_N\}$, подлежащих выполнению на вычислительной системе. Каждый модуль w_i выполняется без прерываний и переключений с одного процессора на другой, а длительность его выполнения равна $t_i = t(w_i)$, $i = \overline{1, N}$. На множестве W задано отношение частичного порядка выполнения в виде ориентированного графа $G = (W, A)$, состоящего из нескольких последовательных цепочек, где W – множество узлов, A – множество дуг. Если $(w_i, w_j) \in A$, то модуль w_j может выполняться только после завершения модуля w_i. В этом случае будем также использовать обозначение $w_i \to w_j$. Если

$$w_{i_1} \to w_{i_2} \to \ldots \to w_{i_{n-1}} \to w_{i_n}, \qquad (1)$$

то модули w_{i_j}, $j = \overline{1, n-1}$, являются предшественниками модуля w_{i_n}. Введем обозначения:

$$P(w_i) = \{w_j \in W : w_j \to w_i\}, \; Q(w_i) = \{w_j \in W : w_i \to w_j\}, \qquad (2)$$

$$P_0 = \{w_i \in W : P(w_i) = \varnothing\}, \quad Q_0 = \{w_i \in W : Q(w_i) = \varnothing\}, \qquad (3)$$

т.е. $P(w_i)$ и $Q(w_i)$ – это соответственно непосредственный предшественник и непосредственный последователь прикладного модуля w_i, а P_0 и Q_0 – это прикладные модули, не имеющие соответственно непосредственного предшественника и непосредственного последователя.

Помимо прикладных модулей в системе имеется K модулей контроля, $K \le N$. Каждый модуль контроля связан с некоторым прикладным модулем и выполняется сразу же после завершения этого прикладного модуля. С каждым прикладным модулем связан не более чем один модуль контроля. Предполагается, что время выполнения модуля контроля существенно меньше времени выполнения прикладных модулей и им можно пренебречь. Пусть $\overline{W} = \{w_{i_1}, w_{i_2}, ..., w_{i_K}\}$ – множество всех прикладных модулей, с которыми связаны модули контроля. Будем называть его расстановкой модулей контроля (или, просто, расстановкой).

Модуль контроля после своего выполнения сигнализирует об отсутствии или наличии ошибки. В первом случае вычисления продолжаются по ранее построенному расписанию. В случае обнаружения модулем контроля ошибки необходимо повторить выполнение некоторых прикладных модулей следующим образом.

Пусть модулем контроля, связанным с некоторым прикладным модулем $w_{i_n} \in \overline{W}$, была обнаружена ошибка. В графе G рассматривается цепочка π вида (1), в которой $w_{i_j} \notin \overline{W}$, $j = \overline{2, n-1}$, и, кроме того, либо $w_{i_1} \in P_0$, либо существует прикладной модуль $w_{i_1-1} \in \overline{W}$, такой, что $w_{i_1-1} \to w_{i_1}$. Иными словами, указанная цепочка начинается с прикладного модуля, который либо не имеет непосредственного предшественника, либо имеет непосредственного предшественника, с которым связан модуль контроля, а все остальные прикладные модули, кроме w_{i_n}, не являются таковыми. Будем называть такие цепочки π цепочками рестарта. В случае обнаружения ошибки модулем контроля, связанным с прикладным модулем w_{i_n}, необходимо для цепочки

вида (1) повторить выполнение всех ее прикладных модулей. Длиной цепочки рестарта π вида (1) будем называть величину $t(\pi) = \sum_{j=1}^{n} t_{i_j}$.

Пусть $\Pi(w_{i_n})$ – множество всех цепочек π вида (1) и пусть $t(\Pi(w_{i_n}) = \max_{\pi \in \Pi(w_{i_n})} t(\pi)$, т.е. $t(\Pi(w_{i_n})$ – это максимальная длина таких цепочек. Допустимой расстановкой будем называть такую расстановку $\overline{W}$, при которой каждый прикладной модуль из Q_0 связан с модулем контроля, т.е.

$$Q_0 \subseteq \overline{W}. \quad (4)$$

Если расстановка не является допустимой, то контроль вычислений не может быть выполнен полностью. Всюду в дальнейшем будем предполагать, что $K \geq |Q_0|$ и что к каждому прикладному модулю из Q_0 прикреплен модуль контроля, поскольку при $K < |Q_0|$ допустимой расстановки не существует.

Пусть Ω – множество всех допустимых расстановок. Задача заключается в выборе допустимой расстановки $\overline{W}$, для которой величина $\max_{w \in \overline{W}} t(\Pi(w))$ минимальна. Иными словами, требуется определить величину

$$T_{opt} = \min_{\overline{W} \in \Omega} \max_{w \in \overline{W}} t(\Pi(w)) \quad (5)$$

и допустимую расстановку $\overline{W}$, на которой реализуется указанный минимакс. Такую расстановку будем называть оптимальной. Таким образом, при оптимальной расстановке минимизируется максимальная длина цепочки рестарта.

Рассмотрим случай, когда граф G является последовательной цепочкой $w_1 \to w_2 \to \ldots \to w_N$. В этом случае $Q_0 = \{w_N\}$ и в силу (4) любая допустимая расстановка имеет вид $\overline{W} = \{w_{i_1}, w_{i_2}, \ldots, w_{i_{K-1}}, w_{i_K} = w_N\}$. Без ограничения общности можно считать, что в этом случае $\Omega = \{\overline{W} : 1 \leq i_1 < i_2 < \cdots < i_{K-1} < i_K = N\}$. Введем обозначения:

$I_k = \{i_{k-1}+1, \cdots, i_k\}$, $T_k = \sum\limits_{i \in I_k} t_i$, где $k = \overline{1, K}$, $i_0 = 0$. В соответствии с (5) задача заключается в поиске величины

$$T_{opt} = \min\limits_{W \in \Omega} \max\limits_{k=\overline{1, K}} T_k \tag{6}$$

и расстановки $\overline{W}$, реализующей указанный минимакс. Разработаны два алгоритма – точный (алгоритм 1) и приближенный (алгоритм 2). Алгоритм 1 основан на переборе всех допустимых расстановок, число которых составляет C_{N-1}^{K-1}. Его вычислительная сложность при фиксированном K составляет $O(N^{K-1})$, т.е. алгоритм 1 является полиномиальным. Введем обозначения:

$$T_1^* = \left(\sum\limits_{i=1}^{N} t_i \right) / K \,;\; T_2^* = \max\limits_{i=\overline{1, N}} t_i;\; T^* = \max(T_1^*, T_2^*). \tag{7}$$

Каждая из величин T_1^*, T_2^* и T^* является нижней оценкой величины T_{opt}, т.е. $T_{opt} \geq T^*$.

Алгоритм 2 минимизирует максимальное отклонение величин T_k, $k = \overline{1, K}$, от T^*, т.е. находит $\min\limits_{W \in \Omega} \max\limits_{k=\overline{1, K}} \left| T_k - T^* \right|$ и расстановку $\overline{W}$, реализующую этот минимакс. Его вычислительная сложность составляет $O(KN)$. Для определения отклонения величины $T = \max\limits_{k=\overline{1, K}} T_k$ от величины T_{opt} применима оценка $T - T_{opt} \leq T - T^*$, которая может быть вычислена после работы алгоритма 2.

Рассмотрим случай, когда граф G состоит из p независимых последовательных цепочек, длины которых равны N_i, $i = \overline{1, p}$. Для этого случая разработан алгоритм 3, основанный на специальной процедуре включения модуля контроля в цепочку рестарта. Согласно (5), этот модуль контроля должен разбивать указанную цепочку на две цепочки так, чтобы длина максимальной из них

была бы минимально возможной. Вычислительная сложность алгоритма 3 составляет $O((\sum_{i=1}^{p} N_i)(K-p))$, где p – число цепочек.

Литература:

1. *Grassi V., Donatiello L., Tucci S.* On the Optimal Checkpointing of Critical Tasks and Transaction-Oriented Systems // IEEE Trans. Software Eng. – Jan. 1992. – Vol. 18. № 1. – P. 72-77.

2. *Coffman E., Gilbert E.* Optimal Strategies for Scheduling Checkpoints and Preventive Maintenance // IEEE Trans. Reliability. – Apr. 1990. – Vol. 39. № 1. – P. 9-18.

3. *Bruno J.L., Coffman E.G.* Optimal Fault-Tolerant Computing on Multiprocessor Systems // Acta Informatica. – 1997. – Vol. 34. – P. 881-904.

4. *Белый Д.В., Сушков Б.Г.* Модель организации рестартов в системах реального времени. – М.: ВЦ РАН, 1996. – 32 с.

5. *Гречук Б.В., Фуругян М.Г.* Алгоритмы организации рестартов в системах реального времени с произвольным графом связей. – М.: ВЦ РАН, 2004. – 32 с.

Сташенко В.И., Скворцов О.Б., Троицкий О.А.

Особенности оценки вибрационных воздействий в электромеханических системах с импульсным управлением

Аннотация: Рассмотрены вопросы генерации вибрации в проводниковых элементах мощного энергетического оборудования, работающих в условиях прохождения электрических импульсов. Проводниковые элементы в условиях действия токов высокой плотности испытывают не только значительные температурные воздействия, но и большие механические динамические нагрузки. Действие механических вибраций влияет на механические свойства металла и может приводить к снижению усталостной прочности, но может также быть использовано при решении задач диагностики состояния обмоток мощных электрогенераторов и двигателей.

Ключевые слова: электрогенератор, импульсный инвертор, электрический импульс, вибрация, циклическая

усталость, надежность, ускорение, деформация, электропластический эффект, вибропластический эффект, диагностика

Введение

При выборе конструкционных материалов мощного электроэнергетического оборудования внимание в первую очередь обращают на обеспечение заданных электрических характеристик, например, на снижение величины активного сопротивления. При этом конструкционные элементы также испытывают значительные динамические нагрузки. В соответствии с ГОСТ 5616-89 элементы генераторов ГЭС и ГАЭС рассчитаны на действие вибрации с частотой 1-100 Гц и амплитудой не более 1 g. Перспективные направления энергетики, такие как солнечная энергетика, а также ветровая энергетика и гидроэнергетика с имеющими переменную скорость вращения агрегатами, предполагают использование мощных импульсных инверторов. Эксплуатация такого оборудования связана с обеспечением непрерывной работы с импульсными напряжениями и токами высокой плотности. Приведенные ниже результаты экспериментальных исследований показывают, что на конструкционные элементы в виде электропроводящих шин и элементы их крепления действуют вибрационные ускорения, частоты и амплитуды которых существенно превышают указанные в ГОСТ 5616-89 и в других нормативных документах. Вибрации повышенной частоты при этом могут быть причиной снижения надежности оборудования из-за проявления процессов циклической усталости [1]. Действие электрических импульсов на электропроводящие материалы находит промышленное применение [2,3] и проявляется как изменение механических свойств материала под влиянием электропластического эффекта.

Методика исследования влияния электрических импульсов на проводники

В данной работе было проведено исследование вибрационных процессов, возникающих в проводниках при воздействии на него электрических импульсов. Для этой цели использован стенд, структурная схема которого показана на рисунке 1.

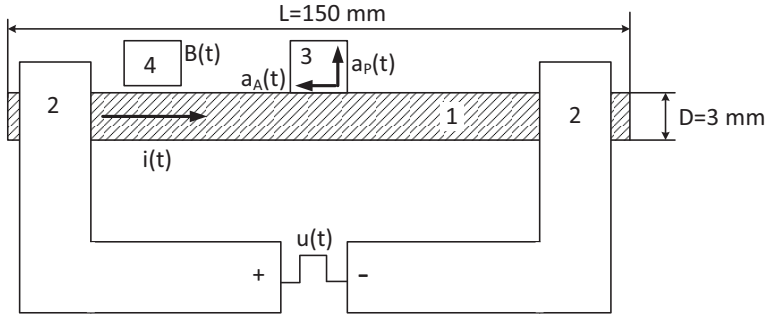


Рисунок 1 – Структурная схема эксперимента по определению вибрационного отклика в проводнике 1 на действие внешнего электрического импульса u(t). Проводник закреплен между шинами 2. Контроль осевой вибрации $a_A(t)$ и поперечной вибрации $a_P(t)$ выполняется двухкомпонентным акселерометром 3. Контроль тока i(t) по изменениям магнитной индукции B(t) выполняется датчиком магнитного поля 4

Сигналы от датчиков вибрации и магнитного поля поступают на компьютерную систему для хранения и последующего анализа. Пример полученных сигналов представлен на рисунке 2. Сигналы ускорения в поперечном направлении Az для диаметрально расположенных акселерометров показывают, что при воздействии электрического импульса проводник испытывает изгибные колебания в виде механических ударов противоположных направлениях в моменты начала переднего и заднего фронтов электрического импульса. Синхронно записанные сигналы компонент пространственного вектора магнитной индукции By и Bz показывают, что в моменты времени начала электрического импульса величина тока еще очень мала. Представленные сигналы получены при пропускании электрического импульса длительностью 980 мкс, создающего среднюю величину плотности тока в проводнике порядка 400 А/мм^2.

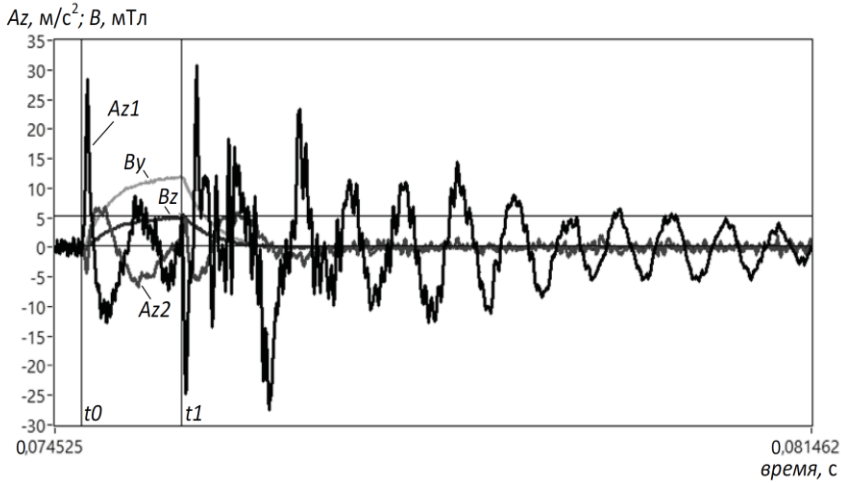


Рисунок 2 – Сигналы вибрационного ускорения и компонент магнитной индукции при пропускании прямоугольного электрического импульса через проводник из серебра диаметром 2 мм и длинной 150 мм

Ударные механические процессы вызывают последующие затухающие гармонические колебания в материале проводника.

Обсуждение результатов

Направление наблюдаемых вибраций в проводнике зависит от направления приложенного электрического поля [4]. На рисунке 3 приведен пример сигналов от датчиков магнитной индукции в увеличенном масштабе. В этом случае можно видеть, что в начальные моменты фронтов электрического импульса *t0* и *t1* наблюдаются всплески величины магнитного поля, близкие по времени с моментами возникновения ударных механических процессов в материале проводника. Последующее плавное увеличение магнитного поля связано с изменениями тока через проводник, определяемое процессами самоиндукции и скин-эффекта. Такие плавные изменения практически не влияют на происходящие вибрационные процессы в проводнике.

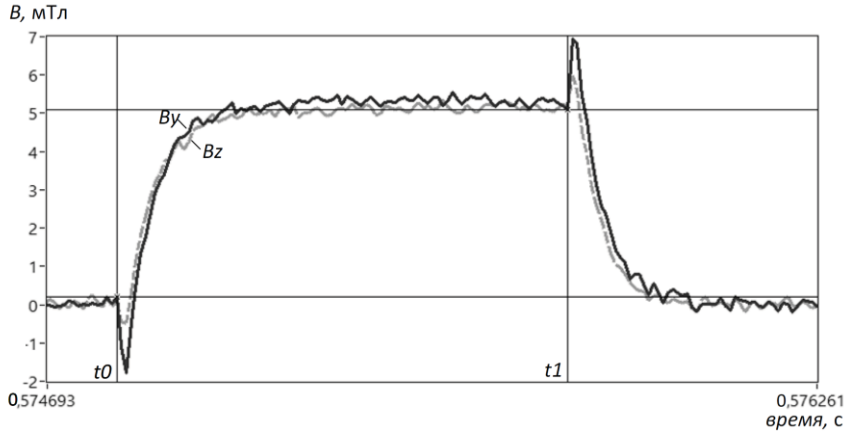


Рисунок 3 – Пример сигналов компонент магнитной индукции при действии электрического импульса на проводник из нержавеющей стали диаметром 3 мм и длинной 150 мм

Несмотря на продолжительную историю исследования вопроса о механизмах формирования механического отклика в материале проводника на действие электрического импульса [2,3,5], предлагаемые гипотезы имеют ряд противоречий данным экспериментов. Получаемые амплитудные оценки вибрационного отклика характеризуются линейной зависимостью от амплитудных оценок величины электрического импульса, как показано на рисунке 4.

Действие одиночных электрических импульсов не вызывает сколько-нибудь значительного нагревания проводника. Нагрев импульсом длительностью 1000 мкс с плотностью тока 1000 А/мм^2 вызывает нагревание на 1-5 градусов в зависимости от свойств материала проводника [6]. Это, как и линейный характер деформационного отклика показывает, что вклад тепловых эффектов действия электрического импульса незначителен.

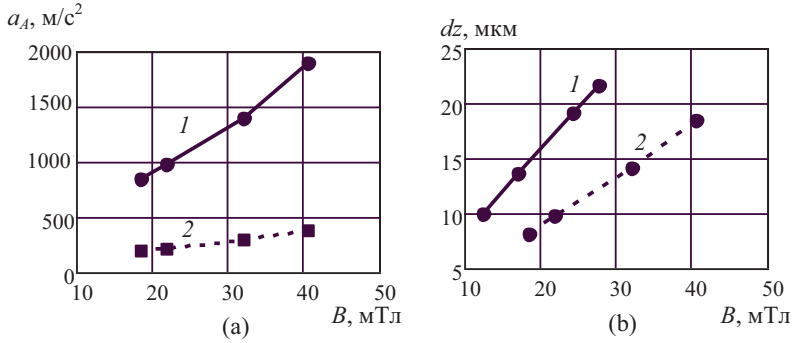


Рисунок 4 – Зависимость размаха вибрационных сигналов осевого ускорения (a) и поперечного перемещения (b) от размаха сигнала магнитной индукции B для проводников из серебра диаметром 2 мм - *1* и прямоугольного сечения площадью 2 мм^2 - *2*

Действие последовательности импульсов на проводники [7] сопровождается формированием последовательности ударных механических импульсов, каждый из которых вызывает формирование затухающих гармонических колебаний. Такие гармонические вибрации могут создавать циклические нагружения материала проводника. Периодические ударные механические нагружения материала проводящих шин способствуют образованию дефектов. Гармонические колебания, возбуждаемые в материале, приводят к проявлению многоцикловой и сверхмногоцикловой усталости материала из-за понижения порога пластической деформации, наблюдаемого на *S-N* диаграммах большинства конструкционных материалов, используемых в мощном энергетическом оборудовании.

Заключение

Рассмотренные особенности вибрационного отклика проводников на пропускание через них импульсных токов необходимо принимать во внимание при конструировании электропроводящих узлов мощного энергетического оборудования. Такие вибрации могут иметь значительную амплитуду вибрационного ускорения, которое сопровождается возникновением больших локальных механических напряжений.

Это может стать причиной усталостных нагрузок, наряду с типовыми вибрациями удвоенной промышленной частоты, проявление которых определяется эффектом близости.

Возбуждение нормированных по амплитуде высокочастотных вибраций одиночными электрическими импульсами и получаемый вибрационный отклик можно также использовать для диагностирования качества крепления электропроводящих элементов мощного электрооборудования вместо применения механических ударов для оценки собственной частоты таких элементов.

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 10.10.2021).

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.: Изд-во «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.: Изд-во «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.

Чинакал В.О.

Создание систем усовершенствованного мониторинга и управления для повышения эффективности и безопасности управления сложными промышленными объектами

Аннотация: Рассматривается подход к повышению безопасности и эффективности управления сложными промышленными объектами в классе непрерывных производств на базе создания перспективных интегрированных систем усовершенствованного мониторинга состояния и управления объектом AMS&APC (AMS – Advanced Monitoring System, APC – Advanced Process Control). Разработаны требования и структура AMS&APC, обеспечивающая автоматизированную комплексную обработку измеряемой и технологической информации об объекте и квазиоптимальное управление таким объектом. Предложена реализация прототипа AMS&APC с использованием интеллектуальных методов анализа данных, прогнозирования и ретроспективного оценивания.

Ключевые слова: безопасность управления, сложные промышленные объекты, технологические процессы, непрерывное производство, AMS, APC

Введение

Создание перспективных распределенных систем усовершенствованного мониторинга состояния и управления сложными промышленными объектами (СПО) в классе непрерывных технологических производств (ТП), таких как пищевая промышленность, строительные материалы, нефтехимия, нефтепереработка и другие является одной из актуальных задач [1]. В настоящее время существенно усложняются требования к функционалу систем контроля и управления СПО, повышению безопасности управления (БУ) объектами и повышению реальной эффективности работы всех автоматических и автоматизированных систем в режимах контроля и управления.

Необходимо не только обеспечивать контроль и управление объектом в условиях сильных, нестационарных, часто не полностью измеряемых возмущений, но и автоматически оценивать текущее состояние СПО и технических средств контроля и управления (ТСУ) объекта, своевременно обнаруживать и оценивать изменения ключевых технологических параметров (КТП) материальных потоков, выявлять наличие или предпосылки возникновения нештатных и аварийных ситуаций, обеспечивать оперативную поддержку решения других сложных задачи в реальном времени.

Применительно к данному классу СПО в данной работе разрабатывается концепция построения интегрированных систем усовершенствованного мониторинга и управления объектом – AMS&APC (AMS – Advanced Monitoring System, APC – Advanced Process Control), как развитие подхода, предложенного в [2].

Для решения проблем контроля и управления СПО создаются различные типы интеллектуальных систем поддержки управления (ИСПУ). На уровне автоматизированных систем оперативно-диспетчерского управления производством (MES-системы) могут разрабатываться и применяться мощные интеллектуальные системы поддержки принятия решений (ИСППР) [1,3]. Для поддержки автоматического решения отдельных сложных задач контроля и управления СПО применяют локальные ИСПУ (агенты), в частности, встраиваемые в систему контроля и управления интеллектуальные компоненты (ВИК) [4].

Опыт ведущих фирм в области автоматизации производства с использованием разработок и эффективного применения в промышленности отдельно AMS и APC-систем показывает [1], что создание интегрированных AMS&APC-систем и их промышленное применение позволит существенно повысить эффективность и безопасность работы СПО.

Внедрение интегрированной AMS&APC-системы позволит пользователям иметь и использовать:

– все доступные оперативные данные, поступающие на входы подсистемы AMS от штатных средств мониторинга и управления объектом (данные измерений параметров технологических потоков от поточных датчиков и анализаторов, данные о состоянии резервуаров и установок, данные всех лабораторных анализов, текущие данные от измерительных средств автоматического

мониторинга состояния основного динамического и статического оборудования (EAM-систем)) [1,2,4];

– расчетные данные от LIMS-систем и виртуальных анализаторов (ВА) [1,2,5];

– дополнительную информацию, получаемую в результате применения интеллектуальных методов обработки текущих данных реального времени, актуальных технологических данных и различных архивных данных [2,4,5];

– адаптивные модели виртуальных анализаторов, применяемые для оперативной оценки редко измеряемых параметров ТП с учетом их связи с другими, более часто измеряемыми параметрами ТП, а также оперативные корректировки параметров соответствующих косвенных моделей ВА [1,6] с использованием различных измерений;

– реализацию интеллектуальных методов (ИМ) для формирования гипотез и их оценки при различных ситуациях возможного возникновения изменений параметров ТП в прошлом и настоящем времени [5,6];

– общий источник проверенных и откорректированных оперативных и интегрированных данных на выходах подсистемы AMS, единых для всех пользователей и систем СПО;

– возможность использования выходных данных подсистемы AMS как в эксплуатирующихся традиционных АСУТП, так и в современных системах усовершенствованного управления непрерывными технологическими процессами (ТП) (APC-системы), а также в диспетчерских MES-системах [1].

Следует отметить, что при создании интегрированной AMS&APC-системы необходимо учитывать целый ряд характерных особенностей и разнообразных ограничений, свойственных многим производствам данного типа (разновременные измерения показателей, редкие и часто запаздывающие измерения, имеющие разную погрешность, наличие взаимовлияния параметров, сложность описания и не стационарность динамических процессов, различные виды неопределенностей и т.п.) [1,2].

Наличие единой системы AMS&APC позволит в дополнение к традиционным методам статистического оценивания параметров ТП использовать также современные методы интеллектуального анализа оперативных данных [5-7], учесть имеющуюся

дополнительную технологическую информацию о типах и параметрах сырья, заданных требованиях к режимам его переработки на различных установках с учетом их состояния, имеющихся ресурсов и влияния других значимых факторов [5]. В итоге применение AMS&APC может существенно повысить общую эффективность управления СПО для данного класса производств.

При разработке AMS&APC-систем использованы модели типовых КТП для оценки изменений их параметров в зависимости от различных причин. При построении и корректировке параметров модели ВА используются методы текущего регрессионного анализа [5-7], а в APC методы предикторного управления [1]. Данный подход достаточно эффективен при не слишком больших вариациях состава сырья, хорошей стабилизации режимов работы установок и возможности периодической корректировки отклонений регулируемых показателей. При существенных колебаниях состава сырья, и значительных изменениях режимов работы установок целесообразно с помощью AMS обеспечить выбор и настройку ВА с использованием набора альтернативных моделей [5]. Выбор применяемых методов текущей регрессии и начальных параметров производится с использованием продукционных правил, обеспечивающих учесть конкретную ситуацию с типом сырья, текущие оценки его качества, заданные режимы работы установки и фактические возможности систем измерения [5-7].

Далее рассмотрим кратко пример структуры и связей основных блоков простой AMS&APC, в составе традиционной системы регулирования, подсистемы AMS и подсистемы APC в составе ИСПУ АСУТП.

Пример структуры AMS&APC-системы

На рисунке 1 представлен пример структуры и связей основных блоков простой AMS&APC с указанием основных потоков и уровней получения, передачи, хранения и обработки информации в системе. Основные элементы: – Объект управления (ОУ); – Штатная система регулирования и управления нижнего уровня (СУ); – Исполнительные механизмы (ИМ); – Система измерения входов ОУ и параметров внешней среды (ИС1); – Система частых периодических измерения количественных выходов ОУ (ИС2); – Система редких изменения фазовых координат ОУ на моменты

времени t+1 – t+k при заданной стратегии управления и текущих оценках параметров по измерениям на скользящем интервале t-π – t.

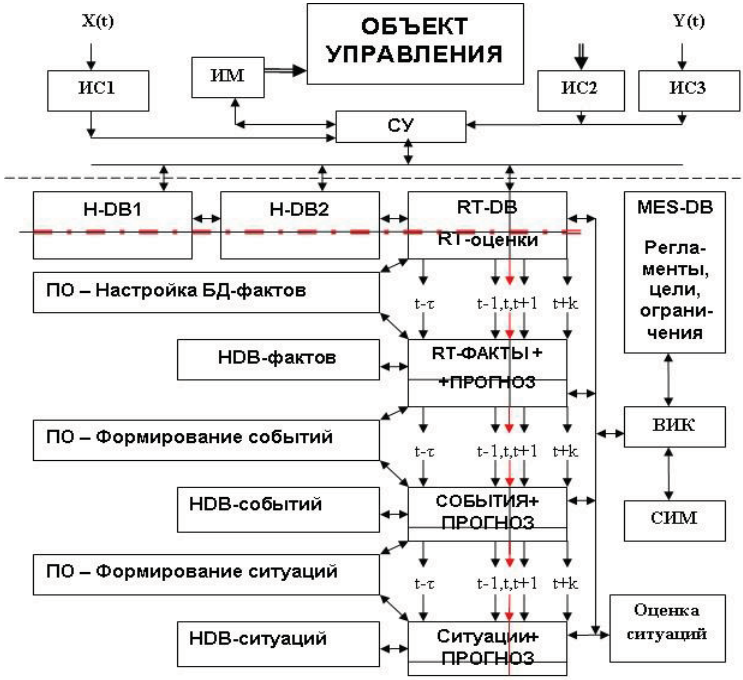


Рисунок 1 – Структура и связи основных блоков простой AMS&APC

Обозначения основных этапов формирования и хранения логических массивов данных и соответствующего программного обеспечения (ПО): – RT-DB – база данных (БД) измерений реального времени; RT-факты – БД логических массивов результатов сравнения текущих измерений с регламентными ограничениями; – H-DB1, H-DB2 – краткосрочная и долгосрочная архивные БД всех измерений; MES-DB – БД верхнего уровня, содержащая значения текущих регламентов, целей и ограничений; HDB – архивные БД логических массивов фактов, событий,

ситуаций; ПО – программное обеспечение логической обработки соответствующих уровней данных.

Пунктирной линией и стрелкой обозначены все основные этапы последовательного получения, обработки и хранения результатов некоторого измерения i-го параметра в t-момент времени и отражение его влияния на изменения наборов фактов, событий и ситуаций.

Заключение

Разработка эффективных AMS&APC-систем и их промышленное применение в качестве надежного единого источника оперативных данных для традиционных АСУТП, MES-систем и для систем усовершенствованного управления APC сложными промышленными объектами в классе непрерывных производств позволит существенно повысить общую эффективность и безопасность управления объектами этого класса.

Литература:

1. *Ицкович Э.Л.* Перспективная автоматизация агрегатов предприятий технологических отраслей. – М.: Горячая линия–Телеком, 2018. – 544 с.

2. *Чинакал В.О.* Об одном подходе к мониторингу непрерывных технологических процессов. / Труды 17-ой международной конференции CAD/CAM/PDM – 2017 «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта». – М.: ИПУ РАН, 2017. – С. 438-440.

3. *Рассел С., Норвиг П.* Искусственный интеллект: современный подход. – М.: Изд. дом Вильямс, 2007. – 1408 с.

4. *Чинакал В.О.* Разработка и применение встраиваемых интеллектуальных компонентов, построенных с использованием матричных методов / Труды 8 международной научно-практической конференции «Инженерные системы – 2015». Т.1. – М.: РУДН, 2015. – С. 145-150.

5. *Чинакал В.О.* Проектирование виртуальных анализаторов с использованием альтернативных моделей / Труды 17 международной научно-практической конференции CAD/CAM/PDM – 2017 «Системы проектирования, технологической подготовки производства и управления этапами

жизненного цикла промышленного продукта (CAD/CAM/PDM – 2017, Москва)». – М.: ИПУ РАН, 2017. – С. 364-357.

6. *Дж. Бокс, Г. Дженкинс.* Анализ временных рядов. Прогноз и управление. – М.: МИР, 1974. – Выпуск 1 – 406 с. Выпуск 2– 197 с.

7. *Гребенюк Е.А., Ицкович Э.Л.* Повышение точности оценки значений текущих качественных показателей по их дискретным лабораторным анализам с использованием алгоритмов экстраполяции // Автоматизация в промышленности. – 2016. – №8. – С. 4-9.

VIII. Правовые вопросы обеспечения безопасности сложных систем

Чернов И.В., Шелков А.Б., Потапова О.А., Богатырева Л.В.

Технология сценарно-прогнозной экспертизы законопроектов в области регулирования процессов цифровизации

Аннотация: Рассмотрены задачи сценарно-прогнозной экспертизы законопроектов, основной целью которой является повышение эффективности процессов разработки законодательных актов в области регулирования общественных отношений в условиях цифровизации.

Ключевые слова: законотворчество, правовое регулирование, цифровизация, информационное общество, сценарный анализ

Введение

Современный этап развития информационного общества вносит на повестку дня становящуюся все более острой проблему совершенствования системы законодательного регулирования процессов социально-экономического и технологического развития России. Главной целью трансформации права 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].

Особая сложность в эффективном решении данных проблем заключается в необходимости глубокого анализа характера и динамики социально-экономического развития общества и государства, а также в обеспечении возможности своевременно диагностировать возникающие проблемы, предвосхищать возможность возникновения и выявлять альтернативные пути развития проблемных ситуаций, а также, что особенно важно,

оценивать как позитивные, так и возможные негативные последствия реализации решений в области трансформации права в условиях цифровой эпохи.

Все это ужесточает требования к законотворческому процессу, особенно на стадиях выявления потребности в правовой регламентации связанной с цифровыми технологиями сферы общественных отношений, выделения факторов, способствующих или препятствующих достижению целей устойчивого социально-экономического развития страны, а также прогнозной оценки результатов принятия и реализации разрабатываемых нормативно-правовых актов. В этих условиях возрастает актуальность проблем создания эффективных и одновременно с этим достаточно универсальных методов и механизмов опережающей сценарно-прогностической оценки эффективности разрабатываемых правовых актов [2].

1. Анализ основных проблем повышения эффективности законотворческих процессов

Оценка эффективности действия как вновь разрабатываемых (в том числе принципиально новых и отвечающих требованиям времени) законодательных актов, так и адаптированных уже сложившихся юридических норм к возникшим информационным правоотношениям и связанным с ними проблемам, является чрезвычайно сложной комплексной и по своей сути мультидисциплинарной проблемой.

Во-первых, непосредственное влияние процессов нормативно-правового регулирования на развитие общественных отношений крайне трудно вычленить и, соответственно, проанализировать, особенно в условиях интенсивного развития высоких технологий и внутренних процессов общественного (социального, экономического, научно-технического и т.д.) развития, а также характерного для сегодняшнего дня негативного влияния внешней среды.

Во-вторых, на практике достоверная статистическая оценка эффективности законодательного акта возможна только на достаточно большом временном горизонте, поскольку только при таком подходе имеется возможность проведения полноценного анализа влияния закона на развитие общественных отношений в

заданном направлении, а также возможных негативных (как прямых, так и косвенных) последствий его реализации. В силу этого в процессе подготовки правовых актов необходима опережающая оценка ожидаемых результатов их действия после утверждения.

В-третьих, трудности в решении рассматриваемой проблемы существенно возрастают в силу необходимости значительного изменения (трансформации) структуры, состава и содержания правовых инструментов обеспечения поступательного развития страны и безопасности личности, общества и государства в условиях цифровизации, а также отсутствия практического опыта в решении значительной части возникающих проблем, связанных с развитием высоких технологий.

В-четвертых, высокие темпы развития инфокоммуникационных технологий, интенсивный рост вовлеченности в информационные отношения юридических и физических лиц, непрерывное расширение масштабов, методов и способов использования средств информационно-психологического воздействия на граждан нашей страны геополитическими противниками России крайне затрудняют решение не только проблем закрепления уже сложившихся социальных норм и информационных правоотношений, но и в гораздо большей степени предвосхищения возможных путей развития ситуации в условиях цифровой эпохи, а также предвидения и прогнозирования возникающих в связи с этим принципиально новых угроз и возможных последствий их реализации.

Все это значительно усложняет задачу повышения эффективности процессов законодательного регулирования и правоприменения, поскольку ее решение должно базироваться на результатах комплексного исследования объективных причинно-следственных связей социальных, экономических, политических и т.д. процессов, анализа сложившихся в исследуемом периоде тенденций общественного и государственного развития, а также выявления проблем и диагностирования «узких мест».

Во многом решение данных проблем возможно на базе сценарного подхода, позволяющего проводить комплексную (в том числе прогнозную) оценку эффективности ожидаемых результатов реализации принимаемых нормативно-правовых решений и их возможного влияния (как позитивного, так и негативного) на

российское общество и наиболее важные сегменты социально-экономической системы страны [3,4].

2. Основные задачи сценарно-прогнозной экспертизы законопроектов

В рамках законотворческого процесса (рисунок 1) сценарно-прогнозная экспертиза должна обеспечивать решение следующих основных задач.

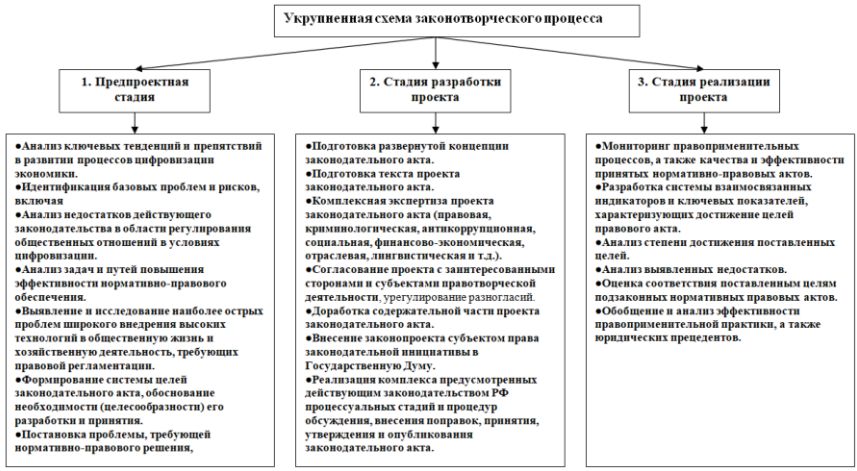


Рисунок 1 – Стадии законотворческого процесса

Предпроектная стадия.

- Разработка базовых сценариев социально-экономического развития государства и общества на длительном временном горизонте.
- Сценарный анализ базовых проблем развития процессов цифровизации, выявление «окон» уязвимости, оценка неопределенности и рисков.
- Оценка существующих и возможных угроз безопасности личности, общества и государства.
- Сценарная оценка текущего уровня урегулированности информационных правоотношений.

- Сценарный анализ эффективности действующих правовых норм и правоприменительной практики, выявление и оценка сложности имеющихся проблем, а также последствий их нерешенности.
- Разработка и анализ аттрактивных и синергических сценариев развития исследуемой ситуации (эффективности решения проблемы, являющейся предметом нормативно-правового регулирования), оценка планируемых результатов и возможных негативных общественно-значимых последствий.

Стадия разработки проекта.

- Разработка, сценарный анализ и оценка эффективности альтернативных путей решения проблемы, выбор наилучшего решения.
- Сценарная оценка ожидаемой результативности законодательного акта, диагностика уязвимостей и оценка влияния неопределенностей.

Стадия реализации проекта.

- Разработка системы взаимосвязанных индикаторов и ключевых показателей, характеризующих достижение целей правового акта.
- Анализ степени достижения поставленных целей правового регулирования в процессе реализации нормативно-правовых актов на основе оценки значений ключевых показателей.
- Сценарная оценка влияния внешних угроз и внутренних рисков, а также иных видов неопределенности на процессы достижения поставленных целей.
- Анализ выявленных в процессе практического действия принятых нормативно-правовых актов недостатков и их влияния на конечный результат.
- Сценарный анализ целесообразности дополнения, корректировки либо исключения отдельных положений нормативно-правовых актов, прогнозная оценка ожидаемых результатов.

Результаты использования сценарно-прогнозной экспертизы на всех основных этапах правотворческого процесса позволят:

- повысить обоснованность системы долгосрочных и среднесрочных целей трансформации системы правового регулирования процессов цифровизации;

- проводить сценарный анализ эффективности альтернативных путей развития системы нормативно-правового обеспечения процессов управления социально-экономическим развитием общества и государства в условиях неопределенности;
- формировать структурированное представление и проводить оценку приоритетности проблем, требующих правового регулирования в условиях развития информационного общества;
- проводить опережающую оценку результативности действия разрабатываемых нормативно-правовых актов и процессов поэтапного достижения поставленных целей.

Заключение

Несмотря на то, что в настоящее время накоплен значительный опыт решения прикладных и практических задач в области сценарного анализа внешних и внутренних источников угроз социальной, экономической, общественной, региональной и техногенной безопасности, при решении проблем повышения эффективности законотворческих процессов и оценки качества и разрабатываемых правовых норм данный подход в настоящее время практически не используется. Однако анализ актуальных и требующих решения задач повышения эффективности процессов трансформации права показывает, что использование именно сценарного подхода в сложившихся условиях позволит существенно повысить эффективность законотворческих процессов.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта 18-29-16151 «Разработка методов управления процессами трансформации права в условиях цифровой технологии»

Литература:

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

2. *Шульц В.Л., Кульба В.В., Шелков А.Б.* и др. Методы анализа влияния процессов трансформации права на развитие социально-экономической системы в условиях цифровизации: сценарный

подход (постановка задачи) // Российский журнал правовых исследований. – 2021. – Т. 8. №1. – С. 19-36.

3. 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.

4. *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.

Аникина Е.В.

Управление рисками сложной компьютерной сети на основе общей арбитражной схемы

Аннотация: В работе рассматривается модель управления рисками сложной системы на основе общей арбитражной схемы.

Ключевые слова: локальный риск, интегральный риск, обобщенная арбитражная схема, максимально стимулирующее решение

Одним из подходов для решения проблем обеспечения безопасности и управления рисками сложных систем является использование различных теоретико-игровых моделей, в том числе, на основе арбитражных схем [1-3]. В рамках указанного подхода предполагается, что субъект, которого мы будем называть в дальнейшем «защитник», осуществляет управление рисками системы путем эффективного распределения имеющегося в его распоряжении однородного ресурса между ее элементами.

В работе [1] было показано, что в случае, когда функции локальных рисков элементов системы являются детерминированными, а взаимное влияние элементов друг на друга отсутствует (элементы являются «независимыми»), для нахождения эффективного распределения ресурса может быть использована *арбитражная схема, основанная на принципах стимуляции и неподавления* (МС-решение). В работах [2,3] был рассмотрен случай, когда элементы системы являются «зависимыми» и могут оказывать на локальные риски друг друга определенное

воздействие. В этом случае, для нахождения решения был предложен другой подход с использованием *игры на когнитивной карте* («когнитивная игра»).

В настоящей работе указанный подход получает дальнейшее развитие и обобщается на случай, когда элементы системы являются «независимыми», а функции локальных рисков являются, вообще говоря, *случайными функциями*.

Общая арбитражная схема

Рассмотрим множество $I = \{I_k\},\ k \in N = \{1, \dots, n\}$, элементы которого будем называть *игроками* и соответствующий им класс $\mathcal{M} = \{A\}$ кооперативных игр, где каждая игра отождествляется с множеством возможных «выигрышей» ее участников:

$$A = \{a = (a_1, \dots, a_n) : a_i \geq 0, i \in N\} \subset \mathbb{R}_+^n \qquad (1)$$

Зададим на $\mathcal{M}$ некоторое частичное упорядочение относительно предпочтения $\succcurlyeq$.

Обозначим $p = (p_1, \dots, p_n)$ некоторую перестановку чисел $\{1, \dots, n\}$ и предположим, что класс $\mathcal{M}$ разбит на пересекающиеся подклассы $\mathcal{M}_p$ такие, что при $A \in \mathcal{M}_p$ «вклад» в игру p_1-го игрока «не меньше» «вклада» p_2-го, «вклад» p_2-го игрока «не меньше» «вклада» p_3-го игрока и так далее. Обозначим $\mathcal{M}_0 = \bigcap_p \mathcal{M}_p$ и

$$\mathcal{B} = \left\{b = (b_1, \dots, b_n) : b_i = b_j, i, j \in N, i \neq j\right\} \subset \mathbb{R}_+^n \qquad (2)$$

– биссектрису в $\mathbb{R}_+^n$.

Решением для игр из класса $\mathcal{M}$ будем называть определенную на $\mathcal{M}$ вектор-функцию множеств $\pi(A) = (\pi_1(A), \dots, \pi_n(A))$ такую, что для любого $A \in \mathcal{M}$ вектор $\pi(A) \in A$ и $\pi_k(A)$, $k \in N$ – выигрыш k-го игрока в игре $A \in \mathcal{M}$. Таким образом, решение $\pi(A)$ является *селектором* $A \in \mathcal{M}$.

Обозначим $\bar{A}$ – замыкание множества A, $\delta(A)$ – границу множества A, $\Pi(A)$ – оптимальную по Парето границу множества

$A \in \mathcal{M}$, $e(A) = \Pi(A) \cap \mathcal{B}$ – *равномерный селектор*.

Определим класс $\mathcal{P}$ «стимулирующих» селекторов $\pi(A)$ со следующими свойствами:

C1: для любого $A \in \mathcal{M}$: $\pi(A) \in \Pi(A)$.

C2: для любых $A_1 \in \mathcal{M}$ и $A_2 \in \mathcal{M}$ таких, что $A_1 \succcurlyeq A_2$:

$\pi(A_1) \geq \pi(A_2)$, то есть, $\pi_k(A_1) \geq \pi_k(A_2)$, $k \in N$ и существует $j \in N$ такое, что $\pi_k(A_1) > \pi_k(A_2)$.

С3: для любого $A \in \mathcal{M}_p$: $\pi_{p_1}(A) \geq \pi_{p_2}(A) \geq \cdots \geq \pi_{p_n}(A)$ (в частности: если $A \in \mathcal{M}_0$: $\pi_{p_1}(A) = \pi_{p_2}(A) = \cdots = \pi_{p_n}(A)$, иначе: $\pi(A) \in \mathcal{B}$).

Класс $\mathcal{P}$ может содержать много селекторов и необходимо выделить среди них один, в некотором смысле наиболее эффективный. Отметим, что без каких-либо дополнительных предположений о классе $\mathcal{M}$ класс $\mathcal{P}$ может оказаться пустым.

Рассмотрим сначала случай двух игроков p_1 и p_2, и определим понятие МС-селектора.

Определение 1. Пусть $A \in \mathcal{M}_p$, тогда назовем селектор $\hat{\pi}(A) \in A$ «максимально стимулирующим» (МС-селектором) если:

1) $\hat{\pi}(A) \in \mathcal{P}$;
2) $\hat{\pi}_{p_1}(A) = \sup\limits_{\pi(A) \in \mathcal{P}} \pi_{p_1}(A)$.

В этих условиях справедливо следующее утверждение, которое существенно обобщает соответствующие предложения в [4, 5], хотя методика доказательства отличается очень мало.

Утверждение 1. Пусть класс $\mathcal{P}$ не пуст и множества $A \in \mathcal{M}$ замкнуты, тогда МС-селектор существует и единственен.

Доказательство опускаем.

Перейдем теперь к общему случаю.

Определение 2. Пусть $A \in \mathcal{M}_p$, тогда назовем селектор $\hat{\pi}(A) \in A$ «максимально стимулирующим» (МС-селектором) если:

1) $\hat{\pi}(A) \in \mathcal{P}$;
2) $\hat{\pi}_{p_1}(A) = \sup\limits_{\pi(A) \in \mathcal{P}} \pi_{p_1}(A)$;

$\hat{\pi}_{p_2}(A) = \sup\limits_{\pi(A) \in \mathcal{P}_{p_1}} \pi_{p_2}(A)$;

$\cdots$

$\hat{\pi}_{p_{n-1}}(A) = \sup\limits_{\pi(A) \in \mathcal{P}_{p_1 \ldots p_{n-2}}} \pi_{p_{n-1}}(A)$, где

$\mathcal{P}_{p_1 \ldots k} = \left\{\hat{\pi}(A) : \hat{\pi}(A) \in \mathcal{P}, \pi_{p_1}(A) = \hat{\pi}_{p_1}(A), \ldots, \pi_{p_k}(A) = \hat{\pi}_{p_k}(A)\right\}$

Обозначим $V_+^0 = \{v = (v_1, \ldots, v_n) : v_i > 0, i \in N\}$ и

$K(A) = \overline{\delta(A) \cap V_+^0}$ – замыкание границы множества $A \in \mathcal{M}$ в положительном ортанте пространства V_+^0.

Предположим, по аналогии с [4,5], что множества $A \in \mathcal{M}$ с введенным на нем предпочтением $\succcurlyeq$ удовлетворяют следующим требованиям:

T1: $A \in \mathcal{M}$ – компактно;

T2: $(0,\dots,0) \in A$;

T3: любая исходящая из точки $(0,\dots,0) \in \mathbb{R}^n$ уходящая в бесконечность непрерывная кривая ℓ пересекает $K(A)$;

T4: $K(A) \subset \Pi(A)$;

T5: если $B \succcurlyeq A$, то $B \supseteq A$, где знак «$\supseteq$» означает, что множество B содержит множество A или совпадает с ним.

Справедливо следующее утверждение (доказательство опускаем), которое в обобщенной постановке становится почти тривиальным.

Утверждение 2. Класс $\mathcal{P}$ не пуст.

Перейдем, теперь, к общему случаю. Поскольку непосредственное обобщение Утверждения 2 на случай 3-х и более игроков невозможен (это связано с возможным нарушением монотонности по совокупности 2-й, 3-й и т.д. координат) наша задача сводится к поиску дополнительных (и не очень жестких) условий на множества $A \in \mathcal{M}$, которые обеспечили бы существование хотя бы одного монотонного селектора при переходе от n-мерной к $(n-1)$-мерной задаче.

Пусть заданы произвольные множества $A \subset \mathbb{R}^k_+$, $B \subset \mathbb{R}^k_+$, $k \in N = \{1,\dots,n\}$. Будем писать, что $A \supsetneq B$, если: $A \supset B$ и

$K(A) \cap K(B) = \emptyset$.

Для любых $A \subset \mathbb{R}^n_+$ и $k \in \{1,\dots,n-1\}$ выделим в $\mathbb{R}^n_+$ семейство плоскостей вида $V_i^0(a_i) = \{v = (v_1,\dots,v_n): v_i = a_i > 0, i \in N\} \subset \mathbb{R}^n_+$. Обозначим $A_I(a_1,\dots,a_k)$, где $I = \{(i_1,\dots,i_k): i_m, i_l \in N, i_m \neq i_l\}$, проекцию сечения множества A плоскостями вида $V_i^0(a_i)$ на пространство, образованное оставшимися $(n-k)$ координатами.

Для любых $A \in \mathcal{M}$, $B \in \mathcal{M}$ обозначим:

$$\Delta_{inf}(A,B) = \inf_{x \in B, y \in A} |x - y| \tag{3}$$

и

$$\Delta_{sup}(A,B) = \sup_{y \in A} \Delta_{inf}(y,B) \tag{4}$$

Предположим, что в дополнение к требованиям T1-T5 выполнено требование:

T6: если $A \in \mathcal{M}$, $B \in \mathcal{M}$ и $B \succcurlyeq A$, то для любых $k \in \{1,\dots,n-2\}$,

$I = \{(i_1, \dots, i_k): i_m, i_l \in N, i_m \neq i_l\}$,$(x_1, \dots, x_k) \in \mathbb{R}_+^k$, $(y_1, \dots, y_k) \in \mathbb{R}_+^k$ таких, что множества $B_I(x_1, \dots, x_k)$ и $A_I(y_1, \dots, y_k)$ не пусты, выполнено одно из следующих соотношений:

а) $B_I(x_1, \dots, x_k) \subsetneqq A_I(y_1, \dots, y_k)$;

б) $B_I(x_1, \dots, x_k) \supsetneqq A_I(y_1, \dots, y_k)$;

в) $B_I(x_1, \dots, x_k) = A_I(y_1, \dots, y_k)$.

В этих условиях оказываются справедливыми следующее утверждение о существовании и единственности МС-селектора в общем виде (ОМС-селектора).

Утверждение 3. Пусть $A \in \mathcal{M}_p$ (для простоты будем полагать, что $p = (1, 2, \dots, n)$) и выполнены условия Т1-Т6, тогда МС-селектор $\hat{\pi}(A) \in A$ существует и единственен.

Заключение

В работе рассматривается общая модель сложной системы, в рамках которой взаимодействуют два субъекта: природа и игрок. Каждый из субъектов осуществляет воздействие на сеть путем распределения имеющегося в его распоряжении ресурса между ее узлами. Для обобщения подхода вводится понятие обобщенной арбитражной схемы, основанной на принципах стимуляции и неподавления и доказывается существование и единственность обобщенного МС-решения.

Литература:

1. *Калашников А.О., Аникина Е.В.* Модели управления информационными рисками сложных систем // Информация и безопасность. – 2020. – №2(4). Т. 23. – С. 191-202.

2. *Kalashnikov A.O., Anikina E.V.* Management of Risks for Complex Computer Network/Proceedings of the 23rd International Conference on Distributed Computer and Communication Networks: Control, Computation, Communications (DCCN-2020, Moscow). – Cham: Springer. – 2020. – Vol. 1337. – P. 144-157.

3. *Калашников А.О., Аникина Е.В.* Управление информационными рисками сложной системы с использованием механизма «когнитивной игры» // Вопросы кибербезопасности. – 2020. – № 4(38). – С. 2-10.

4. *Калашников А.О.* Модели и методы организационного управления информационными рисками корпораций. – М.: «Эгвес», 2011. – 312 с.

5. *Ротарь В.И.* О принципе стимуляции в арбитражной схеме // Экономика и математические методы. – 1981. – Т. XVII. Вып. 4. – С. 751-764.

Карпов С.Ю., Прус Ю.В.

Информационно-аналитическая модель профессионального выбора кандидатов на должность дознавателя МЧС России

Аннотация: Наибольшую сложность в принятии управленческого решения по выбору сотрудника происходит в направлениях, где работа связана с интеллектуальной деятельностью, в результате которой принимаются, например, процессуальные решения. К такой деятельности относится работа дознавателя МЧС России. Актуальность кадрового потенциала в вопросах обеспечения пожарной безопасности и эффективности расследования пожаров, связана, в том числе, с запросом общества на качественное и своевременное расследование пожаров. Поэтому, руководителю структурного подразделения, как и организации в целом необходимы современные алгоритмы и модели поддержки принятия управленческих решений при выборе кандидатов на должность дознавателя МЧС России.

Ключевые слова: ресурсообеспечение, дознаватель, пожар, управление кадрами, алгоритм выбора сотрудника, расследование пожара, модель

В условиях оптимизации структуры органов исполнительной власти, вопросы кадрового потенциала приобретают стратегическую значимость. Эти вопросы актуальны и при выборе сотрудников МЧС России. Одна из важнейших задач государства – это обеспечение пожарной безопасности, которая решается, в том числе, через качественное и своевременное установление причин пожаров. Деятельность по расследованию пожаров в большей степени относиться к интеллектуальной сфере. Поэтому выбор кандидата (сотрудника) на вакантную должность предусматривает более сложный подход и логический анализ, в отличие, например,

от работника производства, где есть количественные показатели его деятельности и нормативы их выработки.

Правоприменительная деятельность дознавателя МЧС России связана с установлением истины, которая основывается на принципах справедливости, независимости, объективности, беспристрастности и соблюдения прав человека. Деятельность дознавателя по делам о пожарах, с учетом специфики расследования, подразумевает наличие у него достаточных знаний и компетенции в области права и «пожарного дела». То есть знаний, которые необходимы для производства расследования, составления процессуальных документов, вынесения объективного решения по делу, закономерностях развития пожара, изменения свойств веществ и материалов и т.п. Следует учитывать и то, что сотрудник работает в сложных условиях и стрессовых ситуациях. Современный дознаватель по делам о пожарах должен обладать пожарно-техническим и юридическим образованием, а также быть эффективным управленцем в своей деятельности.

В настоящее время к дознавателю МЧС России предъявляются общие требования, которые ограничиваются образованием, опытом работы по специальности (направлению подготовки), состоянием здоровья. Так, например, в соответствии с приказом МЧС России от 01.12. 2016 г. № 653 «О квалификационных требованиях к должностям в федеральной противопожарной службе Государственной противопожарной службы», для должностей среднего начальствующего состава, кем может являться дознаватель, – допускается наличие среднего профессионального образования по направлению деятельности. При этом в нормативных документах не прописано, наличие какого именно профиля (специальности) образования должен иметь сотрудник, занимающий конкретную должность. Деятельность по расследованию пожаров требует значительных знаний в разных областях науки и специальностях. Поэтому уровень подготовки должностного лица должен быть высоким и предусматривать наличие образования не ниже высшего пожарно-технического с дополнительной юридической подготовкой. Необходимы концептуально качественные и количественные критерии (компетенции), позволяющие сформировать модель современного «пожарного» дознавателя. Представленная модель выбора

кандидата на должность дознавателя по делам о пожарах позволяет обеспечить поддержку принятия управленческого решения ЛПР (рисунок 1). Модель включает в себя множество критериев и факторов, состоящих из профессиональных компетенций и личностных качеств, а также предпочтений.

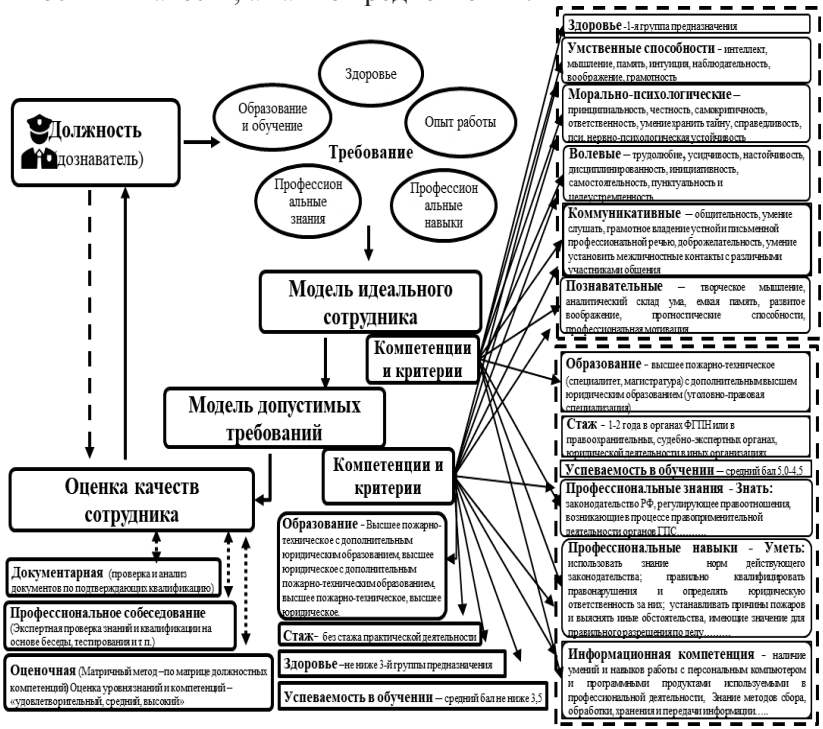


Рисунок 1 – Модель выбора сотрудника на должность дознавателя по делам о пожарах

Решение о назначении на вакантную должность принимается, как правило, коллегиально и зачастую руководителями, которые не имеют достаточных знаний в предметной области, связанной с деятельностью дознавателя. Поэтому при принятии управленческого решения должна быть разработана модель и алгоритм с последующим решением задачи, по которым можно было объективно оценить претендентов и спрогнозировать лучший выбор.

Внедрение алгоритмов и моделей профессионального отбора в деятельность по управлению персоналом позволит оптимально принять решение на основе многокритериального подхода. Для автоматизации процесса анализа критериев и качеств кандидата на должность можно использовать программу системы принятия решений «MPRIORITY 1.0», которая позволит ранжировать множества альтернатив и оказать поддержку принятия решения ЛПР при выборе наилучшего варианта.

В зависимости от рассматриваемой должности и опыта сотрудника требования к компетенциям должны быть дифференцированные. Для молодого специалиста – одни, для более опытного – другие. Не стоит завышать или занижать требования, так как это может привести к некачественному выполнению функций, нужно найти оптимальный вариант.

Решение задачи по выбору кандидата на должность дознавателя можно представить в виде иерархии (рисунок 2). С помощью матрицы попарных сравнений факторов (критериев) определяются приоритеты (таблица 1).

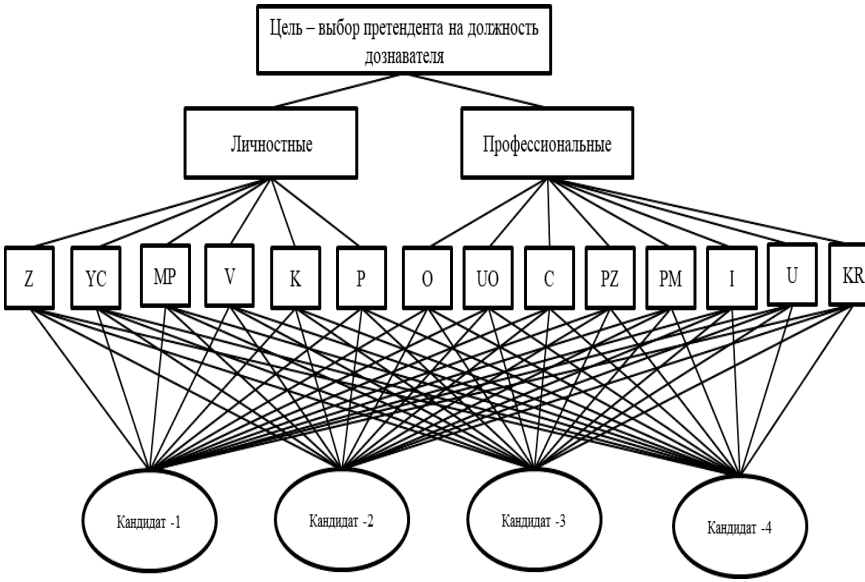


Рисунок 2 – Иерархия задачи прогнозирования результата предпочтения при выборе кандидата на должность дознавателя

Таблица 1 – Критерии и предпочтения

Критерии					
	№	Обозначение	Наименование	Описание	Предпочтение
Личностные	1	Z	health **Здоровье**	1 группа предназначения – виды деятельности: тушение пожаров (сотрудники, принимающие непосредственное участие в тушении пожаров); 2 группа предназначения – виды деятельности: тушение пожаров (сотрудники, обеспечивающие тушение пожаров); 3 группа предназначения – личный состав органов и подразделений государственного пожарного надзора, профилактике пожаров, испытательных пожарных лабораторий, судебно-экспертных учреждений	Предпочтение – 1 группа предназначения. Допускается 2, 3 группа предназначения
	2	YC	Mental abilities **Умственные способности**	Интеллект, мышление, память, интуиция, наблюдательность, воображение, грамотность (тестирование умственных способностей и способностей к анализу текстовой, числовой и логической информации)	Предпочтение – высокий уровень. Допускается – средний уровень
	3	MP	Moral and psychological **Морально-психологические**	Принципиальность, честность, самокритичность, ответственность, умение хранить тайну, справедливость, нервно-психологическая устойчивость (тестирование психологических особенностей, личностных качеств и психотипа)	Предпочтение – высокий уровень. Допускается – не ниже среднего уровня
	4	V	Strong - willed **Волевые**	Трудолюбие, усидчивость, настойчивость, дисциплинированность, инициативность, самостоятельность, пунктуальность, целеустремленность, работоспособность в трудных условиях	Предпочтение – без дисциплинарных взысканий. Допускается – незначительные дисциплинарные проступки

	5	K	Communicative **Коммуникативные**	Общительность, умение слушать, грамотное владение устной и письменной профессиональной речью, доброжелательность, умение устанавливать межличностные (психологические) контакты с различными участниками общения, умение использовать психотехнологии и психотехники в конфликтных ситуациях при расследовании пожаров	
	6	P	Cognitive- prognastic **Познавательно-прогностические**	Творческое мышление, аналитический склад ума, емкая память, развитое воображение, прогностические способности, профессиональная мотивация	
Профессиональные	1	O	Education **Образование**	Высшее профессиональное образование	Предпочтение – высшее пожарно-техническое (специалитет, магистратура) с дополнительным высшим юридическим образованием (уголовно-правовая специализация). Допускается – высшее пожарно-техническое с дополнительным юридическим образованием или высшее юридическое с дополнительным пожарно-техническим образованием. Минимальный – высшее пожарно-техническое или высшее юридическое

	2	UO	Academic performance **Успеваемость в обучении**	Определяется средний бал успеваемости по оценкам в дипломах	Предпочтение – средний бал (5,0-4,5). Допускается средний бал (4,4-4,0). Минимальный средний бал (3,9-3,5)
	3	C	Experience **Стаж**	Опыт работы по расследованию преступлений сопряженных с пожарами	Предпочтение – стаж работы не менее 1-2 года в органах ФГПН или в правоохранительных, судебно-экспертных органах, юридической деятельности в иных организациях. Допускается – без стажа практической деятельности
	4	PZ	Professional knowledge **Профессиональные знания**	Знать: законодательство РФ, регулирующее правоотношения, возникающие в процессе правоприменительной деятельности органов Государственной противопожарной службы; правовую квалификацию преступлений и других правонарушений по делам, связанным с пожарами и требованиями пожарной безопасности; правовые аспекты и процессуальный порядок проверки сообщений о пожаре и возбуждении уголовных дел, порядок направления материалов по подследственности или подсудности; порядок регистрации и учета пожаров; права и обязанности	

				сотрудников органа дознания в сфере уголовного судопроизводства; криминалистические методики и тактики расследования преступлений, связанных с пожарами; тактику и технологию проведения осмотра места пожара и отдельных предметов, порядок изъятия вещественных доказательств; порядок выдвижения и проверки версий о причине возникновения пожара и обстоятельствах, влияющих на развитие и распространение горения; методы и методики исследования конструкций, предметов, веществ и материалов на месте происшествия и в лабораторных условиях; систему следов и признаков, образующихся при возникновении и развитии пожара, служащих источниками информации об обстоятельствах пожара; порядок организации взаимодействия с правоохранительными органами при расследовании преступлений, связанных с пожарами; порядок производства административного расследования по делам о нарушениях противопожарных	
	5	PN	Professional skills **Профессиональные навыки**	Уметь: использовать знание норм действующего законодательства; правильно квалифицировать правонарушения и определять юридическую ответственность за них; устанавливать причины пожаров и выяснять иные обстоятельства, имеющие значение для правильного разрешения по делу; принимать, регистрировать и проверять	

				сообщения о пожарах; возбуждать и отказывать в возбуждении уголовного дела, передавать дела по подследственности; проводить дознание по пожарам; производить неотложные следственные действия и выполнять отдельные поручения по уголовным делам; проводить административное расследование по делам о пожарах и нарушениях ТПБ; выявлять и принимать меры по устранению причин и условий, способствовавших возникновению и развитию пожара; обрабатывать, анализировать и систематизировать информацию, получаемую при расследовании правонарушений, связанных с пожарами; взаимодействовать в установленном порядке с другими правоохранительными органами при расследовании преступлений; назначать пожарно-техническую и другие виды экспертиз; принимать решение по результатам проверки по факту пожара о возбуждении или отказе в возбуждении уголовного дела; проводить осмотр и описание места пожара, изъятие вещественных доказательств; проводить иные следственные действия; готовить процессуальные документы по расследуемому факту пожара; направлять материалы уголовного дела по подследственности или подсудности; проводить анализ следственных и экспертных версий при расследовании пожара; описывать и исследовать вещественные доказательства	

				при установлении их информативности об обстоятельствах возникновения и развития пожара; участвовать в расследовании и судебном рассмотрении уголовных дел в качестве специалиста, эксперта, лица, поддерживающего обвинение, составлять обвинительный акт	
	6	I	Information competence **Информационная компетенция**	Наличие умений и навыков работы с персональным компьютером и программными продуктами, используемыми в профессиональной деятельности. Знание методов сбора, обработки, хранения и передачи информации; уметь планировать информационный поиск, систематизировать и структурировать информацию и делать выводы	
	7	U	Organizational and managerial **Организационно-управленческие**	Самоорганизованность, организаторские способности, требовательность, собранность, целеустремленность, мобильность, умение вести диалог с людьми разных уровней и возрастов, умение ставить цели и задачи, умение брать ответственность за принятые решения	
	8	KR	Corporate **Корпоративные**	(на основе общепринятых ценностей и кодексов организации), например, способность к исполнительной деятельности, коммуникативность, адаптивность к изменениям, самоотверженность, стремление к профессиональному развитию	

Литература:

1. *Карпов С.Ю.* Определение факторов и критериев оценки деятельности дознавателя МЧС России на основе экспертного метода // Технологии техносферной безопасности. – 2019. – №4 – С. 87-95.

2. *Зинченко А.А.* Количественные моделирование процесса подбора персонала // Управленческие науки. – 2015. – №3 – С. 70-75.

3. *Беллман Р., Заде Л.* Принятие решений в расплывчатых условиях / Вопросы анализа и процедуры принятия решений. – М.: Мир, 1976. – С. 172-215.

4. *Судаков В.А., Сивакова Т.В.* Поддержка принятия решений для подбора персонала на основе нечеткой логики // Плехановский научный бюллетень. – 2020. – № 2(18). – С. 106-118.

5. *Абакаров А.Ш., Сушков Ю.А.* Программная система поддержки принятия решений «MPRIORITY 1.0» // Электронный журнал «Исследовано в России». – 2005. – № 8. – С. 2130-2146. – URL: http://zhurnal.ape.relarn.ru/articles/2005/207.pdf (дата обращения 14.10.2020).

6. *Томас Л. Саати* Об измерении неосязаемого. Подход к относительным измерениям на основе главного собственного вектора матрицы парных сравнений. – Cloud of Science. – 2015. – Т. 2. №1. – С. 5-39. – URL: https://www.elibrary.ru/item.asp?id=23174572 (дата обращения 14.10.2021).

7. *Зуев Л.Ю.* Личностные и профессионально важные качества как основа профессиональной компетенции дознавателя // Психопедагогика в правоохранительных органах. – 2009. – № 1 (36). – С. 17-19.

Кловач Е.В., Ткаченко В.А.

Об обосновании использования аудита промышленной безопасности

Аннотация: Представлены аргументы необходимости расширения ряда элементов регулирования промышленной безопасности. С использованием математического аппарата теории управления приведено обоснование возможности использования аудита в этих целях. Сделан вывод о том, что наличие новых элементов регулирования позволит повысить общий уровень промышленной безопасности.

Ключевые слова: элемент регулирования, промышленная безопасность, аудит

Стремление обеспечить необходимый уровень безопасности таких сложных систем, как действующие организации, эксплуатирующие опасные производственные объекты, и постоянно повышать уровень этой безопасности приводит заинтересованные стороны к поиску новых способов достижения этой цели. Среди возможных нововведений в этой области управления рассматривается возможность использования аудита в сфере промышленной безопасности. Проводится подготовительная работа, на практике отрабатываются механизмы его применения [1], но помимо этого необходимо и, по возможности, научное обоснование его использования, чему и посвящена настоящая работа.

При этом обосновании использована терминология из области общей теории управления организационными системами [1], к коим, безусловно, можно отнести и модель взаимодействия «государство» – «организации, эксплуатирующие опасные производственные объекты» на более высоком уровне, и «системы управления промышленной безопасностью в организациях, эксплуатирующих опасные производственные объекты» на более низком [2].

Пусть «Центр» – госрегулятор в области промышленной безопасности (Ростехнадзор), который определяет и внедряет через нормативное регулирование элементы управления промышленной

безопасностью в части осуществления контрольных и надзорных функций.

Агент – организация, эксплуатирующая опасные производственные объекты (далее – **АГ**).

y – действия, которые может осуществлять **АГ** исходя из того, что ему предоставляет и позволяет Центр.

Тогда **A** – множество возможных действий **АГ** – то бишь, по сути, набор возможностей использования элементов регулирования, предоставляемых и регулируемых Центром (внедрение систем управления, осуществление производственного контроля, дистанционный контроль, аудит промышленной безопасности и т.д.). При этом, $\mathbf{y} \in \mathbf{A}$.

z – результат внедренных действий (после осуществления **АГ** действий **y** из множества **A** под влиянием обстановки), другими словами, полученный результат от использования того или иного элемента регулирования, будь он окончательный, или промежуточный.

Тогда $\mathbf{A_0}$ – множество возможных результатов **АГ** (рост/снижение аварийности, рост/снижение количества инцидентов, поддержание уровня промышленной безопасности на прежнем уровне, рост/снижение затрат на обеспечение промышленной безопасности и т.д.). Конечно же, $\mathbf{z} \in \mathbf{A_0}$. Важно отметить, что множество $\mathbf{A_0}$ по сути является стабильным по своему составу в отличие от множества **A**, которое может пополняться и расширяться за счет внедрения Центром новых элементов регулирования промышленной безопасности.

Возможное несовпадение действия **АГ** и результата его деятельности может быть обусловлено влиянием обстановки – внешней среды, действий других участников ОС (здесь и далее – организационная система) (другие надзорные органы, поставщики услуг (например, аудит промышленной безопасности)) и т.д.).

$\mathbf{R_{A0}}$ – предпочтение **АГ** из всего множества возможных результатов. Множество возможных предпочтений **АГ** тогда – $\mathfrak{R}_{\mathbf{A0}}$ (снижение аварийности, снижение количества инцидентов, развитие системы управления промышленной безопасностью, снижение затрат на обеспечение промышленной безопасности и т.д.). Это подмножество формируется вполне примитивным естественным образом.

Предпочтения из множества $\mathfrak{K}_{A0}$ **АГ** можно параметризировать переменной **r**, принимающей значения из подмножества **Ω** действительной оси, $\Omega \in R^1$. То есть множество $\mathfrak{K}_{A0}$ **АГ** параметризируется множеством переменных r_1, r_2, r_3 и т.д. В рассматриваемом случае переменной будет являться количественный параметр промышленной безопасности, который сразу или же путем итераций должен привести к целевому показателю, назначаемому Центром и принимаемому **АГ** – задаваемый уровень промышленной безопасности (будь то организации, региона, страны). Получаем, что общая цель в области промышленной безопасности (**Ц$_{ПБ}$**) для Центра есть сумма предпочтений из множества предпочтительных результатов всех **АГ** $Ц_{ПБ} = \sum R_{A0}$.

При выборе действия $y \in A$ **АГ** руководствуется своими предпочтениями (в том числе и используемым параметром) и тем, как выбираемое действие влияет на результат деятельности $z \in A_0$, то есть некоторым законом $W_I(\times)$ изменения результата деятельности в зависимости от действия (форма реализации в конкретном **АГ**, выбор поставщиков услуг, компетентность собственного персонала **АГ**, компетентность инспекторского состава Центра, качество оборудования и программного обеспечения, и т.д.) и обстановки, информация о которой отражена переменной **I** (в нее входит информация и о самом элементе регулирования, механизме его использования, ранее полученных результатах у аналогичных **АГ**, возможных вариантах использования и т.д.). Выбор действия агентом определяется правилом индивидуального рационального выбора P^{WI} ($\mathfrak{K}_{A0}$, **A**, **I**) $\in$ **A**, которое выделяет множество наиболее предпочтительных, с точки зрения **АГ**, действий. Предпочтение определяется, в том числе, и наличием тщательной нормативной проработки каждого элемента регулирования промышленной безопасности со стороны Центра.

Таким образом то, что выберет **АГ**, зависит от наличия этого элемента регулирования промышленной безопасности, как такового, массива информации, а также от того, что благодаря именно этому элементу регулирования **АГ** хочет, и может на основе ранее полученного у других **АГ** результата, достичь.

Правило индивидуального рационального выбора определим следующим образом. Примем две гипотезы:

1) гипотезу рационального поведения, заключающуюся в том, что **АГ** с учетом всей имеющейся у него информации выбирает действия, которые приводят к наиболее предпочтительным результатам деятельности;

2) гипотезу детерминизма, заключающуюся в том, что **АГ** стремится устранить (с учетом всей имеющейся у него информации) существующую неопределенность и принимать решения в условиях полной информированности (другими словами, окончательный критерий, которым руководствуется лицо, принимающее решения (ЛПР), – примем его за руководителя **АГ**, то есть организации, эксплуатирующей опасные производственные объекты, – не должен содержать неопределенных параметров).

Существуют несколько способов задания индивидуальных предпочтений. Наиболее распространены два из них: отношения предпочтения (полученного сиюминутного результата благодаря использованию элемента регулирования) и функции полезности (вклада полученного сиюминутного результата благодаря использованию элемента регулирования в интегральное достижение единой конечной цели $\mathbf{Ц_{ПБ}}$). Бинарное отношение определяет для пары альтернатив, какая из них является «лучше»; функция полезности ставит в соответствие каждой альтернативе действительное число – полезность этой альтернативы. В соответствии с гипотезой рационального поведения **АГ** выбирает альтернативу из множества «лучших» альтернатив. В случае функций полезности это множество является множеством альтернатив, на которых достигается максимум функции полезности (то есть минимальности пути достижения конечной цели $\mathbf{Ц_{ПБ}}$).

Итак, речь идет о «наилучшей» альтернативе. Но, если предпочтения **АГ** определены на множестве результатов деятельности, зависящих, помимо его действий, от обстановки (а это так, потому как в деятельность по обеспечению промышленной безопасности вклиниваются экономические аспекты (падение/рост валют), технологические (внедрение нового оборудования/новой технологии в **АГ**), форс-мажорные (актуальный пример с пандемией), появление новых «вводных» со стороны Центра, и

т.д.), то в общем случае не существует однозначной связи между действием **АГ** и результатом его деятельности. Поэтому, принимая решение о выбираемом действии, **АГ** должен *предсказывать*, к каким результатам могут привести те или иные действия (здесь существенна та информация, которую он имеет относительно обстановки, включая информацию об «использовании» элемента регулирования – то бишь, «нормальных», однозначно трактуемых, понятных, детальных требований, установленных Центром, а также информация о полученном опыте использования конкретного элемента регулирования), и анализировать предпочтительность соответствующих результатов деятельности.

При рассмотрении математических моделей принятия решений будем различать (основание классификации – объекты и субъекты, относительно которых имеется недостаточная информация) объективную неопределенность, носящую в том числе и прогнозную составляющую (неполная информированность относительно параметров обстановки (экономические аспекты (падение/рост валют), технологические (внедрение нового оборудования/новой технологии в **АГ**), форс-мажорные и т.д.)) и субъективную неопределенность (неполную информированность о принципах поведения других субъектов (появление новых «вводных» со стороны Центра, «поведение» подрядчиков по предоставлению услуг, наличие их как таковых, качество оказываемых ими услуг, и т.д.)).

Будет использовать следующую модель предпочтений и информированности **АГ**. Пусть предпочтения **АГ** на множестве возможных результатов деятельности заданы его функцией полезности $\mathbf{v}(\times)$, а результат деятельности $\mathbf{z} \in \mathbf{A}_0$ зависит от действия $\mathbf{y} \in \mathbf{A}$ и обстановки $\boldsymbol{\theta} \in \boldsymbol{\Theta}$ известным образом (использование такого описания не снижает общности, так как в многоэлементных системах партнеры (государство, поставщики, конкуренты, кредиторы, владельцы) каждого **АГ** могут рассматриваться как внешняя для него среда и их стратегии будут образовывать «состояние природы» (которое, правда, будет для каждого из **АГ** свое)): $\mathbf{z} = \mathbf{w}(\mathbf{y}, \boldsymbol{\theta})$. Тогда закон $\mathbf{W}_1(\times)$ определяется функцией (отображение, связывающее действия и обстановку с результатами деятельности, может рассматриваться как «технология» функционирования некоторого объекта, управление

которым осуществляет **АГ** (что, собственно, есть ничто иное, как непосредственное функционирование соответствующего структурного подразделения **АГ**, регламентированное внутренними документами **АГ**, разработанными на основе, в том числе, установленных Центром требований)) **w(×)**, отражающей структуру управляемого объекта и той информацией **I**, которой обладает **АГ** на момент принятия решений о выбираемом действии.

Исходя из принципов гипотезы детерминизма, в целях достижения максимального гарантированного результата **АГ**, устраняя неопределенность, переходит от предпочтений, зависящих от неопределенных факторов, к предпочтениям, зависящим от его собственных действий, – к индуцированным предпочтениям. То есть **АГ** выбирает те действия, которые являются наилучшими с точки зрения его индуцированных предпочтений, и стремится этим выбором действия максимизировать свою целевую функцию.

Таким образом, приходим к выводу, что чем больше у **АГ** вариантов использования различных элементов регулирования промышленной безопасности, включая и аудит, тем больше вероятность достижения большинства предпочтимых результатов, которые интегрально дадут достижение цели в области промышленной безопасности и для **АГ**, и для Центра. При этом действие информационной неопределенности минимизируется максимумом нормативного регулирования использования этих элементов со стороны Центра, то есть, по возможности, приближает **АГ** к случаю детерминированного изменения результата деятельности – когда он не зависит от обстановки, когда каждому действию $\mathbf{y} \in \mathbf{A}$ соответствует единственный результат деятельности, что позволяет максимально быстро добиться факта достижения цели.

Литература:

1. *Селезнев Г.М., Ермошин В.А., Грибков А.Б., Галяутдинов А.В., Кручинина И.А. Ткаченко В.А.* Опыт комплексного обследования состояния опасных производственных объектов на примере АО «Апатит» // Безопасность труда в промышленности. – 2020. – № 2 – С. 62-66.

2. *Новиков Д.А.* Теория управления организационными системами. – М.: МПСИ, 2005. – 584 с.

3. *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.

Скворцов О.Б.

Стандартизация и нормирование вибрационной усталости механизмов и машин

Аннотация: Представлен критический анализ действующих нормативно-правовых документов и принятых в них методик оценки влияния вибрации на состояние сложного технического оборудования. Обоснована необходимость учета высокочастотных вибрационных составляющих с частотами, как правило, выходящими за диапазон контроля типовых современных систем непрерывного вибрационного мониторинга машин и механизмов.

Ключевые слова: вибрация, мониторинг, противоаварийная защита, диагностика, усталость, ускорение

Введение

Начиная с международного стандарта ISO 2372, в настоящее время замененного на серию стандартов в более новых редакциях, и до ГОСТ Р 56646-2015 и современного ГОСТ ИСО 8528-9-2021 для оценки вибрации машин и механизмов принято использовать среднеквадратичные значения интенсивности вибрационной скорости. Такие оценки позволяют оценить текущее значение уровня вибрации оборудования и ориентированы на решение задачи вибрационной диагностики. Такой подход не гармонизирован с нормативными документами и методиками оценки влияния вибрации на надежность, а также работоспособность конструкционных материалов и оборудования при их испытаниях на вибрационные нагрузки. При таких испытаниях важен не только уровень интенсивности вибрации, но и ее продолжительность ее воздействия. Как отмечено в [1], ориентация на оценки интенсивности вибрационной скорости или вибрационного

перемещения не позволяет оценить влияние динамических сил на проявление циклической усталости при действии вибрационных нагрузок. При оценках по интенсивности перемещений и скорости из-за кинематических особенностей практически полностью теряется информация о влиянии высокочастотных вибрационных составляющих.

Присутствие высокочастотных составляющих [2] в реальных вибрационных сигналах от акселерометров, устанавливаемых на сложном роторном оборудовании, оказывает существенное влияние на процессы вибрационной усталости. Экспериментальные исследования прочности металлов в условиях воздействия двухчастотного нагружения [3] показывают, что даже незначительные по амплитуде высокочастотные вибрации резко снижают порог усталостного разрушения. Двухчастотное вибрационное перемещение (деформация) может быть представлено в виде

$$d(t) = D_1 \cdot \sin\left(2\pi f_1 t\right) + D_2 \cdot \sin\left(2\pi f_2 t\right), \quad (1)$$

или в виде вибрационного ускорения

$$a(t) = A_1 \cdot \sin\left(2\pi f_1 t\right) + A_2 \cdot \sin\left(2\pi f_2 t\right), \quad (2)$$

Соответствующие этим соотношениям сигналы перемещения и ускорения представлены на рисунке 1. Из данного рисунка видно, что сигналы совершенно не похожи, хотя и представляют один и тот же вибрационный процесс. В сигнале перемещения практически незаметен вклад высокочастотных составляющих, а в сигнале ускорения незаметно влияние низкочастотной составляющей.

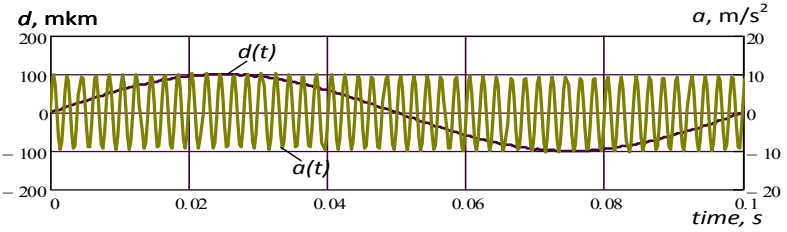


Рисунок 1 – Двухчастотной вибрационный сигнал по перемещению *d(t)* и ускорению *a(t)* при амплитудах перемещении D_1=100 мкм и D_2=1 мкм и частотах f_1=10 Гц и f_2=500 Гц первой и второй частотных составляющих

Такие особенности оказывают существенное влияние не только на внешний вид сигналов. Они оказывают влияние на методику учета влияния воздействия вибрации на надежности оборудования по результатам вибрационного мониторинга.

Методика и обсуждение результатов

Схема контроля вибрации с использованием акселерометра приведена на рисунке 2. Акселерометр 4 обеспечивает контроль величины ускорения *a(t)*, например, в виде соотношения (2). В соответствии с действующими нормативными документами сигнал ускорения *a(t)* преобразуется в сигнал скорости *v(t)*

$$v(t) = \int a(t)dt = \frac{A_1}{2\pi f_1} \cdot \sin\left(2\pi f_1 t\right) + \frac{A_2}{2\pi f_2} \cdot \sin\left(2\pi f_2 t\right) , \quad (3)$$

или перемещения *d(t)*

$$d(t) = \iint a(t)dt^2 = \frac{A_1}{4\pi^2 f_1^2} \cdot \sin\left(2\pi f_1 t\right) + \frac{A_2}{4\pi^2 f_2^2} \cdot \sin\left(2\pi f_2 t\right) , \quad (4)$$

Действующая на элемент 3 крепления детали 1 массой *m* динамическая сила *F* определяется вторым законом Ньютона

$$F(t) = F1(t) + F2(t) = mA_1 \cdot \sin\left(2\pi f_1 t\right) + mA_2 \cdot \sin\left(2\pi f_2 t\right) , \quad (5)$$

Из этого соотношения можно получить оценку динамических механических напряжений для элемента крепления с площадью поперечного сечения *S*

$$\sigma N(t) = \frac{F(t)}{S} . \quad (6)$$

С другой стороны, элемент крепления испытывает деформации в осевом направлении, определяемые соотношением (4). Из этого соотношения можно оценить величину механических напряжений в соответствии с законом Гука

$$\sigma G(t) = E\frac{d(t)}{L} , \quad (7)$$

где E – модуль Юнга материала элемента крепления, L – длина деформируемой части этого элемента.

Для количественной оценки рассмотрим пример крепления шины энергетического гидрогенератора массой m=1 кг при двух частотах: 5 Гц (частота вращения) и 10 КГц (частота гидродинамических колебаний) при величинах вибрационных

скоростей соответствующих предельно допустимому уровню в 11,2 мм/с. Результаты таких оценок приведены в таблице 1. Такие оценки близки к оценкам, получаемым системами мониторинга вибрационного состояния энергетического оборудования [4,5].

Таблица 1 – Оценки механических напряжений для элемента крепления детали массой 1 кг

материал, Vrms	частота, Гц	σG, МПа	σN, МПа
медь	5	553	0,025
11,2 мм/с	10000	2,7	50,5

Полученные оценки показывают, что механические напряжения, связанные с низкочастотными вибрациями, на порядок превышают динамические механические напряжения от инерционных сил и близки к пороговым значениям, при которых наблюдается переход к пластическому характеру деформации материала. Тем не менее, динамические механические напряжения от высокочастотной вибрации составляют заметную часть от механических напряжений деформации. Влияние высокочастотной вибрации при этом может проявляться в виде процесса циклической усталости, описываемого *S-N* диаграммой, представленной на рисунке 2.

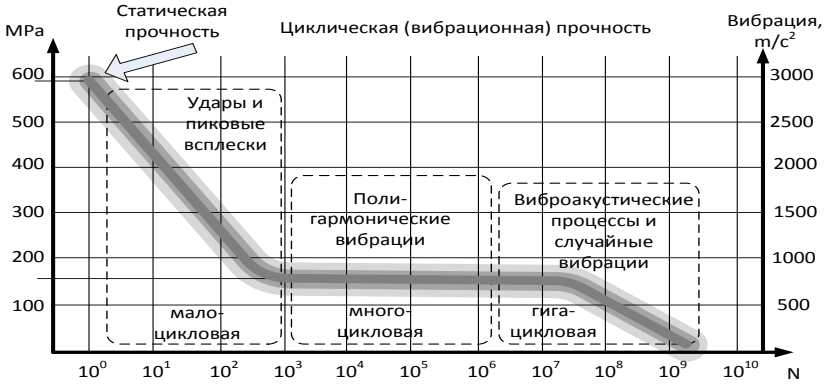


Рисунок 2 – Типовая S-N диаграмма с дополнительной шкалой уровней вибрации в единицах ускорения

При одинаковом времени эксплуатации, высокочастотным вибрациям соответствует существенно большее число циклов нагружения *N*, а в этом случае порог усталости может стать существенно более низким (в том числе и практически на порядок) для случая проявления многоцикловой или гигацикловой усталости.

Представленные в таблице 1 оценки не учитывают возможного проявления на повышенных частотах такого явления как резонансы [6]. Наличие высокочастотных резонансов закрепленных элементов крепления деталей может приводить к существенному росту реально действующих ускорений. На практике подъем уровня вибрации на частоте механического резонанса частот достигает 20-25 дБ. В этом случае механические напряжения, связанные с наличием высокочастотных вибраций могут стать доминирующей причиной вибрационной усталости и при даже относительно малом числе циклов нагружения и времени наработки.

Заключение

При использовании вибрационного мониторинга ответственных элементов конструкции машин и механизмов, таких как, например, шпильки крепления, обеспечивается контроль локальных динамических нагрузок, которые могут приводить к повреждению таких элементов. Такие динамические нагрузки могут быть связаны с вибрациями на повышенных частотах, выходящих за пределы диапазона измерения большинства систем непрерывного вибрационного мониторинга, который, как правило, ограничиваются частотным диапазоном 5-1000 Гц. Учет динамических циклических вибрационных нагрузок их вклада в вибрационную усталость необходимо принимать во внимание при разработке нормативно-правовых требований к аппаратуре вибрационного мониторинга.

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 10.10.2021).

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. 394-416. – URL: https://elibrary.ru/item.asp?id=35451216 (дата обращения 09.10.2021).

4. *Скворцов О.Б.* Вибрационный мониторинг энергетического оборудования и IIoT технологии / Четвертый междисциплинарный научный форум с международным участием «Новые материалы и перспективные технологии» (27-30 ноября 2018 г. Москва): Сборник материалов. Т. I. – 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 // IOP Conference Series: Materials Science and Engineering. – Volume 1005. – 17th International School-Conference "New Materials: Advanced Technologies" (5-8 November 2019 Moscow). – Published under licence by IOP Publishing Ltd, 2020. – P. 012021. – URL: https://iopscience.iop.org/article/10.1088/1757-899X/1005/1/012021/pdf (дата обращения 10.10.2021).

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. Т. 1. – М.: РТУ МИРЭА, 2021. – С. 444-449.

Авторы

Bachtadze N.	ИПУ РАН
Chilachava T.	SSU
Lepeshkin O.M.	MAC
Ostroumov O.A.	MAC
Plotnikov N.I.	SRPCAI «AviaManager»
Pochkhua G.	SSU
Rusetsky A.	CIU
Sinyuk A.D.	MAC
Zaikin O.	Warsaw School of Computer Science
Żylawski A.	Warsaw School of Computer Science
Абдулова Е.А.	ИПУ РАН
Абросимов В.К.	ГНИИМЦ ПВ
Авдеева З.К.	ИПУ РАН
Аникина Е.В.	ИПУ РАН
Анохин А.М.	ИПУ РАН
Асратян Р.Э.	ИПУ РАН
Ахромеева Т.С.,	ИПМ им. М.В. Келдыша РАН
Байрамов О.Б.	ВЦ ФИЦ ИУ РАН
Балакина Е.П.	РУТ (МИИТ)
Баранов Л.А.	РУТ (МИИТ)
Богатырева Л.В.	ИПУ РАН
Боресков Г.К.	ИПУ РАН
Бугайский К.А.	ИПУ РАН
Быстров В.В.	ИИММ КНЦ РАН
Волгина О.А.	ИПУ РАН
Володина Н.Н.	ИНП РАН
Головченко Е.В.	ВУНЦ ВВС «ВВА»
Гончар Д.Р.	ФИЦ ИУ РАН
Горелова Г.В.	ИУЭС ЮФУ
Грабчак Е.П.	Минэнерго России
Грузман В.А.	ИПУ РАН
Гучук В.В.	ИПУ РАН
Датьев И.О.	ИИММ КНЦ РАН
Дашков Р.Ю.	Нефтегазовая компания «Сахалин Энерджи Инвестмент Компани Лтд.»
Дударикov О.Н.	ВУНЦ ВВС «ВВА»

Евдокимова А.В.	ФГАОУ ВО СПбПУ
Жарко Е.Ф.	ИПУ РАН
Жуковская Л.В.	ЦЭМИ РАН
Изотова И.А.	ООО «ТС Цифровые технологии»
Исхаков А.Ю.	ИПУ РАН
Исхаков С.Ю.	ПАО Промсвязьбанк
Кадиев Ш.К.	АГПС МЧС России
Карпов С.Ю.	АГПС МЧС России
Кафидов В.В.	РАНХиГС при Президенте РФ
Кереселидзе Н.Г.	СГУ
Кловач Е.В.	ЗАО НТЦ ПБ
Коврига С.В.	ИПУ РАН
Козлов А.Д.	ИПУ РАН
Комендантова Н.П.	МИПСА
Комков Н.И.	ИНП РАН
Кротова М.В.	ИНП РАН
Кулагин М.А.	АО «ВНИИЖТ»
Кульба В.В.	ИПУ РАН
Курако Е.А.	ИПУ РАН
Лантер Н.Н.	ИНП РАН
Лещенко В.В.	ФГУП НИИР
Логинов Е.Л.	ИНЭС
Логинова Л.Н.	РУТ (МИИТ)
Малинецкий Г.Г.	ИПМ им. М.В. Келдыша РАН
Мамченко М.В.	ИПУ РАН
Маслобоев А.В.	ИИММ КНЦ РАН
Махов А.Н.	АО «НИИП»
Меденников В.И.	ВЦ ФИЦ ИУ РАН
Мелихов А.А.	ООО «Новые Облачные Технологии»
Мельник Э.В.	ИТ и ПУ, ЮНЦ РАН
Мельников А.К.	АО «Вычислительные решения»
Мещеряков Р.В.	ИПУ РАН
Мистров Л.Е.	Центральный филиал РГУП, ВУНЦ ВВС «ВВА»
Муромцев В.В.	РГГУ
Муромцева А.В.	РГГУ
Мусаев В.К.	НИУ МГСУ

Мысак М.Ю.	АО «Россельхозбанк»
Нижегородцев Р.М.	ИПУ РАН
Нога Н.Л.	ИПУ РАН
Овсяников Г.П.	РУТ (МИИТ)
Орда-Жигулина Д.В.	ИТ и ПУ, ЮНЦ РАН
Орда-Жигулина М.В.	ИТ и ПУ, ЮНЦ РАН
Орлов В.Л.	ИПУ РАН
Охапкина Е.П.	РГГУ
Пискурева Т.А.	АО «НИИП»
Полюхович М.А.	СПбПУ
Посашков С.А.	Финансовый университет при Правительстве РФ
Потапова О.А.	ИПУ РАН
Правиков Д.И.	ИБР
Промыслов В.Г.	ИПУ РАН
Прус М.Ю.	РАНХиГС при Президенте РФ
Прус Ю.В.	ВНИИ ГОЧС
Райков А.Н.	ИПУ РАН
Рей А.С.	ИПУ РАН
Ройзензон Г.В.	ИСА ФИЦ ИУ РАН
Саломатин А.А.	ИПУ РАН
Сафронов А.И.	РУТ (МИИТ)
Семенков К.В.	ИПУ РАН
Сивокоз В.Н.	Представительство компании «Сахалин Энерджи Инвестмент Компани Лтд.»
Сидоренко В.Г.	РУТ (МИИТ)
Сидоренко И.А.	ВУНЦ ВВС «ВВА»
Сиротюк В.О.	ИПУ РАН
Скворцов О.Б.	ИМАШ РАН
Смирнов А.М.	МГТУ им. Н. Э. Баумана
Соколов А.В.	ИППИ 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
Тимошенко А.А.	УП РФ
Тисленко А.В.	Представительство компании «Сахалин Энерджи Инвестмент Компани Лтд.»

Ткаченко В.А.	ЗАО НТЦ ПБ
Торгашев Р.Е.	РГГУ
Торопыгина С.А.,	ИПМ им. М.В. Келдыша РАН
Троицкий О.А.	ИМАШ РАН
Усманова Т.Х.	ИНП РАН
Фейзов В.Р.	ИПУ РАН
Фомичев А.Н.	РАНХиГС при Президенте РФ
Фуругян М.Г.	ФИЦ ИУ РАН
Хабибулин Р.Ш.	АГПС МЧС России
Ходырева Н.Е.	ВУНЦ ВВС «ВВА»
Цыганов В.В.	ИПУ РАН
Чернов И.В.	ИПУ РАН
Чернов К.В.	ИГЭУ
Чинакал В.О.	ИПУ РАН
Шелков А.Б.	ИПУ РАН
Широкий А.А.	ИПУ РАН
Шульц В.Л.	ЦИПБ РАН

Сокращения

CIU	Caucasian International University
MAC	Military Academy of Communications
SRPCAI «AviaManager»	Scientific Research Project Civil Aviation Institute «AviaManager»
SSU	Sokhumi State University
АГПС МЧС России	ФГБОУ ВО Академия Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий
АО «ВНИИЖТ»	Научно-исследовательский институт железнодорожного транспорта
АО «НИИП»	Акционерное общество «Научно-исследовательский институт приборов»
АО «Россельхозбанк»	Акционерное общество «Российский сельскохозяйственный банк»
ВНИИ ГОЧС	ФГБУ Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России, федеральный центр науки и высоких технологий
ВУНЦ ВВС «ВВА»	Военный учебный научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е.Жуковского и Ю.А.Гагарина»
ВЦ ФИЦ ИУ РАН	Вычислительный центр им. А.А. Дородницына ФИЦ «Информатика и управление» РАН

ГНИИМЦ ПВ	Главный научно-исследовательский испытательный межвидовой Центр перспективного вооружения Министерства Обороны РФ
ЗАО НТЦ ПБ	Закрытое акционерное общество «Научно-технический центр исследований проблем промышленной безопасности»
ИБР	АО «ИБ Реформ»
ИГЭУ	ФБГОУ ВО Ивановский государственный энергетический университет имени В.И. Ленина
ИИММ КНЦ РАН	Институт информатики и математического моделирования Федерального исследовательского центра «Кольский научный центр Российской академии наук»
ИМАШ РАН	Институт машиноведения им. А.А. Благонравова РАН
ИНП РАН	ФГБУН «Институт народнохозяйственного прогнозирования РАН»
ИНЭС	Институт экономических стратегий
ИПМ им. М.В. Келдыша РАН	Институт прикладной математики им. М.В. Келдыша РАН
ИППИ РАН	Институт проблем передачи информации им. А.А. Харкевича РАН
ИПУ РАН	Институт прикладной математики им. М.В. Келдыша РАН ФГБУН Институт проблем управления им. В.А.Трапезникова РАН
ИСА ФИЦ ИУ РАН	Институт системного анализа Федерального исследовательского центра «Информатика и управление» РАН

ИТ и ПУ, ЮНЦ РАН	Южный научный центр РАН
ИУЭС ЮФУ	Институт управления в экономических, социальных и экологических системах Южного федерального университета
МГТУ им. Н. Э. Баумана	Министерство науки и высшего образования «Московский государственный технический университет им. Н. Э. Баумана» (национальный исследовательский университет)
Минэнерго России	Министерство энергетики Российской Федерации
МИПСА	Международный институт прикладного системного анализа
НИУ МГСУ	Научно-исследовательский университет Московский государственный строительный университет
РАНХиГС при Президенте РФ	Российская академия народного хозяйства и государственной службы при Президенте РФ
РГГУ	ФГБОУ ВО «Российский государственный гуманитарный университет»
РУТ (МИИТ)	ФГАОУ «Российский университет транспорта»
СГУ	Сухумский государственный университет
СПбПУ	ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого»
УП РФ	ФГКОУ ВО Университет прокуратуры Российской Федерации

ФГУП НИИР	Федеральное государственное унитарное предприятие «Ордена Трудового Красного Знамени Российский научно-исследовательский институт радио имени М.И. Кривошеева»
ФИЦ ИУ РАН	ФГУ Федеральный исследовательский центр «Информатика и управление» РАН
Центральный филиал РГУП	Центральный филиал Российского государственного университета правосудия
ЦИПБ РАН	ФГБУН Центр исследования проблем безопасности РАН
ЦЭМИ РАН	ФГБУН Центральный экономико-математический институт РАН

Научное электронное издание

ПРОБЛЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ

Материалы
XXIX Международной научной конференции
(15 декабря 2021 г., Москва)

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

Локальное электронное издание
Номер госрегистрации в НТЦ «Информрегистр» 0322103523

Мин. системные требования:
Pentium 4, Acrobat reader 4.0 и выше
Дата подписания к использованию 18.11.2021
1 электронно-оптический диск (CD-R), 6,1 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

978-5-91450-257-4