



## XXXI МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ «ПРОБЛЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ»

В декабре 2023 г. в Институте проблем управления им. В.А. Трапезникова РАН состоялась XXXI Международная научная конференция «Проблемы управления безопасностью сложных систем». Организаторы конференции – Министерство науки и высшего образования Российской Федерации, Институт проблем управления им. В.А. Трапезникова РАН, Институт прикладной математики им. М.В. Келдыша РАН, Научный совет РАН по теории управляемых процессов и автоматизации, Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий.

В работе конференции приняли участие 102 автора из 41 организации, представивших 72 доклада. Работа конференции велась по следующим секциям:

1. Общетеоретические и методологические вопросы обеспечения безопасности.
2. Проблемы обеспечения экономической и социально-политической безопасности.
3. Проблемы обеспечения информационной безопасности.
4. Кибербезопасность. Особенности обеспечения безопасности в социальных сетях.
5. Экологическая и техногенная безопасность.
6. Методы моделирования и принятия решений при управлении безопасностью сложных систем.
7. Автоматизированные системы и средства обеспечения безопасности сложных систем.

Одной из отличительных особенностей настоящей конференции является достаточно большое количество докладов, посвященных проблемам повышения эффективности процессов управления обеспечением национальной безопасности нашей страны в самом широком понимании данного термина. Рассматриваемая проблематика представляет собой один из наиболее сложных комплексов задач теории и методологии организационного управления, а также целого ряда смежных научных дисциплин.

По сложившейся в последние годы традиции конференцию открыл доклад *Г.Г. Малинецкого, В.В. Кульбы, Т.С. Ахромеевой, С.А. Торопыгиной*

«Стратегическая стабильность, искусственный интеллект и управление рисками военных конфликтов», посвященный анализу геополитического, экономического и военно-политического противостояния государств в современном мире. Как подчеркивается в докладе, одной из базовых причин и предпосылок возникновения и развития конфликтов в настоящее время являются принципиально различные цивилизационные стратегии государств, и в первую очередь крупных мировых держав. Россия, на протяжении столетий формировавшаяся как государство, объединяющее различные культуры, национальности, религии, традиционно выступает за поддержание внутренней стабильности и гармонии, а также налаживание тесных и конструктивных взаимосвязей с другими цивилизационными общностями. Данный подход по сути определяет стратегию диалога цивилизаций, которая помимо России оказалась близка и многим другим странам. В работе большое внимание авторы уделили многостороннему анализу стратегии диалога цивилизаций с позиций теории самоорганизации (синергетики), а также практических путей ее реализации с целью предотвращения междоцивилизационных конфликтов и столкновений.

С другой стороны, подчеркивают авторы, Запад исходит из противоположной стратегии, предусматривающей не диалог, а столкновение цивилизаций. К данному тезису можно лишь добавить, что и реализуемая на практике в рамках упомянутой западной стратегии концепция глобализации в совокупности с решением целого ряда геополитических задач (стремление к обладанию мировыми природными ресурсами, военно-политическому господству, финансово-экономическому доминированию и т.д.), в конечном счете направлена на унификацию мира и объединение под началом Запада других цивилизаций, что является одной из фундаментальных первопричин большинства глобальных и локальных конфликтов как исторического прошлого, так и современности. Одновременно с этим необходимо отметить, что рассматриваемая проблема развития и взаимодействия цивилизаций крайне широка, сложна и относится к числу глобальных, вследствие чего не предполага-

ет простых и очевидных решений. Фактическим подтверждением этому являются многолетние и регулярно проводимые на различных уровнях дискуссии научного сообщества, представителей различных общественных движений, религиозных и политических кругов разных стран по проблемам отношений и взаимовлияния цивилизаций.

Доклад *В.В. Цыганова* «Концепция комплекса моделей стратегического управления национальной безопасностью России» посвящен изложению результатов разработки методов и технологий информационной поддержки процессов управления обеспечением национальной безопасности Российской Федерации в условиях ее противостояния с глобальным центром капитала. Предлагаемый в докладе подход к решению рассматриваемой задачи базируется на разработанном комплексе моделей стратегического управления национальной безопасностью России (КМБ), научно-методологической основой которого является теория управления эволюцией социально-экономических систем, активные элементы которых либо рациональны, либо обладают эмоциональным интеллектом.

Прикладные разработки КМБ проводятся в рамках предложенной концепции «ПРОгрессивно-го Комплексного Согласованного Интеллектуального Механизма с Адаптацией» (ПРОКСИМА). Структура КМБ включает комплексы моделей стратегического управления безопасностью, в рамках которых в настоящее время разрабатываются и проходят практическую апробацию функциональные модели «Индикаторное прогнозирование и стратегическое планирование», «Высокие гуманитарные технологии», «Экспертиза и отбор проектов», «Информационный менеджмент», «Информационные войны». Основным назначением перечисленных разработок является интеллектуальная поддержка процессов управления обеспечением безопасности на федеральном, региональном, муниципальном и корпоративном уровнях. Основные положения концепции ПРОКСИМА, как отмечается в докладе, уже апробированы при решении задач стратегического прогнозирования и планирования устойчивого функционирования экономического комплекса Российской Федерации, а также управления развитием транспортной инфраструктуры Сибири, Дальнего Востока и Российской Арктики.

Проблемам обеспечения экономической составляющей национальной безопасности России в современных условиях посвящен доклад *Н.И. Комкова* «Условия трансформации российской экономики». В работе изложены результаты комплексного анализа проблем экономического развития Российской Федерации в услови-

ях неустойчивости сложившегося в настоящее время однополярного порядка мироустройства, а также сформировавшихся узких мест и проблемных ситуаций в производственно-технологическом развитии России. Основное внимание уделено обоснованию необходимости структурных и технологических перемен в национальной экономике России, ряд базовых направлений которых детально рассмотрены в представленной работе.

Среди наиболее существенных проблем экономического развития России в современных условиях автор выделяет, во-первых, отсутствие возможностей государственного регулирования пропорций и взаимоотношений между структурными частями национальной экономики, во-вторых, снижение объема внешних инвестиций, и в-третьих, зависимость от импорта передовых технологий, усугубляемая для предприятий и компаний резким падением доступности экспортных поставок из недружественных стран.

Для ликвидации узких мест, а также как унаследованных из периода становления рыночных отношений и слепого следования рекомендациям западных экспертов, так и возникших в настоящее время проблемных ситуаций в развитии национальной экономики автором предлагаются и обосновываются возможные пути и способы их преодоления. В частности, в докладе в качестве первоочередных мер выделяются: необходимость восстановления и укрепления потенциала инновационной сферы (включая технологическую модернизацию и укрепление отечественного машиностроения) как основы социально-экономического развития страны как минимум в среднесрочной перспективе; роста объемов инвестирования отечественной экономики и ограничения спекулятивных биржевых валютных сделок (включая экспорт накопленных в России финансовых средств и дивидендов); реформирования экономической модели и системы управления государственным развитием, включая переход к стратегическому нормативному и целевому планированию.

Исследованию методологических проблем повышения эффективности планирования и управления социально-экономическим развитием Российской Федерации в условиях неопределенности и риска посвящен доклад авторского коллектива под руководством чл.-корр. РАН *В.Л. Шульца* «Методы сценарного планирования в организационном управлении». В реалиях сегодняшнего дня, как отмечается в докладе, характеризующихся крайне сложной внешнеэкономической и внешнеполитической ситуацией, а также беспрецедентно жестким санкционным давлением на Российскую Федерацию, разработка и реализация государственной социально-экономической политики не-



возможна без эффективной системы перспективного планирования, определяющей пути достижения долгосрочных целей развития страны. В сложившейся ситуации возрастает актуальность проблем разработки методологии устойчивого планирования на базе сценарных технологий, обеспечивающих возможность учета широкого спектра угроз и ограничений, и, соответственно, опережающей оценки результативности разрабатываемых планово-управленческих решений, а также их динамичной адаптации к возникающим изменениям во внешней среде.

В настоящее время, как отмечают авторы работы, уже накоплен определенный опыт использования аппарата функциональных знаковых ориентированных графов в качестве методологической основы процессов сценарного исследования широкого круга проблем управления развитием сложных социально-экономических систем, а для решения прикладных и практических задач разработан программно-аналитический комплекс сценарного моделирования. При этом основная особенность технологий сценарного анализа, как подчеркивается в докладе, заключается в том, что они функционально не предназначены для генерации «на выходе» конечных плановых документов, поскольку решают другую задачу, заключающуюся в комплексном анализе альтернативных вариантов достижения плановых целей в условиях высокой степени неопределенности. Результаты сценарного анализа и опережающая оценка угроз в конечном счете позволяют обеспечить гибкость (адаптивность) и устойчивость разрабатываемых планов к внешним возмущениям и деструктивным воздействиям. В докладе представлен ряд разработанных авторами и имеющих прикладную направленность подходов к преобразованию сценариев различного типа в конкретные планово-управленческие решения при заданных целевых установках. В заключительной части работы отмечается, что возросшая актуальность рассматриваемых проблем требует дальнейшего развития теоретических и прикладных междисциплинарных исследований в области совершенствования методов и технологий сценарного анализа, а также механизмов их практического применения для решения конкретных задач. Не менее важными являются и проблемы встраивания сценарной технологии в функциональную структуру системы подготовки стратегических и тактических плановых решений с целью формирования единой сквозной информационно-технологической цепочки плановых расчетов.

Различным теоретическим и методологическим подходам к решению широкого круга проблем обеспечения ключевых составляющих национальной безопасности, а также подготовки и принятия

решений и управлению рисками посвящена достаточно широкая группа представленных на конференции докладов: *И.В. Чернов* «Проблемы формирования показателей и индикаторов уровня национальной безопасности»; *О.В. Тасейко*, *В.В. Москвичев* «Управление комплексным территориальным риском социально-природно-техногенных систем»; *Н.Н. Володина*, *Н.И. Комков*, *В.В. Сутягин* «Проблемы социальной гармонизации российской экономической системы»; *Д.А. Кононов* «Организационные системы: учет неопределенности и риска при принятии решений»; *Г.В. Горелова* «Об анализе связности структур сложных систем на когнитивных моделях»; *В.В. Ничепорчук*, *У.С. Постникова* «Модель информационной поддержки управления природно-техногенной безопасностью территорий»; *Н.В. Команич* «Проблемы управления и факторы инновационного регионального развития как аспекты региональной безопасности РФ»; *А.А. Лазарев* «Механизмы формирования договорных цен на инновационные проекты»; *С.И. Белов*, *М.Б. Пушкарева* «Задачи обеспечения кибербезопасности интеллектуальных систем энергоснабжения на розничном рынке электроэнергии»; *Р.Е. Торгашев* «Формирование экологической ответственности в сфере предпринимательства».

Большая группа докладов посвящена решению проблем обеспечения информационной безопасности.

Доклад *Н.Г. Кереселидзе* «Об одном аспекте информационной безопасности в модели борьбы с дезинформацией» посвящен исследованию разработанной автором математической модели противодействия преднамеренному распространению ложной информации. Процесс информационного противоборства в работе представлен в форме задачи оптимального управления, отражающей воздействие дезинформации на три выделенные группы граждан: склонную к восприятию дезинформации группу риска, принимающую ложную информацию группу адептов, а также обладающую иммунитетом (невосприимчивую к дезинформации) группу. В качестве меры оценки уровня информационной безопасности общества вводится понятие допустимого барьера числа адептов. Представленные в работе результаты компьютерного моделирования позволили выделить ряд «окон» уязвимости системы противодействия дезинформации. В частности, в работе показано, что противодействие дезинформации должно вестись на систематической основе, а разовые мероприятия по противодействию отдельным деструктивным информационным акциям, хоть и могут приводить к определенному снижению численности группы адептов, на длительном временном горизонте неэффектив-

ны и, соответственно, не могут обеспечить требуемый уровень информационной безопасности.

В докладе *Е.А. Курако, Р.Э. Асратяна, В.Л. Орлова* «Об одном подходе к обеспечению технологического суверенитета в разработках распределенных информационных систем» рассмотрен комплекс проблем, связанных с практической реализацией процессов импортозамещения распределенных и основанных на применении языка программирования C# информационных систем. Обеспечение технологического суверенитета, как отмечается в докладе, в современных условиях становится одной из наиболее актуальных и неотложных задач. При этом одной из проблем перехода на суверенное программное обеспечение (полностью отечественные разработки или новые программные комплексы с доступными исходными текстами) является необходимость исключения ранее присутствовавших возможных «инородных включений» и компонентов. В этой связи крайне важно, чтобы в процессе как создания новых систем, так и перевода существующих в новое окружение разработчики ориентировались не только на используемые при эксплуатации надежные комплексы (желательно включенные в перечни допустимых программных средств), но и применяли проверенные среды проектирования. Большое внимание в работе уделено описанию методов преобразования систем рассматриваемого класса с целью обеспечения возможности их реализации в среде, компоненты которой включены в реестр российского программного обеспечения (основу рассматриваемой среды составляют операционные системы, средства управления базами данных, web-средства, а также фреймворки и программные библиотеки). Обобщен опыт авторов работы по использованию предложенного подхода для переноса распределенных информационных систем из среды ОС Windows в среду ОС Astra Linux.

Проблемам повышения эффективности использования информационной избыточности с целью обеспечения устойчивости информационных систем при сбоях и отказах посвящен доклад *С.К. Сомова* «Показатели надежности работы распределенных систем обработки данных, использующих и не использующих механизмы восстановления разрушенных данных». В нем представлена разработанная автором на базе аппарата теории вероятностей и марковских процессов модель распределенной информационной системы, которая с целью повышения надежности обработки запросов использует оперативное резервирование данных, предполагающее создание и хранение некоторого количества копий и/или предысторий (дампов) информационных массивов. В рамках модели предполагается, что в случае разрушения опера-

тивного резерва в узле он становится неработоспособным и все поступающие в него запросы распределяются между другими работоспособными узлами системы. На основе данной модели получены аналитические выражения для расчета значений основных показателей надежности функционирования распределенных систем обработки данных (среднего времени работы системы до отказа; вероятностей отказа и безотказной работы в заданных интервалах времени и т. д.), позволяющие проводить оценку эффективности вариантов размещения копий оперативного резерва по узлам системы.

Крайне широкому кругу проблем обеспечения информационной безопасности посвящены также работы *М.И. Синцова* «Проблемы выявления угроз, связанных с эксплуатацией уязвимостей в программном обеспечении, через ретроспективный анализ событий информационной безопасности»; *Л.Н. Логиновой, Р.М. Резникова* «Символьная парольная аутентификация как средство повышения информационной безопасности»; *И.В. Чернова, Е.Д. Ермолаева, С.В. Феоктистова* «Выделение базисных режимов динамики факторов, влияющих на информационную безопасность Российской Федерации»; *А.Н. Архиповой, В.Г. Промыслова* «Проблема обеспечения целостности и достоверности радиоастрономических данных в открытых проектах»; *А.С. Рей* «Способ построения оценки интегрального риска информационных систем на основе механизма комплексного оценивания»; *Л.А. Савина* «Применение инструментов обратной разработки для выявления недеklarированных возможностей программного обеспечения систем управления»; *В.О. Сиротюка* «Управление информационной безопасностью евразийского экспертно-информационного пространства»; *А.В. Муромцевой, В.В. Муромцева, Д.В. Кузнецова* «Информационные угрозы виртуального пространства»; *О.А. Волгиной* «Анализ технологий коммуникативного воздействия на поведение агентов гетерогенной модели социальной сети»; *В.А. Зорина, Ю.А. Ненашевой, Р.Р. Галина, Р.В. Мещерякова* «Противодействие фишингу с использованием беспилотных аппаратов на публичные Wi-Fi-сети на массовых мероприятиях»; *М.Д. Черняева* «Сравнение методов оценки риска ФСТЭК и EBIOS».

Значительный интерес участники Конференции традиционно проявляют к проблемам обеспечения техногенной безопасности, надежности функционирования технологических комплексов, потенциально опасных объектов, транспортной и энергетической инфраструктуры, а также управления ликвидацией последствий чрезвычайных ситуаций различного типа, о чем свидетельствует достаточ-





но большое количество разнообразных по тематике докладов: *В.О. Чинакал* «Проблемы обеспечения безопасности управления сложными промышленными объектами при модернизации производства в современных условиях»; *В.В. Лещенко* «Повышение надежности и живучести сложных систем с ядерным реактором»; *В.В. Ведущев, Р.В. Батищев* «Вероятностный подход при управлении технологией как фактор повышения уровня информационной безопасности производства листового проката»; *Е.В. Кловач, В.А. Ткаченко* «Производственный контроль как элемент управления промышленной безопасностью»; *Р.Ш. Хабибуллин* «Задача управления пожарными рисками на объектах топливно-энергетического комплекса на основе методов оптимизации и искусственного интеллекта»; *В.К. Мусаев* «Численное моделирование сейсмических воздействий (волновая теория сейсмической безопасности) на десятиэтажное здание с подвалом»; *О.Б. Байрамов* «Вопросы безопасности ГТС и управление водохранилищем»; *А.Г. Давыдовский* «Алгоритмы превентивного управления надежностью персонала беспилотных авиационных комплексов»; *Д.М. Мельник, Е.А. Куклев* «Сценарный анализ в управлении безопасностью полетов на авиационном предприятии гражданской авиации»; *Е.А. Куклев* «Модель «Спящей катастрофы Ризона» в качестве элемента СУБП в гражданской авиации»; *А.Н. Фомичев* «Методика экономической оценки надежности функционирования пассажирских транспортных систем»; *Л.А. Баранов, А.Е. Ермакова, С.Е. Иконников* «Информационная безопасность систем диспетчерского управления на железнодорожном транспорте»; *А.И. Сафронов, А.С. Иконников* «Применение методов интеллектуального анализа данных к поиску рациональных вариантов автоматизированного построения графиков движения пассажирских поездов метрополитена»; *А.Д. Козлов, Н.Л. Нога* «Метод оценки риска, связанного с субъективными факторами, в интеллектуальных транспортных системах»; *Л.Ю. Филимонюк* «Метод обеспечения безопасности сложных систем в условиях воздействия неблагоприятных факторов и событий»; *А.А. Воронин, Ю.В. Прус* «Математическое распознавание аварийных ситуаций с помощью систем датчиков и взаимодействие со службами экстренного реагирования».

Следует также отметить целый ряд представленных на конференции заметных работ, которые, несмотря на большое разнообразие тематики, объединяет актуальность рассматриваемых проблем и востребованность результатов их решения: *М.Е. Степанцов* «Моделирование конкуренции

трех акторов, бинарное отношение сил которых представляет собой цикл»; *М.Г. Фуругян* «Алгоритмы планирования работ в вычислительных системах реального времени в условиях неопределенности»; *А.А. Широкий* «Учет влияния структуры сложной системы на ее интегральный риск на примере задачи оптимального размещения элементов в простой цепи»; *Д.Р. Гончар* «Решение методом ветвей и границ минимаксной задачи составления расписания с параллельной реализацией»; *В.А. Еременко, Н.И. Манаенкова* «Оценка границ безопасного диапазона длины импульсов при наклонном зондировании ионосферы»; *О.Б. Скворцов, В.И. Сташенко* «Вибрационная прочность и усталость электромеханического оборудования»; *К.В. Чернов* «Способность технического устройства создавать сциентные эффекты техногенного воздействия»; *А.В. Рожнов* «О гибридных моделях анализа среды функционирования для проектной работы и аудита в приложениях многошагового семантического анализа профессиональной коммуникации».

Подробно ознакомиться с представленными работами можно в опубликованных в электронном виде материалах<sup>1</sup>, либо на официальном сайте конференции: URL: <https://iccss2023.ipu.ru/>.

В заключительном слове председательствовавший на конференции д-р техн. наук, профессор *В.В. Кульба* сообщил о планах организации XXXII конференции по рассматриваемой тематике, проведение которой планируется в октябре – ноябре 2024 г. в Институте проблем управления им. В.А. Трапезникова РАН. Телефон оргкомитета (495) 198-17-20, доб. 1407, e-mail: [iccss@ipu.ru](mailto:iccss@ipu.ru). Технический секретарь конференции – Алла Фариссовна Ибрагимова.

Ученый секретарь Оргкомитета конференции  
А.Б. Шелков

**Шелков Алексей Борисович** – канд. техн. наук, Институт проблем управления им. В.А. Трапезникова РАН, г. Москва,  
✉ [abshelkov@gmail.com](mailto:abshelkov@gmail.com)  
ORCID iD: <https://orcid.org/0000-0003-1408-5212>

© 2024 г. Шелков А.Б.



Эта статья доступна по [лицензии Creative Commons «Attribution» \(«Атрибуция»\) 4.0 Всемирная](https://creativecommons.org/licenses/by/4.0/).

<sup>1</sup> Проблемы управления безопасностью сложных систем: материалы XXXI Международной конференции, 13 декабря 2023 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. (7,2 Мб). – Москва: ИПУ РАН. – 2023.



## 31ST INTERNATIONAL CONFERENCE ON PROBLEMS OF COMPLEX SYSTEMS SECURITY CONTROL

A.B. Shelkov

Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

✉ [abshelkov@gmail.com](mailto:abshelkov@gmail.com)

**Abstract.** The conference took place in December 2023. Scientific results presented by the conference participants are briefly described below. The conference included the following sections: general theoretical and methodological issues of security support; problems of economic and sociopolitical security support; problems of information security support; cybersecurity and security aspects in social networks; ecological and technogenic security; modeling and decision-making for complex systems security control; automatic systems and means of complex systems security support. Special attention was paid to the problems of improving the effectiveness of Russia's national security management processes in the realities of today's world. In total, 102 authors from 41 organizations presented 72 papers at the conference.

**Keywords:** conference, complex systems, security control.