УДК 614.8;502.5

# XXXII МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ «ПРОБЛЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ»

Состоявшаяся в ноябре 2024 г. в Институте проблем управления им. В.А. Трапезникова РАН (ИПУ РАН) XXXII Международная научная конференция «Проблемы управления безопасностью сложных систем» была посвящена памяти заслуженного деятеля науки РФ, доктора технических наук, профессора, основателя конференции Владимира Васильевича Кульбы. Конференция проводилась в очном формате, в заседании приняли участие более 100 человек.

Пленарное заседание открыл директор Института проблем управления академик РАН *Д.А. Новиков,* вступительное слово которого было посвящено памяти бессменного руководителя программного комитета конференции В.В. Кульбы.

Основным этапам научной деятельности и направлениям фундаментальных и прикладных исследований В.В. Кульбы посвятил свое выступление председательствовавший на пленарном заседании *И.В. Чернов*. Как подчеркнул докладчик, за время работы в ИПУ РАН с 1962 по 2024 г. В.В. Кульба возглавлял целый ряд крупных научных направлений. Под руководством Владимира Васильевича и при его непосредственном участии разработаны: методы анализа сложных систем управления; теоретические основы использования принципов модульности и типизации при проектировании систем обработки данных; методы и технологии автоматизации проектирования программного и информационного обеспечения систем с открытой архитектурой и реального времени; методологические основы повышения эффективности организационного управления в условиях чрезвычайных ситуаций; методы решения теоретических и прикладных проблем обеспечения информационной безопасности систем управления на организационном и программно-техническом уровнях; методология информационного управления; теоретические и методологические основы сценарного управления.

Особое внимание выступающий уделил любимому детищу Владимира Васильевича – конференции «Проблемы управления безопасностью сложных систем». История организации конференции уходит своими корнями в начало 1990-х гг., когда, поддержав предложение В.В. Кульбы, Институт проблем управления выступил с инициативой проведения Международной научной конференции «Проблемы управления в чрезвычайных ситуациях». Инициатива была поддержана Президиумом РАН и Государственным комитетом по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий при Президенте РСФСР (впоследствии преобразованном в МЧС РФ). К числу организаторов конференции помимо ИПУ РАН были привлечены Научный совет по государственной научно-технической программе «Безопасность», Институт прикладной математики РАН, Институт автоматизации проектирования РАН, Институт проблем передачи информации РАН, Санкт-Петербургский государственный университет. Начиная с 1999 г. (VII конференция) одним из организаторов конференции стал Российский государственный гуманитарный университет (РГГУ).

Первоначально основной тематикой конференции были фундаментальные и прикладные исследования в области повышения эффективности управления в условиях чрезвычайных ситуаций. В дальнейшем в связи с появлением новых научных направлений в рассматриваемой и смежных предметных областях и с существенным расширением тематики представляемых докладов, а также в соответствии с пожеланиями большинства постоянных участников оргкомитетом конференции было принято решение изменить ее название на нынешнее. С тех пор (а точнее, с 1998 г.) и по настоящее время не только название, но и состав секций конференции остаются практически неизменными, и нынешняя XXXII-я конференция не является исключением.

В мероприятии приняли участие 104 автора из 33 организаций, представившие 73 доклада. Работа велась в рамках следующих секций.

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.

Значительное число докладов, представленных на конференции, посвящено исследованию и поиску путей решения проблем обеспечения ключевых составляющих национальной безопасности – военно-политической, научно- и производственно-технологической, социальной, экономической, информационной, техногенной. Актуальность рассматриваемой проблематики, представляющей собой один из наиболее сложных комплексов задач теории и методологии организационного управления, а также ряда смежных научных дисциплин, существенно возросла в последние годы, что связано с широким множеством объективных причин геополитического характера и продолжающимся ростом международной напряженности.

В докладе *В.В. Шумова* «Анализ факторов, влияющих на достижение целей специальной военной операции» рассмотрена концептуальная формализованная модель оценки уровня национальной безопасности государства с использованием степенной производственной функции, отражающая дихотомию человеческих ценностей развития и самосохранения. Разработанное автором формализованное представление функции безопасности структурно является произведением двух компонент: функции суверенности (развития), основанной на использовании степенной функции типа Кобба – Дугласа, и функции сохранения. Первая функция учитывает комплекс географических, демографических и социотехнологических факторов, позволяющих оценивать геопотенциал государства, вторая функция отражает способность государства противостоять деструктивным процессам (в том числе инспирированным извне) и устойчиво развиваться. В докладе приведены результаты моделирования, на основе анализа которых сформированы оценки уровня безопасности России и ее места и роли в мировых процессах на фоне происходящей геополитической инверсии (смены мирового лидера), а также оценки безопасности Европейского Союза и Украины в разрезе ее регионов (по состоянию на 2013 г., т. е. на период, предшествовавший «евромайдану», спровоцировавшему острый политический и экономический кризис).

Основной целью модельных исследований является оценка возможных последствий существенного усложнения военно-политической ситуации в мире, связанного с ростом агрессивности действий геополитических противников нашей страны, направленных на ее ослабление, нанесение России стратегического поражения и в конечном итоге ее расчленение. Результаты проведенного анализа, как отмечается в докладе, показывают, что потенциал наших ответных действий по парированию экзистенциальных угроз российскому государству и обществу превышает возможности западных стран, действия правящих элит которых не отвечают жизненным интересам их народов, что создает объективные условия, благоприятствующие достижению поставленных целей обеспечения безопасности и суверенитета Российской Федерации.

Проблемам повышения эффективности разработки современных систем вооружений посвящен доклад *С.В. Чваркова, С.Н. Подчуфарова, Р.М. Куфрика* «О новом подходе к проектированию сложных организационно-технических систем». В первой части доклада в качестве одной из существенных проблем авторы выделяют не всегда соответствующий современным реалиям уровень исходных целевых постановок задач, которые содержатся в тактико-технических заданиях на разработку сложных изделий и систем, а также неполное соответствие задаваемых требований потребностям практики, что касается прежде всего разработки информационно-управляющих систем, являющихся неотъемлемой частью современных комплексов и систем вооружений, во многом определяющей эффективность их боевого применения. Причиной такого положения, по мнению авторов, является недостаточный уровень корректности описаний конкретных предметных областей (включая смежные), что, с одной стороны, объясняется высоким динамизмом развития информационных технологий, с другой – нерешенностью проблем перехода от неформализованного (лингвистического) описания к формализованному (математическому) представлению решаемых сложными организационно-техническими системами задач управления.

В работе проводится детальный анализ целого ряда организационно-технологических недостатков существующей в настоящее время практики управления разработкой сложных систем рассматриваемого класса, к которым относятся: определенные диспропорции в распределении средств на разработку и модернизацию программно-

математического и аппаратно-технического обеспечения процессов проектирования; нерациональное стремление к созданию дорогих или уникальных, а не унифицированных комплексов управления; недостаточное внимание к разработке прогнозных моделей, позволяющих определять направления развития систем вооружения и проводить анализ характера вооруженной борьбы с учетом асимметрии применения вооруженных сил и невоенных средств и т. д.

На основе результатов проведенного анализа (в том числе и зарубежного опыта решения аналогичных задач) авторами предложен подход к решению рассматриваемых проблем, который позволяет объединить задачи обеспечения национальной безопасности и обороны с задачами экономического, научно-технического и производственно-технологического развития государства с учетом имеющихся реальных возможностей и ограничений, а также уровня развития аналогичных разработок у вероятных противников.

В докладе *Н.И. Комкова, В.В. Сутягина, Н.Н. Володиной* «Возможности активной адаптации экономики РФ к новым вызовам» рассматривается комплекс проблем развития экономического потенциала как важнейшего компонента национальной безопасности нашей страны. Как отмечается в докладе, необходимость противодействия страны военно-политическому и санкционному давлению геополитических противников России, а также попыткам изолировать ее национальную экономику потребовала быстрой адаптации системы государственного управления к возникшим угрозам, благодаря которой, вопреки ожиданиям недоброжелателей, экономика РФ стабильно растет, как и уровень поддержки населением руководства страны. Одновременно с этим сегодня на первый план выходит комплекс новых проблем обеспечения экономического роста в сложившихся неблагоприятных условиях.

Основное внимание в докладе уделено построению и анализу инфологической модели полного воспроизводственного цикла на основе достижений научно-технического прогресса в условиях регулярной смены высоких технологий, формируемых на основе инноваций. Ключевым звеном рассматриваемой модели, подчеркивают авторы, является наука, эффективная реализация потенциала которой во многом определяет базовые направления и темпы инновационного развития современной экономики.

Проведенный авторами ретроспективный анализ показал, что низкая доля высокотехнологической продукции в экономике России с начала с 2000-х гг. была во многом обусловлена доминированием и доступностью импортируемых из стран ЕС и США инновационных технологий. Это фактически блокировало развитие отечественной научной сферы и способствовало снижению интереса промышленных компаний к перспективам своего развития, что в конечном итоге привело к падению объемов и уровня прогнозных исследований по проблемам научно-технологического развития. Оценивая возможности экономического роста в современных условиях, авторы выделяют ряд ключевых факторов, непосредственно влияющих на рассматриваемые процессы, среди которых важнейшими являются: состояние инновационной сферы и ее сопряженность с экономикой; управляемость и скоординированность процессов развития экономики и инновационной сферы; способность к адаптации экономики к эффективному освоению прогрессивных инновационных решений и технологий; наличие необходимых и достаточных финансовых ресурсов, а также решительность и целенаправленность действий органов исполнительной власти по обеспечению согласованности интересов хозяйствующих субъектов и развитию потенциала инновационной сферы и экономики в целом. Инструментом решения поставленных задач инновационного развития, считают авторы работы, должен стать механизм государственного индикативного планирования, формирующий плановые задания компаниям и предприятиям, согласованные с устойчивой налоговой системой, стабильным финансированием и координацией деятельности Центрального банка с финансовыми структурами, обеспечивающими эмиссию денежных средств и облигаций.

Изложению результатов исследования различных методологических и прикладных проблем повышения эффективности процессов управления обеспечением национальной безопасности посвящена достаточно широкая группа представленных на конференции докладов: *Г.Г. Малинецкий, Т.С. Ахромеева, С.А. Торопыгина* «Управление безопасностью сложных систем в новой реальности»; *В.В. Цыганов* «Комплекс моделей стратегической безопасности периметра России»; *Е.А. Дербин* «Актуальные критические угрозы информационно-психологической безопасности социальных объектов»; *А.Н. Фомичев* «Метод псевдоретроспективного манипулирования сознанием как инструмент информационной войны»; *Н.Г. Кереселидзе* «Модель информационной безопасности в случае двух источников дезинформации»; *Г.Г. Малинецкий, В.С. Смолин* «Синергетические основы системного подхода к безопасности

сложных систем»; *А.В. Рожнов* «Обоснование применимости гибридных моделей анализа среды функционирования в описательных примерах оценивания эффективности сложных систем»; *О.И. Кривошеев* «Военная безопасность как фактор социально-экономического и инновационного развития общественных систем»; *Д.Е. Фесенко* «Обоснование Проекта разработки Карты градостроительных рисков применительно к актуальным военно-стратегическим условиям в РФ»; *В.И. Меденников* «Математическое моделирование экономической безопасности в рамках единой цифровой платформы управления производством»; *В.В. Лещенко, И.Н. Пантелеймонов* «Средства систем лазерной космической связи»; *Н.Н. Лантер* «Перспективы сетевого сотрудничества в инновационной системе РФ в новых условиях»; *А.Е. Абрамов, А.А. Сороколад, М.И. Чернова* «Потенциал Программы долгосрочных сбережений как инструмента улучшения пенсионного благосостояния граждан»; *Р.Е. Торгашев* «Экологический суверенитет в условиях устойчивого развития региональных мезосистем»; *О.Б.о. Байрамов* «Об устойчивости страхования инвестиций и займов в микрофинансировании».

Методологическим и прикладным вопросам использования технологий сценарного и когнитивного моделирования в качестве инструмента информационной поддержки процессов подготовки и реализации управленческих решений в условиях неопределенности и риска посвящен целый ряд интересных докладов, среди которых можно отметить работы *И.В. Чернова* «Направления применения сценарного подхода к управлению безопасностью организационных систем»; *З.К. Авдеевой, О.А. Волгиной, Е.Д. Ермолаева, А.А. Черешко* «Разработка системы поддержки прогнозирования на основе интеграции методов когнитивного анализа, мониторинга информационных источников и анализа временных рядов»; *Д.А. Кононова* «Исследование характеристик управления безопасностью сложных систем»; *В.Л. Шульца, И.В. Чернова, А.Б. Шелкова* «Сценарные технологии снижения неопределенности в управлении безопасностью»; *Г.В. Гореловой* «К вопросу анализа устойчивости развития территорий, имитационное моделирование»; *Н.В. Команича* «Структура, принципы и проблемы группового иерархического управления региональной безопасностью»; *Е.Д. Ермолаева, С.В. Феоктистова* «Применимость методов сценарного анализа в сфере информационной безопасности РФ»; *В.Р. Фейзова* «Влияние государственной системы управления на протестный потенциал общества».

Большая группа представленных на конференции докладов посвящена проблемам обеспечения информационной и кибербезопасности, актуальность которых в эпоху бурного развития цифровых технологий непрерывно возрастает.

В докладе *Р.В. Мещерякова, О.О.Евсютина, А.О. Исхаковой, А.В. Душкина* «Обеспечение информационной безопасности слабоструктурированной информации при решении задач защиты информации» рассматриваются вопросы совершенствования механизмов защиты данных, не имеющих фиксированного формата и четкой структуры. Как отмечается в представленной работе, неоднородность слабоструктурированных данных, сложность их обработки и обеспечения сохранности, а также значительный объем (здесь можно добавить, что, по различным оценкам, доля данных рассматриваемого типа в общем объеме корпоративной информации может достигать 80-90 %) требуют создания новых методов оценки информационной безопасности. Основное внимание авторы уделяют анализу перспективных направлений развития систем информационной безопасности, которые, с одной стороны, должны обеспечивать достаточный уровень защиты инфраструктуры и обеспечения сохранности слабоструктурированных данных с учетом особенностей их сбора, обновления, обработки и анализа, с другой – удовлетворять требованиям по скорости обработки и коммуникации информационной системы с источниками данных и конечными пользователями.

Проблемам предотвращения инцидентов, связанных с хакерскими кибератаками на российские распределенные информационные системы и ресурсы, посвящен доклад *Н.Ф. Володиной, А.Д. Козлова, Н.Л. Ноги* «Методика оценки риска информационной безопасности сложных систем». Авторы отмечают, что в настоящее время в результате глобальной цифровизации и в условиях непрекращающихся атак на российские информационные ресурсы со стороны геополитических противников нашей страны актуальность и одновременно с этим сложность решения задач обеспечения информационной безопасности существенно возрастают. В настоящее время изменяется и направленность хакерских атак, целью которых становится как дестабилизация социально-политической обстановки в стране, так и нанесение прямого экономического ущерба путем организации утечек персональных данных и наруше-

ния работоспособности (вплоть до полного разрушения) объектов критической информационной инфраструктуры.

В докладе изложены результаты разработки методологии оценки рисков информационной безопасности на основе математического аппарата нечеткой логики и регрессионного анализа, позволяющей определять совокупность параметров, значения которых в наибольшей степени влияют на возможность реализации различного рода угроз через выявленные уязвимости в узлах и иных структурных компонентах сложных распределенных информационных систем. Практическое применение разработанной авторами методологии позволяет вычислять прогнозные значения уровня риска в условиях неопределенности и неочевидности его зависимости от широкого множества факторов, включая субъективные. Это позволяет повысить эффективность принятия решений по разработке и организации превентивных мер по предотвращению или снижению ущерба от вредоносных атак на информационные системы на наиболее опасных направлениях, а также минимизировать затраты на мероприятия по защите информационных ресурсов.

Повышению эффективности защиты информации в корпоративных сетях крупных организаций посвящен доклад *В.М. Алексеева, С.Н. Чичкова* «Разработка модели анализатора фишинговых атак». Для решения рассматриваемой проблемы авторами разработана двухуровневая структура системы защиты информации в корпоративной полносвязной сети с применением интеллектуальных анализаторов различного типа, позволяющих распознавать и блокировать компьютерные атаки. На первом (внешнем) уровне анализаторы осуществляют контроль и анализ потоков информации на входе в корпоративную сеть, обеспечивая выявление и предотвращение атак типа «отказ в обслуживании» различных видов, фишинговых атак, атак на приложения и иных попыток проникновения внутрь сети извне. На втором уровне анализаторы осуществляют мониторинг активности внутри корпоративной сети, просматривая трафик между автоматизированными рабочими местами пользователей и администраторов, серверами систем, подключенными мобильными устройствами, а также сетевым и периферийным оборудованием, что позволяет выявлять зараженные устройства, предотвращать распространение вредоносного программного обеспечения и т. д.

При разработке и реализации анализаторов применяются методы статистического анализа, временны́х рядов, теории вероятностей и статистики, машинного обучения, оптимизации параметров сетевого мониторинга и распределения ресурсов, а также алгоритмы хеширования и графовые алгоритмы моделирования сетевых взаимодействий. В докладе детально рассмотрены особенности основных методов и подходов к разработке анализатора фишинговых атак на базе их математической интерпретации, а также технологий сигнатурного и эвристического анализа.

Поиску путей решения широкого круга разнообразных задач обеспечения информационной безопасности автоматизированных систем и требуемого уровня защиты данных посвящена большая группа представленных на конференции докладов: *В.В. Ведищев, Р.В. Батищев* «Постановка задачи оптимизации выбора мер и средств защиты информации для государственных информационных систем»; *Р.Э. Асратян, С.С. Владимирова, Е.А. Курако, В.Л. Орлов* «Особенности обеспечения технологической независимости в разработках систем с сервис-браузерной архитектурой»; *А.Д. Домашкин, Л.Н. Логинова* «Сравнительный анализ алгоритмов машинного обучения для обнаружения аномалий в информационных системах»; *М.В. Ведмедева, В.Г. Миронова* «Эволюция информационных систем: от простых решений к комплексным инфраструктурам»; *Л.Е. Мистров* «Основы обоснования критерия информационной безопасности организационно-технических систем»; *А.А. Широкий* «Метод экспресс-оценки рисков компьютерной сети с топологией “звезда”»; *И.А Андронов, В.Г. Сидоренко* «Преимущества применения искусственного интеллекта при работе с документами в части обеспечения информационной безопасности»; *А.А. Сидоренко, Ю.Р. Тедеев* «Повышение информационной безопасности каналов управления путем применения корректирующих кодов»; *А.Ю. Исхаков, М.В. Мамченко* «Алгоритм аутентификации пользователей на основе поведенческой аналитики и машинного обучения для веб-ресурсов»; *А.Г. Уймин* «Система непрерывно-дискретной биометрической идентификации на основе анализа потока данных компьютерной мыши»; *А.А. Саломатин* «Алгоритм аутентификации пользователей на основе статических характеристик аппаратного обеспечения компьютеров»; *А.Г. Чебан, Е.А. Анисимова* «Принципы организации и построения защищенных систем видеоконференции»; *Л.Н. Логинова, А.Д.Дроздов* «Анализ угроз информационной безопасности при использовании Telegram-ботов в бизнесе»; *В.П. Куминов, В.Г. Сидоренко* «Решение задач анализа криптографической стойкости генераторов псевдослучайных чисел с использованием машин-

ного обучения»; *Д.И. Правиков, В.А. Мурашкин* «Подходы к количественной оценке информационной безопасности на предприятии ТЭК»; *В.О. Сиротюк* «Решение задач повышения безопасности цифровых систем управления интеллектуальной собственностью»; *С.К. Сомов* «Способы сокращения вычислительной сложности алгоритмов поиска оптимального размещения массивов данных в распределенных системах обработки данных».

Традиционно разнообразными по тематике являются представленные на конференции доклады, посвященные проблемам предупреждения и ликвидации последствий чрезвычайных ситуаций природного и техногенного характера, а также обеспечения безопасности и надежности функционирования транспортных систем.

В первой тематической группе представленных докладов можно выделить следующие работы: *В.А. Акимов, Д.В. Буряк, Е.О. Иванова* «Формы статистического наблюдения в отношении гидрологической обстановки в населенных пунктах при паводках, вызванных обильными осадками»; *И.Ю .Олтян* «Об управлении индивидуальным риском гибели и получения вреда здоровью в ЧС, обусловленных катастрофическими наводнениями»; *В.А. Акимов, Е.О. Иванова, М.А. Пуликов* «Формы статистического наблюдения в отношении противопожарной обстановки на территориях лесных массивов»; *В.А. Ткаченко* «Обратная связь при проведении аудита систем управления промышленной безопасностью»; *В.А.Зорин* «Атака на робототехнические системы как способ информационно-технического воздействия»; *В.К. Мусаев* «Численное моделирование сосредоточенного вертикального взрывного воздействия на плиту со сплошным фундаментом»; *О.Б. Скворцов, В.И. Сташенко* «Методы виброакустической диагностики оборудования».

Проблемам обеспечения безопасности транспортных систем и объектов посвящены работы *Е.А. Куклева, Д.М. Мельника* «Интеллектуальная поддержка принятий решений при управлении безопасностью полетов поставщиков услуг гражданской авиации на основе сценарного моделирования редких событий»; *В.Г. Новикова* «Обеспечение безопасности движения поездов при координатном способе интервального регулирования»; *С.В. Макшакова* «Система поддержки принятия решений в задачах технического переоснащения в железнодорожной отрасли»; *В.М. Алексеева, Д.Н. Хусенова* «Модель распределенного сенсора с использованием технологии многоволоконного мультиплексирования для контроля местоположения подвижного состава»; *Л.А. Баранова, Чжан Юнцян* «Повышение безопасности движения поездов на линии метрополитена при компенсируемых возмущениях»; *А.И. Сафронова* «Применение дополненного аппарата сетей Петри для моделирования процесса автоматизированного построения плановых графиков движения пассажирских поездов метрополитена»; *Н.Д. Ивановой, И.Ф. Михалевича* «Применение эмулируемой виртуальной среды PNETLab для моделирования интеллектуальных систем водного транспорта»; *Л.А. Баранова, И.Ф. Михалевича, С.С. Соколова* «Концепция создания доверенной среды функционирования объектов автономного судоходства».

Подробно ознакомиться с представленными работами можно в опубликованных в электронном виде материалах[1] либо на официальном сайте конференции: https://iccss2024.ipu.ru/prcdngs.

Проведение очередной XXXIII-й конференции «Проблемы управления безопасностью сложных систем» планируется в ноябре-декабре 2025 г. в Институте проблем управления им. В.А. Трапезникова РАН. О дате и времени проведения конференции будет сообщено в информационном письме оргкомитета, которое будет опубликовано на официальном сайте (https://iccss2025.ipu.ru/), а также разослано участникам, заинтересованным лицам и профильным организациям. Телефон оргкомитета (495) 198-17-20, доб. 1407, e-mail: iccss@ipu.ru. Технический секретарь конференции – *Альфия 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
ORCID iD: https://orcid.org/0000-0003-1408-5212



[1] Проблемы управления безопасностью сложных систем: материалы XXXII Международной конференции, 13 ноября 2024 г., Москва / под общей редакцией А.О. Калашникова, И.В. Чернова; Институт проблем управления им. В.А. Трапезникова РАН Минобрнауки РФ [и др.]. – Электрон. текстовые дан. (9,1 Мб). – Москва: ИПУ РАН. – 2024.

# 32ND 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

**Abstract.** The conference took place in November 2024. 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 theoretical and applied problems of improving the effectiveness of Russia's national economic, information, and technogenic security management processes. In total, 104 authors from 33 organizations presented 73 papers at the conference.

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