УДК 614.8;502.5

DOI: http://doi.org/10.25728/pu.2022.1.6

XXIX МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ «ПРОБЛЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ»

В декабре 2021 г. в Институте проблем управления им. В.А. Трапезникова РАН состоялась XXIX 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 123 автора, представляющих 49 организаций из России и ряда зарубежных стран. Программа конференции включала в себя 84 доклада в рамках восьми 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.
8. Правовые вопросы обеспечения безопасности сложных систем.

Прошедший 2021 год (а конференция традиционно проходит во второй половине декабря) выдался крайне напряженным и богатым вызывающими тревогу событиями. Среди последних отметим прежде всего возрастание сложности противодействия охватившей весь мир пандемии коронавируса, обусловленное появлением новых мутаций COVID–19. При этом, несмотря на необходимость консолидации усилий мирового сообщества в борьбе за выживание человечества в условиях пандемии, по-прежнему обострялась международная обстановка и углублялся кризис в отношениях России и западных стран, принявший форму напряженного военно-политического и экономического противостояния, а также открытой информационной войны.

Развитие пандемии коронавируса COVID–19 и вызванный им глобальный финансовый кризис затронули систему внешнеэкономических связей и мировой торговли, а также внутренние товарно-финансовые рынки даже относительно благополучных стран. Данные негативные процессы привели к масштабному банкротству предприятий малого бизнеса, сокращению рабочих мест, проблемам с занятостью населения, а также необходимости перевода сотрудников многих организаций на удаленный режим работы, что, в свою очередь, вызвало существенный рост киберпреступлений с использованием удаленных атак, фишинга, технологий социальной инженерии и т. д. Одновременно с этим возник целый ряд новых видов киберпреступлений, в том числе различным образом эксплуатирующих темы COVID–19.

Запомнится 2021 год и природно-климатическими аномалиями, по поводу причин возникновения которых в научном сообществе до сих пор нет единого мнения (аномальная жара в России, США, Канаде ряде стран Европы; широкомасштабные лесные пожары в Якутии, Турции, Греции, США; наводнения в Крыму, Краснодарском крае и на Дальнем Востоке, а также в Китае, Индии, Австрии, Чехии, Германии и др. странах; тайфуны и ливни на Дальнем Востоке; беспрецедентное по разрушительной силе торнадо в США; морозы в Африке и Южной Америке и т. д.). Не обошлось и без техногенных аварий и катастроф на объектах промышленности и транспорта.

Сложившаяся ситуация и явно прослеживающиеся негативные тенденции ее возможного (а по некоторым направлениям – весьма вероятного) развития требуют разработки комплексных мер и механизмов системного характера по повышению эффективности противодействия различным внешним и внутренним угрозам безопасности личности, общества и государства. Это приводит к возрастанию актуальности и значения комплексных междисциплинарных фундаментальных и прикладных научных исследований, направленных на разработку методов, средств и механизмов повышения эффективности управления безопасностью (в самом широком понимании данного термина), что не могло не отразиться на тематике представленных на конференции докладов.

По уже сложившейся и многолетней традиции конференцию открыл развернутый доклад *Г.Г. Малинецкого, В.В. Кульбы, Т.С. Ахромеевой, С.А. Торопыгиной, С.А. Посашкова* «Как не оказаться в XVI веке», посвященный анализу влияния происходящих глобальных изменений и обостряющихся противоречий в мировом развитии, а также сопутствующих рисков и угроз. В докладе рассматривается ряд ключевых стратегических задач развития российского общества и государства на длительную перспективу. Большое внимание уделено проблемам развития культуры, науки, высоких технологий, усугубляемых пандемией демографических проблем, а также поиску путей решения иных приоритетных задач поступательного экономического развития страны. На основе результатов проведенного анализа рисков и носящих глобальный характер угроз, возникающих перед российским государством и обществом, авторы сосредоточивают внимание на поиске путей выхода из сложившейся сложной ситуации и достижения базовых национальных целей развития Российской Федерации как на ближайшую, так и на отдаленную перспективу.

Уже второй год внимание авторов представленных на конференции работ привлекают проблемы повышения эффективности управления противодействием пандемии коронавируса. Доклад *А.В. Соколова, Г.В. Ройзензона, Н.П. Комендантовой* «Технология создания систем мониторинга и прогноза состояния опасных явлений и объектов (на примере эпидемии COVID–19)» посвящен разработке методологии оценки эффективности ограничительных мер как инструмента борьбы с распространением коронавируса. В докладе выделяются три базовых группы критериев эффективности рассматриваемых мер, позволяющих оценивать: имеющиеся ресурсы различного типа (коечный фонд, обеспеченность медперсоналом, оборудованием, медикаментами и т.д.); интенсивность расходования и пополнения необходимых для борьбы с пандемией ресурсов; степень достижения поставленных целей. Для оценки эффективности ограничительных мер авторы предлагают применять методы многокритериальной порядковой классификации и вербального анализа принимаемых решений. Значительное место в докладе занимает обобщение накопленного авторским коллективом опыта решения задач мониторинга и прогнозирования новых случаев заражения коронавирусом в Москве в 2020–2021 гг.

Проблемам противодействия пандемии посвящены также работы *М.Е. Степанцова* «Об одной особенности моделирования первого этапа распространения инфекции COVID–19»; *Н.Г. Кереселидзе* «Новые модели распространения вируса SARS-CoV-2 и проблемы управления безопасностью»; *Т.Х. Усмановой, Н.Н. Володиной* «Влияние ограничений из-за коронавируса COVID–19 на безопасность экономических систем».

Отличительной особенностью конференции является большое число разнообразных по тематике работ, посвященных изложению результатов исследования широкого круга методологических и прикладных проблем повышения эффективности процессов управления обеспечением безопасности в условиях цифровизации, бурного развития информационных и коммуникационных технологий, а также сопутствующих данным процессам угроз и рисков.

Проблемам повышения эффективности организационного управления в условиях риска посвящен доклад, подготовленный авторским коллективом во главе с чл.-корр. РАН *В.Л. Шульцем* «Анализ фактора неопределенности в процессе подготовки управленческих решений». Неопределенность при подготовке решений, как утверждается в докладе, фактически проистекает из двух основных источников: субъективного (эпистемологического), представляющего собой результат недостатка необходимых для принятия решений знаний, и объективного (алеаторного, онтологического), являющегося следствием стохастической природы объекта управления или внешней среды. Отдельный класс составляет лингвистическая (субъектная) неопределенность, обусловленная рядом объективных свойств естественного языка. В настоящее время, как отмечается в докладе, вследствие многогранности факторов неопределенности, методология ее оценки развивается в основном в направ-

лении разработки методов решения прикладных задач, ограниченных рамками исследуемых сегментов предметных областей. В то же время попытки разработки универсальных методов оценки влияния неопределенности на эффективность управленческих решений сталкиваются со значительными трудностями, преодоление которых во многом возможно с применением методологии сценарного анализа.

В докладе *А.А. Тимошенко* «Криптовалюты как угроза национальной безопасности России: юридические механизмы противодействия» рассматривается комплекс проблем, обусловленных законодательной неурегулированностью многих аспектов оборота криптовалют в Российской Федерации. Констатируя уже свершившийся факт мирового признания криптовалют как инструмента формирования альтернативных финансовых отношений, автор работы особое внимание уделяет анализу угроз национальной безопасности России, особенно в ситуации, когда виртуальные валюты используются в противозаконных целях. Результаты проведенного анализа угроз неконтролируемого оборота криптовалют с точки зрения целей, задач и функций правоохранительных органов позволили сформулировать ряд конкретных предложений по совершенствованию российской системы законодательного регулирования, включающих внесение соответствующих изменений в действующее законодательство, а также наделение Правительства РФ и профильных ведомств расширенными полномочиями по регулированию и контролю обращения цифровых финансовых активов. Полностью соглашаясь с выводами автора работы, можно лишь подчеркнуть, что актуальность рассмотренных в докладе проблем возрастает еще и в связи с тем, что массовое использование криптовалюты в национальном платежном обороте в условиях большого числа неконтролируемых государством эмитентов в конечном итоге может привести к критическому разрегулированию финансовой системы страны и, что особенно важно, к невозможности эффективного планирования и реализации государством единой денежно-кредитной политики со всеми вытекающими отсюда негативными социально-экономическими последствиями.

Традиционно большой интерес участники конференции проявляют проблемам управления информационной и кибербезопасностью. В докладе *Р.В. Мещерякова* «Подход к защищенному интеллектуальному управлению роботами и их коалициями с использованием интерфейса человек-робот(ы) и робот-робот(ы)» рассматриваются проблемы формирования защищенных механизмов межмашинного обмена данными, актуальность которой в настоящее время возрастает в связи с развитием интернета вещей и с тем, что стандарты безопасности систем управления робототехническими комплексами с использованием человеко-машинных интерфейсов практически отсутствуют. Проведенные автором исследования показали, что разрабатываемые модели и механизмы безопасности систем рассматриваемого типа должны основываться на использовании различных интерфейсов для резервирования каналов связи при подаче команд и получения обратной связи от объектов управления, а также учитывать такие факторы, как помехоустойчивость измерительных каналов, отказоустойчивость системы в целом, воспроизводимость эталонного сигнала, а также наличие единого формата передачи измерительной информации.

Упомянутой выше и крайне широкой тематике посвящены работы *А.М. Смирнова, А.Ю. Исхакова* «Алгоритм двухфакторной аутентификации как инструмент снижения FRR для проактивного фильтра выявления атак»; *В.К. Абросимова, А.Н. Райкова* «Ситуационная осведомленность для безопасной и эффективной работы агророботов»; *Е.Ф. Жарко* «Некоторые вопросы процесса верификации и валидации управления кибербезопасностью»; *Д.И. Правикова* «Концепция информационной безопасности «роя» киберфизических систем»; *К.А. Бугайского* «Определение успешности действий нарушителя в однородной среде»; *Р.Э. Асратяна* «Использование технологии SSL/TLS для создания защищенных сетевых каналов в распределенных системах»; *А.А. Саломатина* «Методы противодействия отслеживанию браузерных отпечатков пользователей»; *В.Л. Орлова, Е.А. Курако* «Сервис-браузер и атаки типа Man in the middle»; *С.К. Сомова* «Проблема оптимизации схемы восстановления разрушенного оперативного резерва данных в распределенных системах»; *А.Д. Козлова, Н.Л. Ноги* «Достоверность информации как элемент обеспечения информационной безопасности и оценка ее уровня»; *В.О. Сиротюка* «Цели, задачи и принципы обеспечения безопасности цифровых систем управления интеллектуальной собственностью»; *А.А. Мелихова* «Обеспечение непрерывной разработки программных продуктов, сертифицируемых по требованиям безопасности».

Ряд интересных докладов посвящен актуальным проблемам обеспечения безопасности в социальных сетях. Это работы *Л.В. Жуковской* «Особенности применяемого математического инструментария для построения систем обеспечения без-

опасности в социальных сетях»; *З.К. Авдеевой, С.В. Ковриги* «Систематизация психологических факторов влияния на изменение убеждений и аттитюдов в результате коммуникативных воздействий в виде модели причинно-следственных влияний»; *М.В. Мамченко, А.С .Рея* «Оценка рисков распространения деструктивного контента в социальных сетях»; *Г.К. Борескова* «Этические аспекты применения инструментов искусственного интеллекта для обеспечения пространства доверия в электронных СМИ»; *Е.П. Охапкиной* «Разработка динамической системы функционирования сообществ социальной сети»; *В.В. Муромцева, А.В. Муромцевой* «Цифровизация – угрозы и риски».

На конференции было представлено большое количество интересных работ, посвященных комплексу проблем управления обеспечением экономической, экологической, энергетической и техногенной безопасности в условиях развития высоких технологий, в последние годы увязываемых с так называемой «зеленой» или «климатической» международной повесткой, декларируемые и реальные цели которой, отметим, представляют собой отдельный предмет детального анализа и в настоящее время широко обсуждаются научным и экспертным сообществами.

В докладе *Г.В. Гореловой, Э.В. Мельника, М.В. Орда-Жигулиной, Д.В. Орда-Жигулиной* «Безопасность состояния водной экосистемы Азово-Черноморского региона, когнитивное исследование» представлены результаты когнитивного анализа и имитационного моделирования процессов в водной экосистеме региона с целью формирования прогнозов экологических угроз и обеспечения безопасности населения и береговой инфраструктуры. Приведена функциональная структура разработанной авторами системы мониторинга развития опасных явлений в природных системах, предназначенной для осуществления непрерывных наблюдений за исследуемыми процессами.

Перспективность предложенного авторами подхода к решению рассматриваемых проблем определяется возможностями в рамках единой системы мониторинга интегрировать большое количество получаемых из различных источников разнородных и разновременных данных, выявлять (в том числе неочевидные) причинно-следственные связи между изучаемыми традиционными методами параметрами гидроэкосистемы и таким образом определять закономерности экосистемных процессов, а также осуществлять интеллектуальную поддержку процессов принятия решений по противодействию экологическим угрозам на основе результатов когнитивного моделирования.

Среди представленных в рамках рассматриваемой широкой тематики работ отметим доклады *Н.Н. Володиной, Н.И. Комкова, В.В. Сутягина* «Проблемы управления развитием крупномасштабных социально-экономических систем»; *Р.М. Нижегородцева* «Формализация институтов, неблагоприятный отбор и управление коррупционным поведением агентов»; *Е.П. Грабчака, Е.Л. Логинова* «Подготовка системы государственного управления России к сверхкритическим ситуациям природного и техногенного характера»; *Е.А. Абдуловой* «Об одном подходе к управлению рисками критической инфраструктуры»; *Н.Н. Лантер* «Структурная устойчивость Арктики как экономической территориальной экосистемы»; *Т.А. Пискуревой, А.Н. Махова* «Цифровая трансформация и импортозамещение во взаимосвязи обеспечения безопасности ядерного объекта»; *В.И. Меденникова* «Системный подход к применению искусственного интеллекта для разрешения проблем экологической безопасности при цифровой трансформации сельского хозяйства»; *М.А. Полюховича* «Основы информационного обеспечения процесса передачи электроэнергии в условиях деструктивного воздействия гидрометеорологических факторов»; *Р.Е. Торгашева* «Комплексный геоэкологический мониторинг лесных геоэкосистем Московского столичного региона».

Традиционно большой интерес участники конференции проявляют к проблемам техногенной и промышленной безопасности. Доклад *В.Г. Промыслова, К.В. Семенкова* «Управление риском кибербезопасности на этапе проектирования для промышленных систем» посвящен изложению результатов разработки технологии оценки риска кибербезопасности в процессе проектирования критически важных промышленных объектов (КВО). Предлагаемая технология состоит из двух базовых этапов. Первый этап включает в себя общую для проектируемой системы оценку риска в условиях неопределенности в понимании деталей реализации системы и частично – требований, предъявляемых к ней. В рамках данного этапа фактически закладываются основные технические решения по обеспечению кибербезопасности. Кроме того, формируемая обобщенная оценка рисков обеспечивает возможность установления приоритетов дальнейшей детальной их проработки в процессе проектирования архитектуры безопасности КВО, например, в части деления на зоны безопас-

ности или классификации активов. Второй (опциональный) этап включает детальную оценку риска с учетом особенностей архитектуры разрабатываемой системы и специфики модели угроз.

Преимуществами предложенной технологии является возможность предотвращения критических ошибок в процессе проектирования системы, связанных с недооценкой или, наоборот, переоценкой требований по обеспечению кибербезопасности, а также сокращения объема (и, соответственно, стоимости и времени) выполнения проектных работ путем исключения процедур детальной оценки риска для отдельных подсистем в случае, если интегральная его оценка для системы в целом не превышает допустимый уровень.

Ряд интересных докладов посвящен проблемам предупреждения и ликвидации последствий чрезвычайных ситуаций техногенного и природного характера, а также обеспечения безопасности и надежности функционирования технологических комплексов и транспортных систем: *В.О. Чинакал* «Повышение безопасности управления сложными объектами в условиях скрытых изменений параметров технологических процессов»; *Л.А. Баранов, Е.П. Балакина, В.Г. Сидоренко* «Безопасное диспетчерское управление в условиях использования интеллектуальных беспилотных систем управления движением городского внеуличного транспорта»; *В.К. Мусаев* «Математическое моделирование сейсмических волн напряжений в полуплоскости вертикальной полостью из резины: соотношение ширины к высоте один к десяти»; *М.Ю. Прус* «Стохастическое моделирование каскадных сценариев развития аварий и катастроф»; *А.В. Евдокимова* «Анализ пожарной безопасности теплоцентрали на основе изучения пожароопасных ситуаций»; *Е.В. Кловач, В.А. Ткаченко* «Об обосновании использования аудита промышленной безопасности»; *О.Б. Скворцов* «Стандартизация и нормирование вибрационной усталости механизмов и машин».

Отметим также целый ряд представленных на конференции заметных работ, которые, несмотря на большое разнообразие тематики, объединяет актуальность рассматриваемых проблем и востребованность результатов их решения: *В.В. Быстров, А.В. Маслобоев, И.О. Датьев* «Инструменты цифровизации управления кадровой безопасностью регионального производственного кластера»; *А.А. Широкий* «Модели и методы естественных вычислений в управлении рисками сложных систем»; *Е.В. Аникина* «Управление рисками сложной компьютерной сети на основе общей арбитражной схемы»; *Л.Е. Мистров, Е.В. Головченко* «Основы моделирования мероприятий информационной безопасности для обеспечения конфликтной устойчивости функционирования социально-экономических организаций»; *А.Н. Фомичев* «Методика расчета экономического ущерба от распространения наркомании»; *В.В. Кафидов* «Миграционная политика и безопасность города»; *В.В. Лещенко* «Обеспечение национальной безопасности в сфере интеллектуальной собственности в России»; *И.А. Сидоренко, О.Н. Дудариков, Н.Е. Ходырева* «Средства информационной поддержки принятия решений по оценке возможностей видовых технических разведок»; *А.М. Анохин* «Анализ прикладных путей повышения метрологической надежности измерительных преобразователей»; *В.И. Сташенко, О.Б. Скворцов, О.А. Трощкий* «Особенности оценки вибрационных воздействий в электромеханических системах с импульсным управлением»; *Д.Р. Гончар* «Балансировка вычислительной нагрузки при параллельной реализации решения минимаксной задачи составления расписания методом ветвей и границ».

Подробно ознакомиться с представленными работами можно в опубликованных материалах[1] либо на официальном сайте конференции: URL: https://iccss2021.ipu.ru/prcdngs.

В заключительном слове председательствующий на конференции д-р техн. наук, профессор *В.В. Кульба* сообщил о планах проведения юбилейной XXX конференции по рассматриваемой тематике, которая, по сложившейся традиции, состоится в декабре 2022 г. в Институте проблем управления им. В.А. Трапезникова РАН. Телефон оргкомитета (495) 198-17-20, доб. 1407, e-mail: 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.

[1] Проблемы управления безопасностью сложных систем: материалы XXIX Международной конференции, 15 дек. 2021 г., Москва / под общ. ред. А.О. Калашникова, В.В. Кульбы. – М.: ИПУ РАН. – 2021. – 544 с.

29TH INTERNATIONAL CONFERENCE ON 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 December 2021. Scientific results presented by the conference participants are briefly outlined below. The conference sections were theoretical and methodological problems of security support, problems of economic and sociopolitical security support, problems of information security support, cybersecurity and features of security 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, legal aspects of complex systems security support. At the conference, 123 authors from 49 organizations (Russia and some foreign countries) presented 84 papers. For the second year, conference participants dealt with improving the efficiency of counteraction to the COVID-19 pandemic in their papers. A distinctive feature of the conference is numerous papers on various topics, presenting research results on a wide range of methodological and applied problems of improving the effectiveness of security control processes in the context of digitalization, the rapid development of information and communication technologies, and the threats and risks associated with these processes.

Keywords: conference, complex systems, security control.