На правах рукописи

Павлов Михаил Александрович

МЕХАНИЗМ СОГЛАСОВАНИЯ ИНТЕРЕСОВ ДЛЯ УПРАВЛЕНИЯ ЦИФРОВОЙ БЕЗОПАСНОСТЬЮ ПРИ ВНЕДРЕНИИ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ

5.2.3. «Региональная и отраслевая экономика»
(7. Экономика инноваций)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата экономических наук

Москва – 2025

Работа выполнена в ФГАОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»

Научный руководитель:	**Кашеварова Наталия Александровна** кандидат экономических наук, доцент
Официальные оппоненты:	**Митяков Евгений Сергеевич** доктор экономических наук, профессор, ФГБОУ ВО «РТУ МИРЭА», заведующий кафедрой КБ-9 «Предметно-ориентированные информационные системы»
	Брынцев Александр Николаевич доктор экономических наук, профессор, ФГБУН «ЦЭМИ РАН», заведующий лабораторией цифровой экономики
Ведущая организация:	ФГУ «Федеральный исследовательский центр «Информатика и управление» Российской академии наук»

Защита состоится 11 декабря 2025 года в 11:00 часов на заседании диссертационного совета 24.2.331.21 на базе Московского государственного технического университета имени Н.Э. Баумана по адресу: 105005, г. Москва, 2-я Бауманская ул., д. 7, ауд. 414ибм.

Ваш отзыв на автореферат в двух экземплярах, заверенный печатью, просим выслать по адресу по адресу: 105005, г. Москва, 2-ая Бауманская ул., д. 5, стр. 1.

С диссертацией можно ознакомиться в библиотеке МГТУ им. Н.Э. Баумана и на сайте www.bmstu.ru.

Автореферат разослан «____» _____ 2025 г.
Телефон для справок 8 (499) 267-17-83.

Ученый секретарь
диссертационного совета, к.э.н., доцент  Н.А. Кашеварова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В условиях стремительного развития технологий и масштабной цифровизации бизнес-процессов безопасность информации и ИТ-ресурсов становится необходимым условием для эффективного функционирования современного бизнеса. Растущий объем, разнообразие и значимость хранимых данных требуют от организаций внедрения комплексных стратегий управления цифровой безопасностью, что подразумевает интеграцию множества элементов бизнес-архитектуры.

Цифровая безопасность включает в себя реализацию таких мер, как контроль доступа, шифрование, антивирусная защита, постоянный мониторинг и аудит систем, управление рисками, а также обучение персонала по вопросам безопасности. Необходимо рассматривать управление цифровой безопасностью как динамичный и многоаспектный процесс, требующий регулярного мониторинга, анализа и корректировки в соответствии с меняющимися угрозами и требованиями регулирующих органов. Управление цифровой безопасностью должно быть интегрировано во все уровни архитектуры предприятия и учитывать не только актуальные на данное время киберугрозы, но и ожидания клиентов и партнеров.

В условиях экономики знаний информация становится одним из наиболее ценных активов организаций. Утечка или несанкционированный доступ к данным могут повлечь за собой серьезные негативные последствия, включая финансовые потери, снижение конкурентоспособности, ущерб репутации, юридические проблемы и риски для непрерывности бизнеса. Финансовые потери могут быть обусловлены как непосредственно кражей денежных средств, утечками финансовых, персональных и других чувствительных данных, а также штрафами от регуляторов. Кибератаки могут вызвать прерывание бизнес-процессов, остановку производств, что приводит к потере продуктивности, негативным последствиям для репутации и возможности утраты клиентов. Также нарушения безопасности могут привести к судебным разбирательствам и штрафам за несоответствие действующим законодательным нормам.

При реализации инновационных проектов, связанных с цифровыми технологиями, расходы на цифровую безопасность возникают на всех этапах жизненного цикла инновации: от разработки и внедрения до обеспечения безопасности информации и ИТ-ресурсов на стадии эксплуатации. Эти расходы включают инвестиции в технологическую инфраструктуру, программное обеспечение, обучение специалистов, консультационные услуги и аудит безопасности. Все эти затраты должны быть учтены при построении модели финансирования инновационных проектов.

Одной из задач бизнеса является минимизация потенциальных убытков от нарушений цифровой безопасности и эффективное распределение ресурсов, обеспечивающее баланс между рисками и затратами на цифровую безопасность. Экономическая оценка рисков, связанных с цифровой безопасностью инновационных проектов, подразумевает анализ финансовых последствий от возможных нарушений и разработку стратегии минимизации этих рисков. При этом требуется детальный анализ новых угроз, вероятностей атак, возможного ущерба и оптимальных мер защиты.

Таким образом, управление цифровой безопасностью выходит за рамки выполнения технических требований, а представляет собой стратегический бизнес-процесс обеспечения защиты интересов организации, её активов и репутации в условиях современного цифрового мира.

Степень разработанности темы исследования. Тема управления ИТ-ресурсами организации, цифровой безопасности предприятия и управления инновационными технологиями цифровой трансформации организации является актуальной и широко исследуемой в современной науке и практике. Множество зарубежных и отечественных авторов вносят вклад в эту область исследований, разрабатывая новые концепции, методы и рекомендации.

В области управления ИТ-инфраструктурой и цифровыми ресурсами организации возникает необходимость эффективного распределения и использования информационных технологий для достижения стратегических целей организации. Среди зарубежных авторов стоит особо выделить: Р. Гупта, П. Вейл, М. Мохания, Р.В. О'Коннор, Д. Росс, М. Мора, М. Райсингани, Р. Стейнберг, Х. Прасад.

В области управления цифровой безопасностью предприятия необходимо выделить таких авторов, как Р. Андерсон, Дж. Дикстра, К. Митник, Р. Стивенс, Д. Парк, Р. Сандху, Дж. Чепмен, Б. Шнайер, Д. Шифалакуа, У. К. Эверетт, Д.В. Валько, Г.С. Сологубова, О.А. Степанов, А.В. Щербак.

При формализации неопределённости при принятии инвестиционных решений по использованию новых технологий и управлении инновационными технологиями цифровой трансформации организации многие исследования фокусируются на комплексном анализе рисков и разработке стратегий управления. Среди зарубежных авторов стоит указать вклад таких исследователей, как Юл Андерсен, Дж. Бауэрс, Д.В. Квак, Д. Л. Олсон, Ю. Дж. Сео, Р. Мейсон -А. Хоракян Р. Шаретт.

Среди отечественных авторов следует выделить таких авторов, как: М.Ю. Арзуманян, Е.В. Виноградов, В. Глушков, О.И. Долганова, Н.И. Диденко, Е.П. Зараменских, Д.В. Кудрявцев, В. Преображенский, Д.Ф. Скрипнюк, Н. Шилова, В.И. Фомин (в области управления ИТ-ресурсами и цифровой безопасности). А.Е. Бром, Ю. М. Брюханова, Л. П. Гончаренко, А. В. Гребенкина, В.Д. Калачанова, В. В. Карачаровского, И.Н. Омельченко, Н.А. Полякова, Н.И. Лапина, Т.Г. Садовской, Е.В. Соколова, С.Г. Фалько, А.В. Колесникова, А.И. Орлова, Д.А. Поспелова, А.С. Птускина, Е.А. Федоровой, В.М. Черненького, В.Е. Шкурко и других исследователей (в области управления инновациями).

Вышепредставленные авторы предлагают решения соответствующих проблем и предлагают свои решения для различных, но локальных аспектов цифровой безопасности и управления ИТ-ресурсами в условиях цифровой трансформации организации. Тема управления ИТ-ресурсами организации, цифровой безопасности предприятия и управления инновациями при цифровой трансформации организации продолжает развиваться, и новые исследования вносят свой вклад в эту область, помогая организациям справиться с новыми вызовами цифровой безопасности организации. Имеющийся в данных работах научный задел был использован при проведении диссертационного исследования.

Цель и задачи исследования. Целью диссертации является разработка ме-

ханизма согласования интересов системы «Организация-Субъекты» цифровой безопасности при внедрении инновационных технологий, обеспечивающего сбалансированность конфликтных стимулов.

Для достижения поставленной решаются следующие основные задачи:

– анализ современной методологии и практики согласования интересов для управления цифровой безопасностью при внедрении инновационных технологий;

– формализация предметной области исследования и формулирование концепции согласования интересов для управления цифровой безопасностью при внедрении инновационных технологий;

– обоснование подхода к разработке механизма согласования интересов для управления цифровой безопасностью при внедрении инновационных технологий;

– разработка модели оценки интересов системы «Организация-Субъекты» цифровой безопасности на основе функции полезности с учетом потребностей в цифровизации и новых видов цифровых угроз;

– разработка модели оценки стоимости цифровой угрозы при внедрении инновационной технологии в рамках согласования интересов в системе «Организация-Субъекты» цифровой безопасности;

– разработка метода согласования интересов системы «Организация-Субъекты» цифровой безопасности на основе совокупной функции полезности;

– практическая реализация механизма согласования интересов системы «Организация-Субъекты» цифровой безопасности при внедрении инновационных технологий;

– разработка рекомендаций по практической реализации механизма согласования интересов системы «Организация-Субъекты» цифровой безопасности при внедрении инновационных технологий.

Объектом исследования является система «Организация-Субъекты» цифровой безопасности критической информационной инфраструктуры.

Предметом исследования является согласование интересов системы «Организация-Субъекты» цифровой безопасности критической информационной инфраструктуры.

Методология и методы исследования. Теоретическая и методологическая основа исследования опирается на общенаучные методы, такие как теория систем, дедукция, индукция, абстракция и формализация. Эти методы позволяют анализировать сложные взаимосвязи и воздействия в рамках организации и выявлять факторы, способствующие возникновению и управлению инновациями.

Дополнительно были применены специальные методы, такие как теория кооперативных игр, теория контрактов, теория полезности, теория измерений, теория принятия решений, теория стейкхолдеров, теория нечетких множеств, коллективный выбор управления проектами, экспертное оценивание, комбинаторная оптимизация, гибридные мягкие вычисления, машинное обучение и прочие подходы специализированного искусственного интеллекта.

Информационно-эмпирическая база исследования включает действующие нормативные правовые акты, стандарты, статистические и аналитические отчеты, доклады и обзоры международных и национальных организаций в области цифро-

визации экономики, цифровой трансформации организации, цифровой безопасности, искусственного интеллекта, управления проектами, управления рисками, управления ИТ-ресурсами.

Сочетание теоретической и методологической основы с информационно-эмпирической базой позволяет выполнить комплексный анализ инноваций и разработать эффективный механизм управления ими в контексте цифровой трансформации организации и обеспечения безопасности цифровой среды организации.

Научная задача заключается в развитии научно-методического аппарата согласования интересов заинтересованных сторон организации при принятии экономических решений по обеспечению цифровой безопасности при внедрении инновационных технологий.

Соответствие паспорту научной специальности. Область исследования соответствует следующим пунктам паспорта специальности 5.2.3. «Региональная и отраслевая экономика» (7. Экономика инноваций):

7.5. Цифровая трансформация экономической деятельности. Модели и инструменты цифровой трансформации.

7.13. Управление инновациями и инновационными проектами на уровне компаний, предприятий и организаций. Инновационные риски.

Научная новизна заключается в том, что с учетом актуальной специфики и трендов развития цифровой безопасности организации разработан механизм согласования интересов системы «Организация-Субъекты» цифровой безопасности при внедрении инновационных технологий, отличающийся учетом изменяющихся потребностей, возникающих новых цифровых угроз безопасности и растущих требований бизнеса к цифровой среде организации.

Основные научные результаты, полученные в ходе исследования лично автором и выносимые на защиту, заключаются в следующем:

1. Предложены формализованный понятийный аппарат и обоснование научно-методического подхода к формированию механизма согласования интересов стейкхолдеров цифровой безопасности при внедрении инновационных технологий, отличающийся учетом новых цифровых вызовов и уязвимостей и использованием современных экономико-математических подходов на основе кооперативно-игрового и мягкого моделирования, и позволяющий сформировать комплекс методов для решения специфических задач согласования интересов при управлении цифровой безопасностью.

2. Разработана модель оценки интересов системы «Организация-Субъекты» цифровой безопасности на основе функции полезности, отличающаяся постановкой и решением проблемы баланса новых потребностей цифровой среды организации и новых видов цифровых угроз, и позволяющая принимать обоснованные решения в части управления цифровой безопасностью при внедрении инновационных технологий.

3. Разработана модель оценки стоимости цифровой угрозы при внедрении инновационной технологии в рамках согласования интересов в системе «Организация-Субъекты» цифровой безопасности, отличающаяся постановкой и решением про-

блемы оценки стоимости мер по предотвращению новых цифровых угроз, и позволяющая принимать обоснованные решения при внедрении инновационных технологий.

4. Разработан метод согласования интересов системы «Организация-Субъекты» цифровой безопасности на основе совокупной функции полезности, отличающийся переопределением функции полезности и решением проблемы баланса требований бизнеса, и позволяющий учитывать расширенные ожидания, интересы и требования субъектов цифровой безопасности бизнеса.

5. Разработаны бизнес-процессная архитектура механизма и рекомендации по практической реализации механизма согласования интересов в системе «Организация-Субъекты» цифровой безопасности при внедрении инновационных технологий, отличающиеся динамической адаптивностью и кросс-функциональностью архитектуры безопасности и обеспечивающие проактивное управление цифровой безопасности.

Теоретическая значимость диссертационного исследования заключается в развитии научных концепций и практики принятия экономических решений в процессе согласования интересов субъектов цифровой безопасности организации при внедрении инновационных технологий.

Практическая ценность диссертационной работы состоит в разработке методов, предложение рекомендаций и апробации в практической деятельности механизма согласования интересов субъектов безопасности цифровой среды организации для поддержки принятия экономически обоснованных решений при внедрении инновационных технологий.

Обоснованность и достоверность научных положений обеспечивается корректным выбором исходных данных, основных допущений и ограничений при постановке научной задачи. Достоверность научных положений и выводов диссертации подтверждается сходимостью полученных результатов с практикой принятия решений по управлению процессами цифровой трансформации организаций. Полученные научные выводы были также апробированы в практической деятельности, а их положительные результаты подтверждают эффективность предлагаемых подходов и методов в области управления инновациями и обеспечения безопасности цифровой среды организации.

Апробация результатов исследования. Основные положения и выводы диссертации доложены и получили положительную оценку на международных и всероссийских научно-практических конференциях: «Тринадцатые Чарновские чтения» (Москва, 2023), «Актуальные вопросы экономики, менеджмента и инноваций (Нижний Новгород, 2023), «XLVI Академические чтения по космонавтике» (Москва, 2022), «Актуальные вопросы экономики, менеджмента и инноваций (Нижний Новгород, 2021).

Основные положения и результаты диссертации использованы в учебном процессе на кафедре «Бизнес-информатика» МГТУ им. Н.Э. Баумана, и реализованы в ООО «УК «Марьина Роща»», что подтверждается соответствующими актами.

Публикации. По теме диссертации опубликовано 12 научных работ общим объемом 7,5, п.л. (авторский вклад – 6,5 п.л.), из них 6 статей общим объемом 4,65

п.л. в рецензируемых изданиях, рекомендованных ВАК при Минобрнауки России, в том числе 4 статьи общим объемом 3,5 п.л. по научной специальности.

Структура и содержание работы. Диссертация изложена на 185 страницах и состоит из введения, трех глав, с выводами по каждой из них, общих выводов по диссертационной работе, списка сокращений и условных обозначений, списка литературы из 279 наименований, содержит 25 таблиц и 32 рисунка.

Рисунок 1 представляет логическую структуру диссертационного исследования, разработанную в соответствии с системным подходом для решения поставленных задач.

Во введении обосновывается выбор и актуальность темы исследования, определяются цель и задачи диссертации, объект и предмет исследования, формулируется научная новизна и практическая значимость исследования, описываются содержание и структура работы.

Рисунок 1 – Логическая структура диссертационного исследования

В первой главе выполняется анализ современной методологии и практики управления цифровой безопасностью при внедрении инновационных технологий. Выполняется обобщение и систематизация актуальной практики управления цифровой безопасностью критической инфраструктуры организации при внедрении инновационных технологий. Исследуются существующие методы оценки и управления цифровой безопасностью при внедрении инновационных технологий, и перспективы их развития на основе новых цифровых технологий, а также актуальные проблемные области, и выявляются ограничения с учетом деловой практики. На основе выявленных противоречий приводится постановка научной задачи, выдвигается научная гипотеза. Разрабатывается логическая структура диссертационного исследования.

Во второй главе излагаются результаты разработки экономико-математических методов комплексной модели согласования интересов при управления цифровой безопасностью при внедрении инновационных технологий. Описывается формализованный понятийный аппарат в области согласования интересов для управления цифровой безопасностью при внедрении инновационных технологий. Предлагается обоснование научно-методического подхода комплексной модели согласова-

ния интересов для управления цифровой безопасностью критической инфраструктуры организации. Разрабатываются метод полезности мер цифровой безопасности организации на основе теории игр, модель согласования инновационных рисков, метода согласования потребностей бизнеса. Предлагается комплексная модель согласования интересов для управления цифровой безопасностью при внедрении инновационных технологий, обеспечивающая повышение эффективности использования ИТ-ресурсов организации и снижению новых видов ИТ-рисков, связанных с нарушениями цифровой безопасности за счет инновационных технологий.

В третьей главе излагаются практические положения диссертации, заключающиеся в практической реализации механизма согласования интересов при управлении цифровой безопасностью критической инфраструктуры организации при внедрении инновационных технологий. Представляются результаты разработки алгоритма согласования интересов при управлении цифровой безопасностью организации при внедрении инновационных технологий, алгоритма согласования ИТ-рисков при управлении цифровой безопасностью организации при внедрении инновационных технологий, алгоритма согласования требований бизнеса при управлении цифровой безопасностью организации при внедрении инновационных технологий. Предлагается комплексный механизм согласования интересов для управления цифровой безопасностью организации при внедрении инновационных технологий. Представляются результаты разработка рекомендаций по совершенствованию механизма согласования интересов для управления цифровой безопасностью организации при внедрении инновационных технологий.

В заключении представлены и сформулированы основные результаты и общие выводы по диссертационной работе, определены пути их эффективной реализации и направления дальнейших исследований по проблематике диссертации.

ОСНОВНЫЕ ПОЛОЖЕНИЯ, ВЫНОСИМЫЕ НА ЗАЩИТУ

1. Формализованный понятийный аппарат и обоснование научно-методического подхода к формированию механизма согласования интересов при управлении цифровой безопасностью при внедрении инновационных технологий

Цифровизация предприятий, интегрируя современные технологии в управление, производство и взаимодействие с клиентами, направлена на оптимизацию функций и повышение конкурентоспособности. Основной целью этого процесса является укрепление позиций на рынке через автоматизацию и внедрение интеллектуальных систем. Тем не менее, развитие цифровизации связано с рисками в области цифровой безопасности. Угрозы кибератак, фишинга и программ-вымогателей растут, что может привести к серьезным финансовым и репутационным потерям из-за утечек критически важной информации. К основным угрозам можно отнести финансовые потери, возникающие как из-за кражи средств, так и из-за убытков от нарушений контрактных обязательств; компрометацию данных, которая ставит под угрозу конфиденциальность; прерывание деятельности, вызывающее задержки и сбои в обслуживании; а также юридическую ответственность, свя-

занную с несоблюдением требований по защите данных. Рисунок 2 отражает субъекты и объекты, участвующие в контуре управления цифровой безопасностью организации:

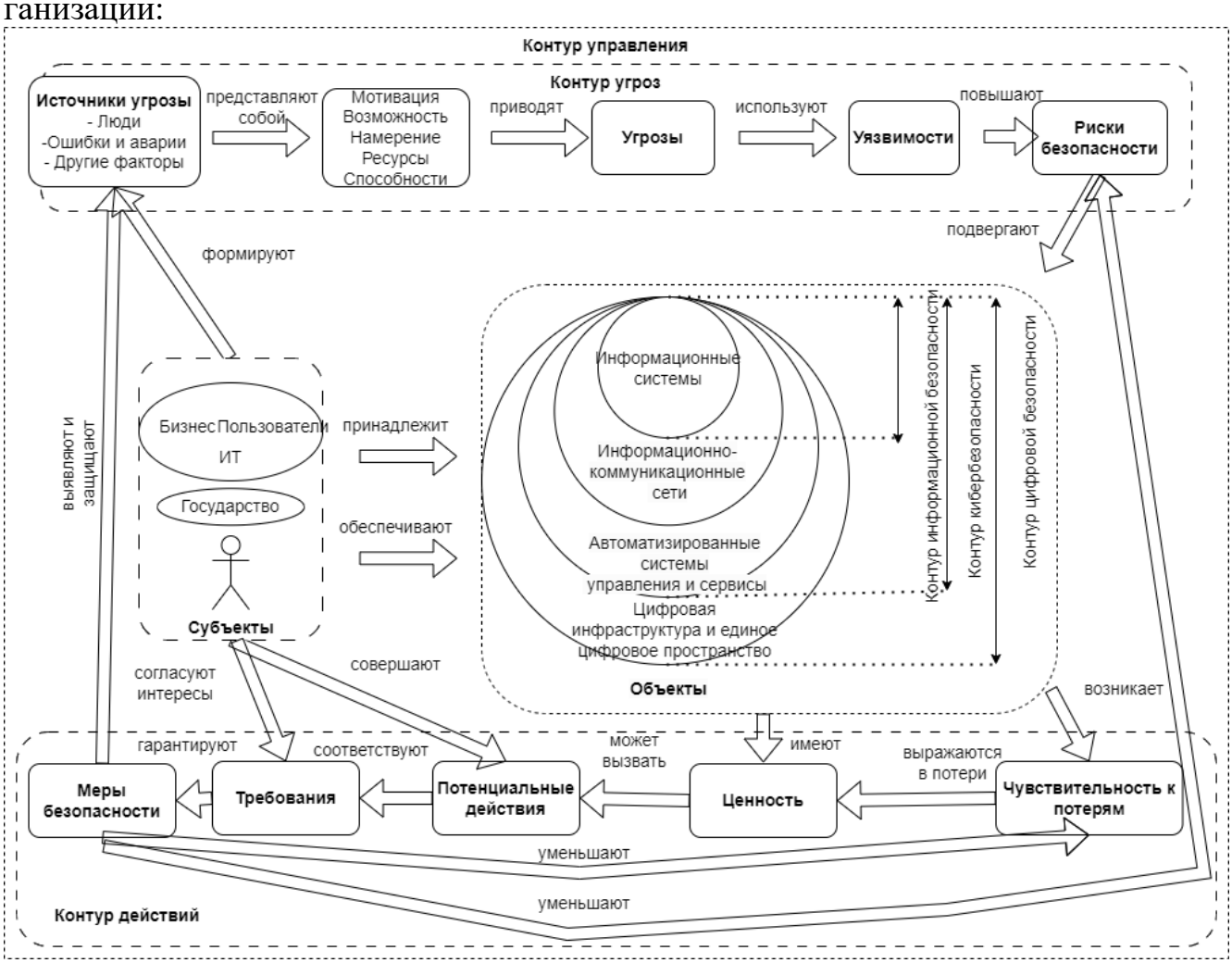


Рисунок 2 – Структурная схема контура управления цифровой безопасностью критической информационной инфраструктуры организации

Для обеспечения необходимых мер цифровой безопасности предприятиям следует разработать комплексные стратегии, которые включают как технические меры, такие как шифрование и аутентификация, так и организационные подходы, например, обучение персонала и подготовку планов реагирования на инциденты.

Важно отметить, что в условиях стремительного развития технологий интеграция фреймворков управления ИТ в бизнес-процессы и их адаптация к требованиям цифровой безопасности становятся жизненно важными для устойчивости организаций и снижения рисков кибератак. Однако процесс внедрения управленческих фреймворков усложняется разнообразием доступных подходов, что требует тщательного анализа их воздействия на цели компании (см. Таблица 1). Реализация таких фреймворков также предполагает значительные инвестиции в технологии и обучение, что может стать проблемой для организаций с ограниченными ресурсами. Кроме того, изменения в рабочих практиках часто встречают сопротивление со стороны сотрудников, привыкших к традиционным методам работы, что создает дополнительные сложности в процессе адаптации к новым условиям. Адаптация

бизнес-процессов к требованиям цифровой безопасности также охватывает критические аспекты, такие как необходимость регулярного обновления защитных механизмов в ответ на постоянно эволюционирующие киберугрозы и внедрение гибких фреймворков, позволяющих компании адаптироваться к изменениям в угрозах. Кроме того, управление рисками информационной безопасности должно стать неотъемлемой частью стратегического планирования, чтобы эффективно минимизировать потенциальные угрозы.

Таблица 1 – Свод требований, корпоративных правил и документов при управлении цифровой безопасностью организации

Основные нормативные документы для ИТ-менеджмента компании	Основные инициативы регуляторов в области ИТ-менеджмента	Основные политики и процедуры ИТ-менеджмента, используемые в России	Основные фреймворки ИТ-менеджмента
Федеральные законы: 149-ФЗ «Об информации…», 152-ФЗ «О персональных данных», 187-ФЗ «О безопасности КИИ», 98-ФЗ «О коммерческой тайне»	Программы импортозамещения ПО и оборудования (Минцифры, Правительство РФ)	Политика ИБ и ИТ-менеджмента, распределение ролей и ответственности (RACI)	ITIL 4 (управление ИТ-услугами)
Подзаконные акты и приказы ФСТЭК: 17, 21, 31, 239, методики по КИИ и ТЗИ	Реестр российского ПО, требования по приоритетному использованию российского ПО	Управление рисками ИТ/ИБ: методика оценки, реестр рисков, план обработки	COBIT 2019 (корпоративное управление ИТ)
Документы ФСБ по криптографии, сертификации СКЗИ и защите ГТ	Инициативы по повышению устойчивости РЗА/КИИ, требования к категорированию объектов КИИ	Классификация и категорирование активов, данные и системы, CMDB	ISO/IEC 27001/27002 (СУИБ и меры)
ГОСТ и ГОСТ Р по ИБ/ИТ: серия ГОСТ Р ИСО/МЭК 2700х, 15408 (Common Criteria), 12207 (ЖЦ ПО), 20000 (СУ Услугами)	Развитие требований по инцидент-репортингу в КИИ и критических секторах	Управление уязвимостями и патч-менеджмент, безопасная конфигурация	NIST CSF 2.0 (Identify–Protect–Detect–Respond–Recover)
Требования Банка России: 382-П, 683-П, Стандарт СТО БР ИББС, указания по киберустойчивости	Инициативы Банка России по киберустойчивости (в т.ч. тесты, обмен индикаторами, ФинСЕРТ)	Управление инцидентами ИБ/ИТ, SOC/SIEM процессы, обмен индикаторами	NIST SP 800-series (управление рисками, инцидентами, контейнерами, облаками)
Закон «О связи», «О связи и связи с ОГИС», нормативы Роскомнадзора по ПДн (локализация, уведомления)	Уточнение практик локализации персональных данных и трансграничной передачи	Политика обработки ПДн, модель угроз ПДн, DPIA/Оценка влияния на ПДн	ISO/IEC 20000-1 (управление ИТ-услугами)

Продолжение таблицы 1

СанПиН/требования отраслевые (медицина, энергетика, транспорт), техрегламенты ЕАЭС	Гармонизация с ЕАЭС/ЕСПД в части сертификации и соответствия	Политика доступа и управления учетными записями, MFA, PAM	TOGAF (архитектура предприятия)
Приказы Минцифры/Минкомсвязи по безопасности госинформсистем (ГИС)	Единые требования к ГИС, интеграционным шлюзам, межведомственному ЭДО	SDLC/SSDLC: требования, дизайн, код-ревью, SAST/DAST, DevSecOps	MITRE ATT&CK/DEFEND (таксономии угроз и защит)
Стандарты и методики по КИИ: категорирование, значимые объекты, планы обеспечения безопасности	Централизация обмена инцидентами (нац. координация), учения/киберполигоны	Резервное копирование и восстановление, DR/BCP, план непрерывности	ISO/IEC 22301 (менеджмент непрерывности)
Требования по криптографии: использование сертифицированных СКЗИ, Гостовые алгоритмы	Обязательная сертификация СКЗИ и средств защиты, импортонезависимость	Управление изменениями (Change/Release), CAB, канареечные релизы	PMBOK/PRINCE2 (управление проектами ИТ)
Требования по журналированию и хранению логов, времени хранения, следам аудита	Инициативы по стандартизации форматов отчётности и лог-экспорта	Логирование, мониторинг, корреляция событий, хранение и форензика	CIS Controls v8 (базовые практики безопасности)
Требования к аутсорсингу/аутстаффингу, договорам и SLA по ИБ	Усиление требований к третьим сторонам и цепочкам поставок	Управление поставщиками: due diligence, TPRM, требования в контрактах	ISO/IEC 27701 (расширение к 27001 по приватности)
Требования по защите облачных сервисов и ЦОД (в т.ч. сертификация площадок)	Инициативы по суверенным облакам, облигации к хранению данных в РФ	Политика облачной безопасности, классификация данных, CASB	ISO/IEC 27017/27018 (облака и персональные данные)
Нормативы по безопасной разработке ГИС/КИИ и SBOM/учёт компонентов	Инициативы по обязательному SBOM для критичных систем	Управление зависимостями, SBOM, SCA, политика подписей артефактов	OWASP SAMM/ASVS (зрелость и требования приложений)
Требования по защите рабочих мест и мобильных устройств	Инициативы по EDR/XDR как обязательным для критических отраслей	EDR/XDR, MDM/MAM, политика BYOD, шифрование на конечных точках	SAFE/Scaled Agile + DevSecOps практики

Согласование процессов цифровой безопасности с общими целями организации играет важную роль в повышении эффективности и конкурентоспособности организации.

Рисунок 3 представляет формализованный понятийный аппарат и обоснование научно-методического подхода к формированию механизма согласования интересов при управлении цифровой безопасностью при внедрении инновационных технологий:

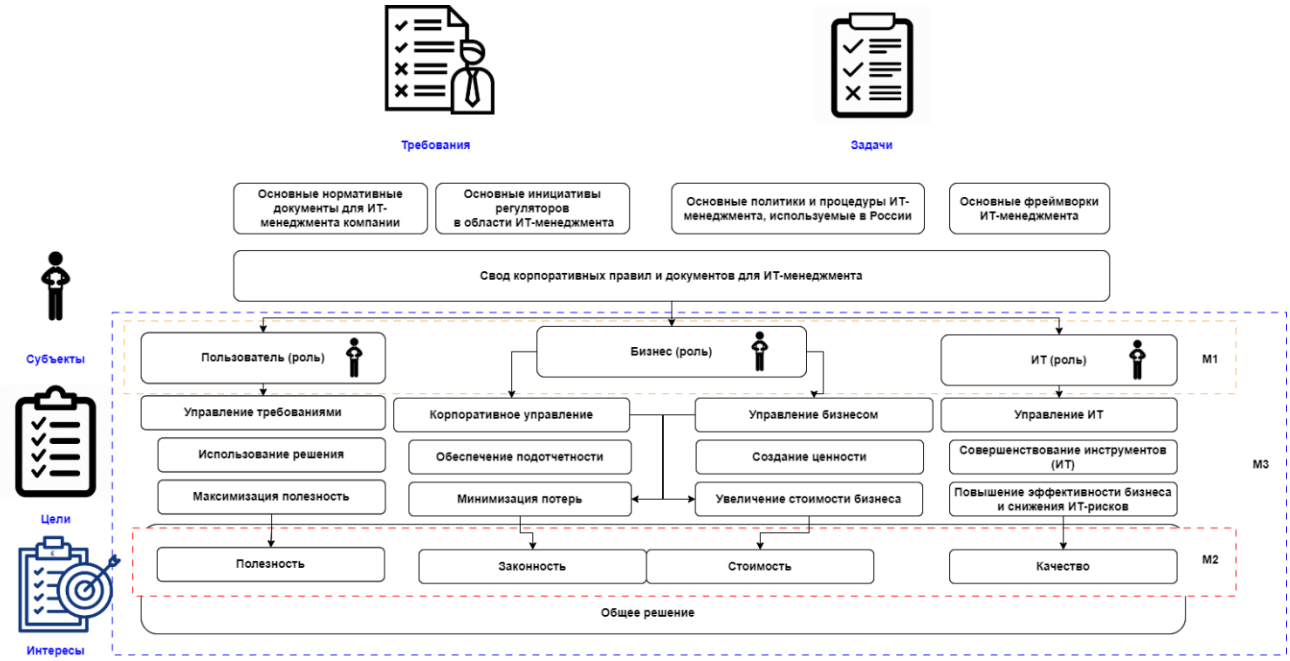


Рисунок 3 – Структурная схема механизма цифровой безопасности при внедрении инновационных технологий для системы «Организация-Субъекты»

Решение этих сложных вопросов требует комплексного подхода, в который необходимо включить организационно-экономический анализ и управление изменениями на всех уровнях, что позволит достичь устойчивого развития и низкого уровня рисков в условиях современного бизнеса.

В соответствии с поставленной научной задачей, в диссертации предложен и обоснован научно-методический подход к ее решению, суть которого состоит в комплексности модели принятия решений за счет согласования интересов системы цифровой безопасности критической инфраструктуры «Организация - Субъекты»

– модель оценки интересов системы «Организация-Субъекты» цифровой безопасности на основе функции полезности (M1) для повышения уровня согласованности интересов субъектов цифровой безопасности за счет создания механизма согласования для защиты и предупреждения новых видов цифровых угроз.

Разрабатывается на основе теоретико-игровых моделей;

– модель оценки стоимости цифровой угрозы при внедрении инновационной технологии (M2) для согласования интересов субъектов цифровой безопасности организации за счет учета новых ИТ-рисков цифровой безопасности.

Разрабатывается на основе комбинации классического риск-менеджмента, управления инновационными рисками и подходов управления ИТ-рисками;

– метод согласования интересов системы «Организация-Субъекты» цифровой безопасности на основе совокупной функции полезности (M3) для повышения уровня согласованности интересов субъектов цифровой безопасности за счет механизма согласования целей бизнеса, ИТ-организаций и конечного пользователя.

Разрабатывается на основе комбинации комплаенс-подхода и теоретико-игровых подходов согласования интересов.

Научная новизна. В результате анализа актуальной теории и практики, и обнаруженных ограничений, возникающих при управлении цифровой безопасностью организации, предложен формализованный понятийный аппарат и систематизация актуальной практики согласования интересов субъектов при управлении цифровой безопасностью при внедрении инновационных технологий на основе исследования международных и отечественных регламентирующих документов, общепринятых стандартов и фреймворков по безопасности информации, кибер- и цифровой безопасности организации, руководств и групп знаний в области цифровой безопасности организации. Обоснован научно-методический подход к разработке механизма согласования интересов субъектов для управления цифровой безопасностью при внедрении инновационных технологий, отличающийся комплексностью модели принятия решений за счет согласования интересов системы «Организация - Субъекты» цифровой безопасности критической информационной инфраструктуры организации (далее ЦБКИИО) , что позволяет получить синергию преимуществ от разработанных методов при решении специфических экономических задач за счет формирования комплексной модели согласованности действий по цифровой безопасности организации.

2. Модель оценки «интересов» системы цифровой безопасности «Организация-Субъекты» на основе функции полезности

Существующий научный задел в области цифровой безопасности сосредоточен на технологических элементах, инвестициях и сотрудничестве между государственным и частным секторами, однако недостаточно внимания уделяется ценностям, создаваемым для заинтересованных сторон. Такой пробел затрудняет формулирование бизнес-стратегий и повышает уязвимость поставщиков цифровой безопасности. Инвестиции в цифровую безопасность критически важны для снижения рисков и последствий инцидентов, но их недостаток ведет к увеличению этих рисков и экономическим потерям.

Для анализа инвестиционных решений в области цифровой безопасности полезна теория игр, так как традиционные методы управления рисками не учитывают динамику стратегий хакеров. Этот подход позволяет оптимально распределять ресурсы цифровой безопасности, учитывая не только финансовые обоснования, но и нефинансовые выгоды, которые могут быть упущены при узком финансовом анализе.

При принятии решений лицом, принимающим решения (далее ЛПР), часто стремится максимизировать ожидаемую полезность, которая зависит от корпоративных "выигрышей". В отличие от традиционного подхода максимизации прибыли, теория ожидаемой полезности учитывает, как корпоративные интересы, так и индивидуальные характеристики ЛПР, включая его профиль риска. Это позволяет более точно оценивать, насколько продукт или услуга удовлетворяет ожиданиям конечного пользователя, что в свою очередь способствует лучшему согласованию интересов в системе цифровой безопасности «Организация-Субъекты».

$$U = \sum_{i=1}^{n} \left(w_i \cdot v_i(x_i) \right) - C \,, \quad (1)$$

где U – чистая полезность для пользователя.

n – количество аспектов или характеристик продукта, которые влияют на полезность. w_i – весовой коэффициент i-го аспекта, отражающий его значимость для пользователя. $v_i(x_i)$ – функция полезности i-го аспекта, зависящая от уровня x_i этого аспекта. C – суммарные издержки или негативные факторы, связанные с использованием продукта.

Функция полезности отражает все функциональные и нефункциональные преимущества, которые конечный пользователь получает в момент достижения эффективного уровня цифровой безопасности с помощью решения по ЦБКИО и соответствующих источников информации. Чистая полезность пользователя представляет собой разность между всеми положительными выгодами и затратами, связанными с использованием этих решений и источников.

Научная новизна. Модель отличается теоретико-игровой формализацией задачи баланса новых потребностей цифровой среды организации и новых видов цифровых угроз посредством совместного создания полезности, и позволяет оценить параметры создаваемый полезности для каждого типа рассматриваемого субъекта.

3. Модель оценки стоимости цифровой угрозы при внедрении инновационной технологии

Междисциплинарный анализ показывает, что процессы вредоносной активности в цифровых системах и динамика инфекционных заболеваний обладают структурной схожестью: у них общие механизмы передачи, сопоставимые состояния системы и узлов, пороговые эффекты и близкие экономико-математические описания, что позволяет рассматривать инциденты как поток событий во времени, а ущерб – как интеграл по траектории состояний, аккумулирующий совокупные потери с учетом интенсивности заражения, длительности воздействия и эффективности реагирования.

В этой аналогии узлы цифровой сети соответствуют агентам в эпидемиологической модели, контакты определяются топологией связности и частотой взаимодействий, а вероятность успешной атаки на контакт выступает прокси для базового числа воспроизводства. Узлы с высокой центральностью функционируют как суперраспространители, и направленная защита на них оказывает непропорционально сильный эффект: снижение активности на высокоцентральных компонентах резко уменьшает как краткосрочный риск, так и ожидаемые интегральные потери по горизонту.

Экономико-математическая оценка стоимости цифровой угрозы при внедрении инновационной технологии целесообразна по аналогии с SIR-динамикой распространения новых заболеваний. Пусть N – численность всех систем, а S(t), I(t),

R(t) – доли защищенных, уязвимых и восстановленных соответственно; β коэффициент передачи угрозы, γ – коэффициент «выздоровления». Тогда динамика – задается SIR-системой

:

$$\begin{cases} \dfrac{dS}{dt} = -\beta \dfrac{S(t)I(t)}{N} \\ \dfrac{dI}{dt} = \beta \dfrac{S(t)I(t)}{N} - \gamma I(t) \\ \dfrac{dR}{dt} = \gamma I(t) \end{cases}, \quad (2)$$

где N – общее число систем (аналог населения в эпидемиологических моделях);

$I(t)$ – число инфицированных (уязвимых) систем в момент времени t;

$S(t)$ – число устойчивых (защищенных) систем в момент времени t;

$R(t)$ – число систем, которые перешли в состояние устойчивости после атаки или интервенции (аналог выздоровевших);

β – коэффициент передачи угрозы, аналогичен коэффициенту заражения в модели распространения болезней;

γ – коэффициент «выздоровления» систем, то есть вероятность перехода из состояния I в R за единицу времени;

Ожидаемая стоимость угрозы естественным образом связывается с динамикой доли уязвимых, испытывающих воздействие, систем *I(t)*: при введении параметров ρ как интенсивности реализации ущерба для одной уязвимой системы за единицу времени и C как среднего ущерба на систему мгновенный риск-убыток *L(t)* определяется как произведение этих величин на текущую долю активных инцидентов, то есть $L(t) = \rho \cdot C \cdot I(t)$. Калибровка ключевых параметров модели проводится на основе эмпирических источников, включающих журналы инцидентов, частоту и своевременность обновлений, среднее время обнаружения и восстановления, а также внешние отраслевые бенчмарки, что обеспечивает идентифицируемость и переносимость оценок. Снижение частоты межсистемной передачи инцидентов и ускорение их разрешения приводят к уменьшению *I(t)* на всем горизонте, что непосредственно снижает ожидаемые потери через *L(t)*. Такая комбинация временного поведения угроз с денежными метриками позволяет рационально планировать проверки и тесты, формировать приоритизацию инвестиций в защитные меры, а также проводить последующую оценку эффекта в стоимостном выражении, выделяя вклад мер, которые сократили распространение, ускорили восстановление и указали на остаточные узкие места.

Научная новизна. Модель отличается гибридизацией подходов оценки рисков новых видов угроз цифровой безопасности и подходов оценки экономической эффективности информационных решений и мер по обеспечению цифровой безопасности. Такой подход позволяет выбрать лучшую методику оценки эффективности инвестиций в меры обеспечения цифровой безопасностью организации на основе новых подходов и технологий.

4. Метод согласования интересов системы «Организация-Субъекты» цифровой безопасности на основе совокупной функции полезности

В рамках теории ожидаемой полезности для субъектов, избегающих рисков, оптимальный объем инвестиций в цифровую безопасность (ЦБКИИО) зависит от уровня потенциальных убытков от инцидентов, не превышая их максимальный размер. Существует минимальный порог потерь, ниже которого оптимальные инвестиции равны нулю, что указывает на то, что вложения в безопасность не всегда пропорциональны степени принятия рисков. Моделируя поведение ответственного лица на предприятии, использующего теорию ожидаемой полезности, можно определить объем инвестиций, который максимизирует полезность в контексте инвестиционной стратегии.

$$U = f(F, T, H, M, P) \xrightarrow[\substack{F \le F_{max} \\ T \le T_{max} \\ H \le H_{max} \\ M \le M_{max} \\ P \le P_{max}}]{} max, \quad (3)$$

где финансовые ресурсы (F);
технологические ресурсы (T);
человеческие ресурсы (H);
маркетинговые и снабженческие ресурсы (M);
производственные ресурсы (P);
$F_{max}, T_{max}, H_{max}, M_{max}, P_{max}$- доступное количество каждого ресурса.

Для анализа инвестиций в цифровую безопасность необходимо рассмотреть событие нарушения безопасности, которое происходит с определенной вероятностью и может привести к фиксированным потерям. Эти потери могут быть как прямыми, связанными с денежным ущербом, так и косвенными, например, ухудшением репутации или юридической ответственностью. Вероятность нарушения безопасности зависит от такой переменной как инвестиции в защиту, внутренней уязвимости систем и внешний риск, представленный хакерской активностью. Внутренняя уязвимость определяется архитектурой информационных систем и их доступностью. Например, система, полностью изолированная от внешних угроз, будет менее уязвима. Выполним переопределение функции полезности (1) с учетом (2) и формализацией (3):

$$U = \sum_{i=1}^{n} \left(w_i \cdot v_i(x_i)\right) - C - w_{R_{DS}} R_{DS}(t) =\cdot \sum_{i=1}^{n} \left(w_i \cdot v_i(x_i)\right) - C - w_{R_{DS}} \cdot \rho \cdot I_{DS}(t) \quad (4)$$

На основе подхода к архитектуре информационных систем и функциональных и нефункциональных требований к ПО, где F – функциональные преимущества, N – нефункциональные преимущества, а R – негативные последствия, изменим (4):

$$\begin{cases} F = \sum_{i=1}^{n} \left(w_i \cdot v_i(x_i)\right); \\ N = C; \\ R = w_{R_{DS}} \cdot \rho \cdot I_{DS}(t); \end{cases} : U = F + N - R \quad (5)$$

Методы оценки удобства использования (5) играют ключевую роль в оптимизации взаимодействия пользователей с продуктами, что ведет к повышению удовлетворенности и улучшению восприятия. В контексте IT-вендоров цифровой безопасности функциональные преимущества касаются эффективности защиты от кибератак и легкости интеграции с существующими системами. Нефункциональные преимущества, такие как репутация вендора и качество обслуживания, также важны, наряду с его адаптивностью к изменениям. Однако, существуют и негативные последствия, например, сложности реализации и риск несоответствия правовым требованиям.

Для бизнеса, использующего решения в области цифровой безопасности, значительными функциональными преимуществами становятся как повышение уровня защиты, так и соблюдение нормативных требований. Нефункциональные аспекты воздействия проявляются через снижение стресса сотрудников и улучшение репутации компании. В свою очередь, негативные последствия включают высокую стоимость внедрения и возможное снижение производительности из-за дополнительных мер безопасности.

Для эффективной систематизации всех этих аспектов можно разработать таблицу, позволяющую динамически представлять функциональные и нефункциональные преимущества, а также негативные последствия, делая анализ более структурированным и понятным для принятия решений.

Научная новизна. Метод отличается гибридизацией подходов оценки экономической эффективности информационных решений и мер по обеспечению цифровой безопасности на основе функции полезности и ИТ-подхода функциональных и нефункциональных преимуществ, который позволяет выбрать лучшую методику согласования интересов системы цифровой безопасности «Организация-Субъекты» при оценке эффективности инвестиций в решения по управлению цифровой безопасностью организации.

5. Бизнес-процессная архитектура механизма цифровой безопасности при внедрении инновационной технологии для согласования ИТ-рисков

При создании единой бизнес-процессной архитектуры цифровой безопасности важно согласование интересов организации и партнеров. В этом процессе ключевую роль играет IT-управление как система интеграции и взаимодействия всех элементов цифровой инфраструктуры. Стратегическое выравнивание ИТ и бизнеса обеспечивает соответствие ИТ-инициатив целям организации, повышая их вклад в корпоративные результаты.

Соблюдение нормативных требований становится не только гарантией легитимности, но и поддерживает устойчивость и конкурентоспособность бизнеса. Управление ИТ-рисками основано на систематическом выявлении и снижении угроз, что уменьшает вероятность инцидентов и потери от них.

Архитектура цифровой безопасности организации представляет собой системное описание встраивания защитных механизмов в устройства, приложения, данные, сетевую инфраструктуру, бизнес-процессы и организационные роли. Поэтому она не сводится к отдельному документу или продукту, а формируется как согласованная стратегия принципов, моделей и артефактов, задающих расположение и способ реализации мер защиты, распределение ответственности за их выполнение, а также характер их взаимодействия на всех фазах жизненного цикла ИТ.

Рисунок 4 представляет практическую реализацию алгоритма согласования:

Рисунок 4 – Бизнес-процесс согласования интересов для управления цифровой безопасностью организации при внедрении инновационных технологий

Бизнес-процессная архитектура цифровой безопасности и алгоритм согласования при внедрении инноваций строятся на интеграции комплаенс-подхода в отношения «Организация-Субъекты». Такой подход позволяет создать устойчивую систему управления ИТ-рисками, адаптированную к нормативным требованиям и обеспечивающую прозрачность процессов цифровой трансформации. Рисунок 5 представляет процессную архитектуру взаимодействия стейкхолдеров системы (клиенты, бизнес, ИТ-компании), «точки возникновения сложности» и согласования интересов:

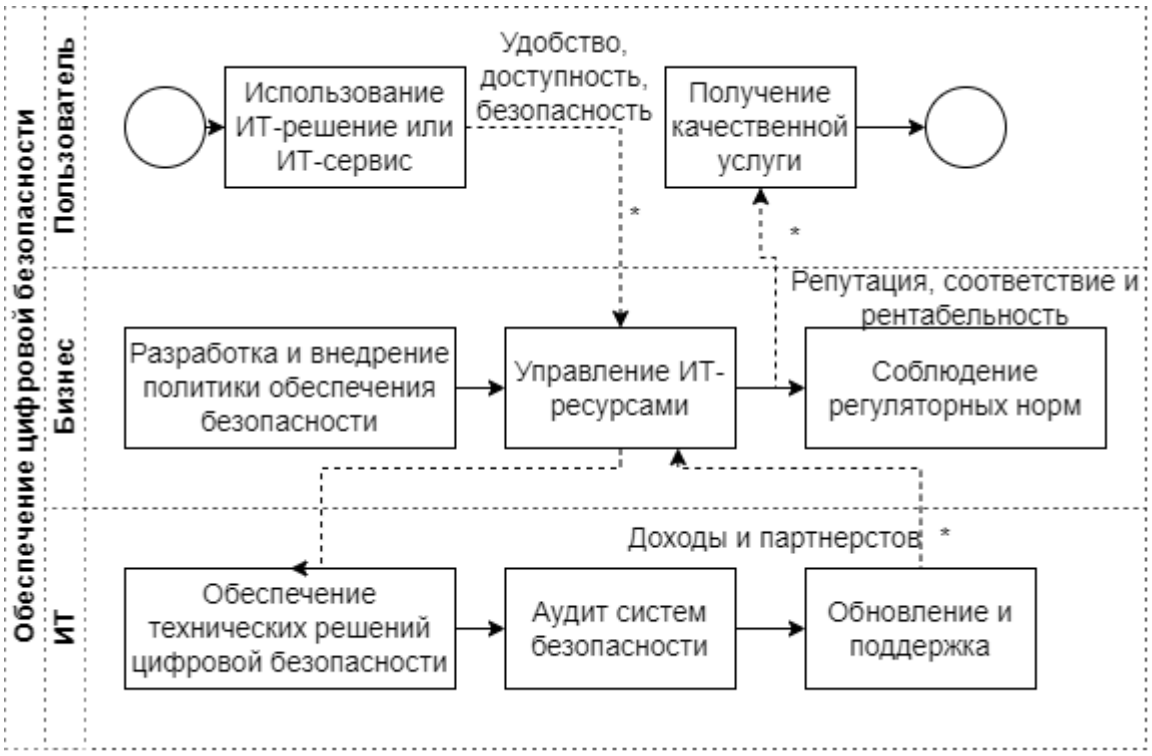


Рисунок 5 – Процессная архитектура взаимодействия стейкхолдеров системы (клиенты, бизнес, ИТ-компании), «точки возникновения сложности» и согласования интересов

Механизм согласования выступает основным инструментом для выявления и минимизации рисков инновационных проектов, используя стандартизированные процедуры и расширяя регламентацию информационных потоков. Это снижает вероятность нарушений и последствия внешних и внутренних угроз.

Согласование управленческих решений на базе принципов согласования обеспечивает баланс интересов бизнеса, угроз и нормативных требований, способствует целостному управлению рисками и выполнению обязательств перед регуляторами, а также повышает устойчивость и согласованность цифровой инфраструктуры в условиях быстро меняющейся технологической среды.

Научная новизна. Алгоритм согласования и архитектурная стратегия механизма цифровой безопасности при внедрении инновационных технологий отличается динамической адаптивностью и кросс-функциональностью, обеспечивая комплексное управление ИТ-рисками на всех этапах процесса, и позволяет гибко учитывать интересы всех участников, своевременно реагировать на изменяющиеся угрозы и поддерживать устойчивое развитие организации в условиях цифровой трансформации.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Механизм согласования интересов в системе цифровой безопасности «Организация-Субъекты» требует осознания, что организациям, сталкивающимся с рисками, необходимо оценивать угрозы в контексте их потенциального ущерба. Такой подход позволяет избежать чрезмерных инвестиций в защиту, особенно если ожи-

даемые убытки не превышают определенный уровень. Основной принцип заключается в том, что затраты на меры безопасности должны быть оправданы ожидаемыми выгодами от предотвращения инцидентов. Существующая связь между уровнем риска и оптимальными вложениями в безопасность требует комплексной оценки для эффективного распределения ресурсов.

Инвестиции в безопасность должны соотноситься со степенью уязвимости систем: если объекты подвергаются целенаправленным атакам, увеличение затрат на защиту оправдано, тогда как в случае с распределенными угрозами необходимо сосредоточиться на наиболее защищенных элементах. В условиях цифровой трансформации также требуется разработка универсальных рекомендаций, включая шифрование данных, использование защищенных сетей и надежных методов аутентификации.

Активный мониторинг систем предусмотрен для предотвращения атак, включая как внешние, так и внутренние угрозы. Внутренние риски, связанные с действиями сотрудников, требуют особого внимания, в частности внедрения систем обнаружения угроз для оперативной реакции. Управление доступом, включая современные методы аутентификации, такие как биометрия и двухфакторная аутентификация, играет критическую роль.

Обучение сотрудников цифровой безопасности существенно снижает риски, связанные с человеческим фактором. Разработка планов реагирования на инциденты способствует быстрой ликвидации угроз и минимизации возможного ущерба через установление четких процедур восстановления. Таким образом, реализация предложенных мер в процессе цифровой трансформации позволит значительно снизить риски, обеспечить устойчивое развитие и повысить безопасность цифровых активов организации.

В рамках диссертации апробация организационно-экономического механизма осуществляется на базе ОАО «В/О «Авиаэкспорт».

Далее можно выполнить расчет чистого экономического эффекта (Выгоды – Затраты) по методике Total Economic Impact (TEI):

$$Total\ Economic\ Impact = NPB + F - R\ :\ NPB = (Bd + Bi) - (Cd + Ci) \qquad (5)$$

где Bd – суммарные прямые выгоды;

Bi – суммарные косвенные выгоды;

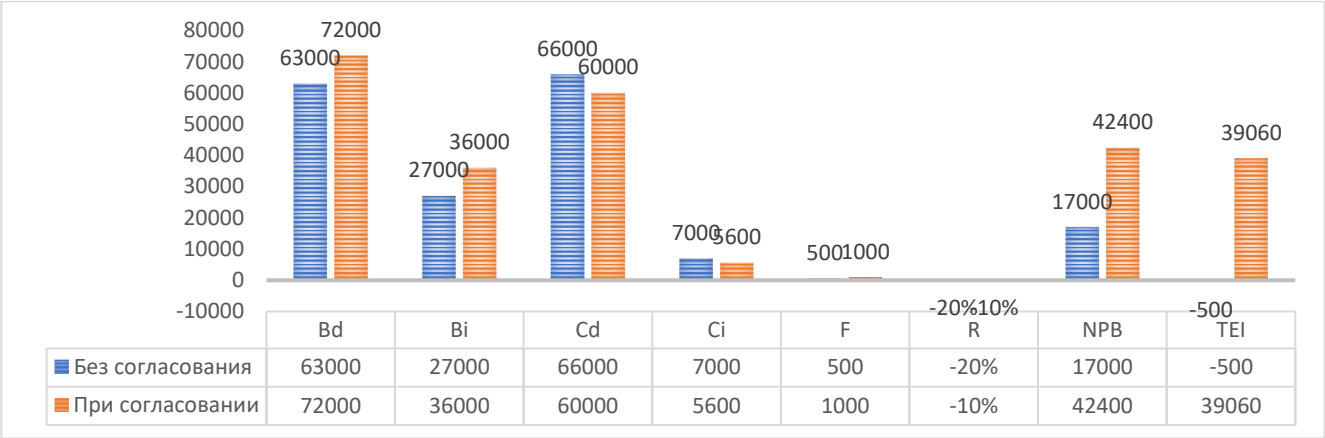
Cd – суммарные прямые затраты на внедрение;

Ci – суммарные косвенные затраты на внедрение;

F – выгода от гибкости применения технологий;

R – сумма потенциальных потерь из-за рисков;

Рисунок 6 представляет результаты расчета общей экономической эффективности с учетом гибкости технологий и факторов риска методом *TEI*:



	Bd	Bi	Cd	Ci	F	R	NPB	TEI
Без согласования	63000	27000	66000	7000	500	-20%	17000	-500
При согласовании	72000	36000	60000	5600	1000	-10%	42400	39060

Рисунок 6 – Результаты расчета общей экономической эффективности с учетом гибкости технологий и факторов риска методом TEI без согласования интересов и при согласовании

Алгоритм оценки эффективности внедрения механизма управления цифровой безопасностью, базирующийся на методике Total Economic Impact (TEI), включает расчёт трёх основных финансово-экономических показателей: чистой приведенной стоимости (Net Present Value, NPV), внутренней нормы доходности (Internal Rate of Return, IRR) и периода окупаемости (Payback Period).

$$NPV_{TEI} = \sum_{t=0}^{n} (B_t - C_t) \Big/ (1+r)^t \quad (5)$$

где B_t – выгоды (benefits) в году t;
C_t – затраты (costs) в году t;
r – ставка дисконтирования;
t – год расчёта (от 0 до n);
n – общее количество лет.

Выгоды и затраты от внедрения системы управления цифровой безопасностью (для угрозы – компрометация учетных записей) без согласования и при согласовании интересов распределены по годам следующим образом (см. Таблица 2):

Таблица 2 – Чистые текущие выгоды (Net Present Benefits, NPB), млн. руб.:

	Без согласования		При согласовании	
Год	Выгоды B_t	Затраты C_t	Выгоды B_t	Затраты C_t
0	0	3	0	2,5
1	2,5	1,5	3,5	1
2	3	1,2	3,5	1
3	3	0,8	3,5	0,5
4	3	0,8	3,5	0,5

Примем, что ставка дисконтирования r=35%. Расчет без согласования интересов:

$$NPV_{TEI} = \frac{0-3}{(1+0{,}35)^0} + \frac{2{,}5-1{,}5}{(1+0{,}35)^1} + \frac{3-1{,}2}{(1+0{,}35)^2} + \frac{3-0{,}8}{(1+0{,}35)^3} + \frac{3-0{,}8}{(1+0{,}35)^4}, = -3 + 0{,}741 + 0{,}988 + 0{,}894 + 0{,}662 = 0{,}28 \text{ млн руб.} \quad (6)$$

Расчет при согласовании интересов:

$$NPV_{TEI} = \frac{0-2{,}5}{(1+0{,}35)^0} + \frac{3{,}5-1}{(1+0{,}35)^1} + \frac{3{,}5-1}{(1+0{,}35)^2} + \frac{3{,}5-0{,}5}{(1+0{,}35)^3} + \frac{3{,}5-0{,}5}{(1+0{,}35)^4}, = -2{,}5 + 1{,}85 + 1{,}37 + 1{,}22 + 0{,}9 = 2{,}85 \text{ млн. руб.} \quad (7)$$

Цифровая безопасность представляет собой комплекс мер, ориентированных на защиту критической информации от несанкционированного доступа, изменения или уничтожения, и включает управление доступом, шифрование данных и реагирование на инциденты. Учитывая постоянное развитие угроз, организациям необходимы не только первоначальные инвестиции, но и постоянное внимание к обновлению и совершенствованию защитных механизмов.

Также необходимо учитывать, что расходы на цифровую безопасность включают не только приобретение новых технологий, но и обучение сотрудников, регулярные аудиты и тестирования, обновление программного обеспечения и оборудование, а также разработку политики и процедур для безопасного управления данными. Таким образом, механизмы согласования интересов между «Организацией» и «Субъектами» становятся критически важными для создания эффективной системы цифровой безопасности.

ЗАКЛЮЧЕНИЕ

1. Результаты обобщения актуальных теоретических и практических работ по теме исследования позволяют сделать вывод о том, что в согласование интересов при управление цифровой безопасностью должно быть рассмотрено как комплексная модели принятия решений за счет согласования интересов системы ЦБКИО «Организация - Субъекты», поэтому необходимо использовать гибридизацию экономико-математических методов управления жизненным циклом цифровых ресурсов, управления цифровой безопасностью организации, формализации неопределенности при принятия экономических решений, методов анализа и управления рисками, для построение комплексного механизма.

2. Разработан формализованный понятийный аппарат согласования интересов для управления цифровой безопасностью при внедрении инновационных технологий, отличающийся учетом специфики оценки новых цифровых вызовов и уязвимостей при согласовании интересов субъектов безопасности цифровой среды организации, что позволяет предложить общую терминологическую базу механизмов поддержки принятия решений.

3. Исходя из результатов выполненного анализа современной практики в контексте безопасности цифровой среды организации в диссертации предложен научно-методический подход к разработке механизма согласования интересов для управления цифровой безопасностью при внедрении инновационных технологий, отличающийся учетом оценки новых цифровых вызовов и уязвимостей и использованием современных экономико-математических подходов (кооперативно-игрового и мягкого моделирования), что позволяет получить комплекс методов для решения специфических задач согласования интересов для управления цифровой безопасностью.

4. Разработан комплекс методов и моделей для принятия решений за счет согласования интересов системы ЦБКИИО «Организация - Субъекты», что позволяет получить синергию преимуществ от разработанных методов при решении специфических экономических задач за счет формирования комплексной модели согласованности действий по цифровой безопасности организации.

5. Выполнена апробация и предложены рекомендации по практической реализации механизма согласования интересов системы цифровой безопасности «Организация-Субъекты» при внедрении инновационных технологий.

Результаты диссертации позволяют сделать вывод о том, что поставленная научная задача решена, а цель диссертации достигнута. Выполненное диссертационное исследование обеспечивает согласования интересов заинтересованных лиц в процессе принятия решений при управлении цифровой безопасностью организации при внедрении инновационных технологий. Направлениями дальнейших исследований по проблематике диссертации являются вопросы инструментальной реализации разработанных подходов, на основе существующих и перспективных цифровых решений в области принятия экономических решений.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Научные статьи в рецензируемых журналах, рекомендованных ВАК при Минобрнауки России (5.2.3.)

1. Павлов М. А., Шиболденков В.А Когнитивный подход к бизнес-аналитике при оценке цифровых рисков безопасности в процессе внедрения новых технологий // Экономика, предпринимательство и право. 2025. Т. 15, № 3. С. 1433-1452. DOI 10.18334/epp.15.3.122783 (1 п.л. / 0,5 п.л.).

2. Павлов М.А. Механизм управления технологическими рисками в условиях цифровой трансформации организации // Экономика и предпринимательство. 2024. № 7(166). С. 1089-1098. (1 п.л.).

3. Павлов М.А. Методика поддержки принятия решений по управлению проектами цифровой безопасности организации на основе подхода системы согласования интересов, угроз, инновационных рисков и требований бизнеса // Экономика и предпринимательство. 2024. № 3(164). С. 1330–1339. (1 п.л.).

4. Павлов М.А., Шиболденков В.А. Подход риск-контроллинга киберугроз и обеспечения цифровой безопасности организации // Контроллинг. 2024. № 3(93) С. 70-78 (1 п.л. / 0,5 п.л.).

Научные статьи в рецензируемых журналах, рекомендованных ВАК при Минобрнауки России

5. Павлов М.А. Фреймворки управления информационными технологиями и киберрисками при цифровой трансформации организации // Динамика сложных систем. 2024. С. 5-15. (1 п.л.)

6. Павлов М.А. Криминологические меры борьбы с преступлениями в сфере компьютерной информации // Студенческий: электрон. научн. журн. 2023. № 40(252). С. 5-7. (0,15 п.л.)

Научные статьи и тезисы докладов в сборниках трудов международных и всероссийских конференций

7. Павлов М.А. Вопросы кибербезопасности и ИТ-рисков обеспечения непрерывности наукоемкого производства // Тринадцатые Чарновские Чтения. Сборник трудов XIII Всероссийской научной конференции по организации производства. Форум современное предприятие и будущее России. Москва, 1 декабря 2023 г. М.: МГТУ им. Н. Э. Баумана, НП «Объединение контроллеров», 2023. С.107 -116 (0,5 п.л.)

8. Павлов М.А., Шаброва А.С., Князев М.А. Оценка экономической эффективности инвестиций в кибербезопасность при цифровой трансформации производственных систем // Тринадцатые Чарновские Чтения. Сборник трудов XIII Всероссийской научной конференции по организации производства. Форум современное предприятие и будущее России. Москва, 1 декабря 2023 г. М.: МГТУ им. Н. Э. Баумана, НП «Объединение контроллеров», 2023. С. 116-128. (0,5 п.л. / 0,25 п.л.)

9. Павлов М.А. Обзор стандартных практик риск-ориентированного обеспечения кибербезопасности при цифровой трансформации организации // Актуальные вопросы

экономики, менеджмента и инноваций: материалы Международной научно-практической конференции. Нижегород. гос. техн. ун-т им. Р.Е. Алексеева. Нижний Новгород, 2023. С.132-138. (0,35 п.л.)

10. Павлов М. А. Интеллектуальная оценка киберрисков цифровой трансформации организации на основе метода анализа компромиссов / ИИАСУ'23 - Искусственный интеллект в автоматизированных системах управления и обработка данных: Сборник статей II Всероссийской научной конференции (Москва, 27-28 апреля 2023 г.): в 5 т. - М.: "КДУ", "Добросвет", 2024. С.50-57. Электронное издание сетевого распространения. URL: https://bookonlime.ru/node/74577/ - doi: 10.31453/kdu.ru.978-5-7913-1354-6-2024-488. (0,5 п.л.)

11. Дроговоз П.А., Коренькова Д. А., Павлов М. А. Кибербезопасность в международной космической индустрии: кооперативно-игровой подход к гармонизации экономических интересов стейкхолдеров. // XLVI Академические чтения по космонавтике, посвященные памяти академика С.П. Королёва и других выдающихся отечественных ученых – пионеров освоения космического пространства (Москва, 25–28 января 2022 г.): сборник тезисов в 4 т. / Российская академия наук, Государственная корпорация по космической деятельности «Роскосмос», Комиссия РАН по разработке научного наследия пионеров освоения космического пространства, Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)». Москва: Издательство МГТУ им. Н. Э. Баумана, 2022. Т. 1. С. 48-52. (0,5 п.л. / 0,15 п.л.).

12. Павлов М.А. Ложная информация, дезинформация и фейковые новости как факторы возникновения киберрисков в цифровой экономике // Актуальные вопросы экономики, менеджмента и инноваций: материалы Международной научно-практической конференции. Нижегород. гос. техн. ун-т им. Р.Е. Алексеева. Нижний Новгород, 2021. С. 59-62. (0,5 п.л.)