МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права

(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

40.05.01 Правовое обеспечение национальной безопасности

(код и наименование направления подготовки / специальности)

Государственно-правовая

(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему «Министерство цифрового развития, связи и массовых коммуникаций в системе органов, обеспечивающих национальную безопасность»

Обучающийся

Д.М. Уртанбаева

(Инициалы Фамилия)

(личная подпись)

Руководитель

канд. юрид. наук, доцент А.А. Мусаткина

(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Аннотация

Актуальность темы исследования обусловлена возрастающей ролью цифровых технологий в обеспечении национальной безопасности Российской Федерации и необходимостью эффективного государственного управления процессами цифровой трансформации общества. В условиях глобальной цифровизации и усиления информационного противоборства особую значимость приобретает деятельность Министерства цифрового развития, связи и массовых коммуникаций РФ как ключевого органа, ответственного за реализацию государственной политики в сфере цифрового развития и обеспечения информационной безопасности страны.

Цель исследования заключается в комплексном теоретико-правовом анализе места и роли Министерства цифрового развития, связи и массовых коммуникаций РФ в системе органов, обеспечивающих национальную безопасность, а также выявлении проблем и определении направлений совершенствования его деятельности в данной сфере.

Объектом исследования выступают общественные отношения, возникающие в процессе деятельности Министерства цифрового развития, связи и массовых коммуникаций РФ по обеспечению национальной безопасности.

Предметом исследования являются нормативные правовые акты, регулирующие деятельность Министерства цифрового развития в сфере обеспечения национальной безопасности, а также практика их применения.

Структура работы обусловлена целью и задачами исследования и включает введение, три главы, состоящие из семи параграфов, заключение и список используемой литературы и используемых источников.

Оглавление

Введение.....	4
Глава 1 Теоретико-правовые основы деятельности Министерства цифрового развития, связи и массовых коммуникаций РФ	7
1.1 Понятие, сущность национальной безопасности и роль цифровизации в её обеспечении.....	7
1.2 Правовой статус и организационная структура Министерства цифрового развития, связи и массовых коммуникаций РФ	15
1.3 Полномочия и функции Министерства цифрового развития, связи и массовых коммуникаций РФ в сфере обеспечения национальной безопасности.....	21
Глава 2 Роль Министерства цифрового развития в обеспечении информационной безопасности государства	28
2.1 Государственная политика в сфере цифровой безопасности и роль Министерства в её реализации	28
2.2 Реализация национальных проектов Министерством в сфере цифровизации как инструмент обеспечения национальной безопасности	37
Глава 3 Проблемные аспекты и направления модернизации системы обеспечения информационной безопасности Министерством цифрового развития в составе национальной безопасности страны.....	47
3.1 Основные проблемы по обеспечению информационной безопасности, как составляющей национальной.....	47
3.2 Совершенствование нормативно-правового регулирования и организационных механизмов обеспечения информационной безопасности.....	57
Заключение	66
Список используемой литературы и используемых источников.....	70

Введение

Актуальность темы исследования обусловлена возрастающей ролью цифровых технологий в обеспечении национальной безопасности Российской Федерации и необходимостью эффективного государственного управления процессами цифровой трансформации общества. В условиях глобальной цифровизации и усиления информационного противоборства особую значимость приобретает деятельность Министерства цифрового развития, связи и массовых коммуникаций РФ как ключевого органа, ответственного за реализацию государственной политики в сфере цифрового развития и обеспечения информационной безопасности страны.

Современные вызовы и угрозы в информационной сфере, развитие технологий искусственного интеллекта, необходимость защиты критической информационной инфраструктуры и обеспечения технологического суверенитета России требуют комплексного исследования роли и места Министерства цифрового развития в системе органов, обеспечивающих национальную безопасность государства.

Необходимость теоретического осмысления данной проблематики также обусловлена тем, что в современной научной литературе отсутствует системное исследование полномочий и функций Министерства цифрового развития в контексте обеспечения национальной безопасности. Кроме того, анализ правоприменительной практики свидетельствует о наличии ряда проблем в сфере нормативно-правового регулирования и организационного обеспечения информационной безопасности, требующих научного осмысления и выработки практических рекомендаций по их решению.

Цель исследования заключается в комплексном теоретико-правовом анализе места и роли Министерства цифрового развития, связи и массовых коммуникаций РФ в системе органов, обеспечивающих национальную безопасность, а также выявлении проблем и определении направлений совершенствования его деятельности в данной сфере.

Для достижения поставленной цели определены следующие задачи:

- исследовать понятие и сущность национальной безопасности и роль цифровизации в её обеспечении;
- проанализировать правовой статус и организационную структуру Министерства цифрового развития;
- изучить полномочия и функции Министерства в сфере обеспечения национальной безопасности;
- рассмотреть государственную политику в сфере цифровой безопасности и роль Министерства в её реализации;
- исследовать реализацию национальных проектов в сфере цифровизации;
- выявить основные проблемы обеспечения информационной безопасности;
- разработать предложения по совершенствованию нормативно-правового регулирования и организационных механизмов обеспечения информационной безопасности.

Объектом исследования выступают общественные отношения, возникающие в процессе деятельности Министерства цифрового развития, связи и массовых коммуникаций РФ по обеспечению национальной безопасности.

Предметом исследования являются нормативные правовые акты, регулирующие деятельность Министерства цифрового развития в сфере обеспечения национальной безопасности, а также практика их применения.

Теоретическую основу исследования составляют труды российских ученых, исследовавших различные аспекты обеспечения национальной и информационной безопасности, в том числе работы В.А. Авдеева, О.А. Авдеевой, Т.А. Поляковой, А.В. Минбалеева, В.М. Редкоуса, Г.Г. Шинкарежкой и других.

Нормативно-правовую основу исследования составляют Конституция РФ, федеральные законы, указы Президента РФ, постановления Правительства РФ и иные нормативные правовые акты в сфере обеспечения национальной безопасности и регулирования деятельности Министерства цифрового развития.

Методологическую основу исследования составляют общенаучные методы познания (анализ, синтез, системный подход) и частно-научные методы (формально-юридический, сравнительно-правовой). Их применение позволило всесторонне исследовать роль Министерства в системе обеспечения национальной безопасности и сформулировать предложения по совершенствованию его деятельности.

Структура работы обусловлена целью и задачами исследования и включает введение, три главы, состоящие из семи параграфов, заключение и список используемой литературы и используемых источников.

Глава 1 Теоретико-правовые основы деятельности Министерства цифрового развития, связи и массовых коммуникаций РФ

1.1 Понятие, сущность национальной безопасности и роль цифровизации в её обеспечении

В условиях стремительной глобализации и цифровой трансформации современного мира проблематика национальной безопасности приобретает особую актуальность и новое содержательное наполнение. Усложнение международных отношений, появление новых вызовов и угроз, связанных с развитием информационно-коммуникационных технологий, требуют переосмысления традиционных подходов к обеспечению национальной безопасности. Особую значимость приобретает исследование диалектической взаимосвязи между процессами цифровизации и обеспечением национальной безопасности государства, что обуславливает необходимость комплексного анализа данной проблематики с учетом современных реалий.

Развитие цифровых технологий существенно трансформирует традиционные представления о национальной безопасности, создавая новую парадигму защиты государственных интересов в киберпространстве. Цифровизация затрагивает все ключевые сферы жизнедеятельности общества – от государственного управления до повседневной жизни граждан, что требует переосмысления подходов к обеспечению безопасности на всех уровнях.

В условиях формирования глобального информационного общества особую значимость приобретает способность государства обеспечивать цифровой суверенитет, защищать критическую информационную инфраструктуру и противодействовать новым формам угроз, возникающим в виртуальном пространстве. Современные вызовы национальной безопасности все чаще носят гибридный характер, сочетая в себе элементы традиционных и цифровых угроз.

Процессы цифровой трансформации создают не только новые риски, но и открывают беспрецедентные возможности для укрепления национальной безопасности. Внедрение передовых технологий в системы мониторинга, анализа и предупреждения угроз позволяет существенно повысить эффективность работы государственных институтов в сфере обеспечения безопасности. Искусственный интеллект, большие данные, технологии распределенного реестра становятся важнейшими инструментами в арсенале средств защиты национальных интересов.

Особое значение приобретает развитие национальной цифровой инфраструктуры и технологических компетенций как фундаментальных факторов обеспечения безопасности государства в современном мире. Способность страны разрабатывать и внедрять собственные цифровые решения, обеспечивать технологическую независимость в критически важных областях становится одним из ключевых показателей уровня национальной безопасности.

Согласно официальному определению, закрепленному в Стратегии национальной безопасности РФ, «национальная безопасность Российской Федерации представляет собой состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны» [20].

Сущность национальной безопасности неразрывно связана с понятием национальных интересов, которые определяются как «объективно значимые потребности личности, общества и государства в безопасности и устойчивом развитии» [20]. При этом важно отметить, что обеспечение национальной безопасности реализуется через систему мер, включающих в себя «реализацию органами публичной власти во взаимодействии с институтами

гражданского общества и организациями политических, правовых, военных, социально-экономических, информационных, организационных и иных мер, направленных на противодействие угрозам национальной безопасности» [20].

Особое значение в контексте национальной безопасности приобретает понимание угроз, которые определяются как «совокупность условий и факторов, создающих прямую или косвенную возможность причинения ущерба национальным интересам Российской Федерации» [20]. В современных условиях спектр таких угроз существенно расширился и включает не только традиционные военные угрозы, но и вызовы в информационной, экономической, экологической и других сферах.

Система обеспечения национальной безопасности представляет собой «совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов публичной власти и находящихся в их распоряжении инструментов» [20]. Важно подчеркнуть, что данная система функционирует на основе стратегического планирования, что позволяет обеспечить комплексный подход к защите национальных интересов.

В современных условиях национальная безопасность России базируется на принципах укрепления обороноспособности, внутреннего единства и политической стабильности. Как отмечается в Стратегии, «последовательно проводимый Российской Федерацией курс на укрепление обороноспособности, внутреннего единства и политической стабильности, на модернизацию экономики и развитие промышленного потенциала обеспечил укрепление суверенной государственности России как страны, способной проводить самостоятельную внешнюю и внутреннюю политику, эффективно противостоять попыткам внешнего давления» [20]. Таким образом, понятие национальной безопасности охватывает широкий спектр взаимосвязанных аспектов, направленных на защиту интересов личности, общества и государства.

В научном сообществе особое внимание уделяется исследованию сущности национальной безопасности. С точки зрения У.Ю. Акаева, понятие национальной безопасности является емким и многогранным, включающим различные виды безопасности, которые постоянно эволюционируют вместе с развитием государства.

Интересен подход У.Ю. Акаева к анализу теоретических основ национальной безопасности через призму исторического развития. Автор подчеркивает, что «проблема безопасности рассматривалась многими философами, политологами, историками, правоведами. Еще Платон, Аристотель и Геродот размышляли о задачах и функциях государства в сфере обеспечения безопасности» [2, с. 95].

Особенно ценным в работе У.Ю. Акаева является выделение двух ключевых источников опасности: внутреннего и внешнего. При этом автор дает четкое определение: «Внутренняя безопасность - это защищенность от угроз, исходящих от процессов, организаций лиц и объектов, которые находятся на территории страны. Внешняя безопасность - защищенность национальных интересов России от угроз, исходящих извне, со стороны других государств» [2, с. 95].

Принципиально важным в позиции У.Ю. Акаева является определение системы безопасности как комплексного механизма, включающего «органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации и объединения, граждан, принимающих участие в обеспечении безопасности в соответствии с законом» [2, с. 95].

Существенный вклад в понимание сущности национальной безопасности вносит предложенная У.Ю. Акаевым классификация основных функций системы безопасности, среди которых особое значение придается выявлению и прогнозированию угроз, созданию и поддержанию в готовности сил и средств обеспечения безопасности.

Заслуживает внимания позиция У.Ю. Акаева относительно правовых форм обеспечения национальной безопасности, которые автор определяет как

«всю деятельностьную составляющую, отражающую содержание механизма правового регулирования, которым располагает государство» [2, с. 95].

Критически оценивая концепцию У.Ю. Акаева, следует отметить, что автор создал фундаментальную теоретическую базу для понимания сущности национальной безопасности. Вместе с тем, в современных условиях требуется существенное расширение данной концепции. В частности, необходим более глубокий анализ угроз, связанных с цифровой трансформацией общества, проблемами кибербезопасности, транснациональной преступностью и международным терроризмом. Кроме того, представляется целесообразным уделить больше внимания вопросам обеспечения информационной безопасности и противодействия гибридным угрозам в условиях глобализации.

С точки зрения О.А. Колоткиной, вопросы обеспечения национальной безопасности приобретают особую актуальность в современных условиях развития общественных отношений, что обусловлено появлением новых опасностей, угроз и рисков. Автор подчеркивает уникальность феномена национальной безопасности как гаранта обеспечения национальных интересов государства, общества и личности.

Особую ценность в работе О.А. Колоткиной представляет анализ правового регулирования общественных отношений в сфере национальной безопасности через призму двух базовых целей. По мнению автора, «правовое регулирование имеет своей целью упорядочивание общественных отношений между субъектами в сфере национальной безопасности и создание условий, при которых субъекты права, достигнув оптимального уровня безопасности, смогут свободно реализовывать потребности более высокого порядка» [9, с. 8].

Принципиально важным является акцент О.А. Колоткиной на влиянии цифровизации на национальную безопасность. Автор справедливо отмечает, что «внедрение цифровых технологий, расширение доступа к информации, активное взаимодействие с иностранными государствами создает

определенные риски для обеспечения национальной безопасности государства» [9, с. 8].

Заслуживает внимания выделение О.А. Колоткиной конкретных угроз национальной безопасности в условиях цифровизации. В частности, автор указывает на опасность криптовалюты, проблемы доступа к информации и киберугрозы. При этом подчеркивается, что «проблема кибербезопасности является глобальной проблемой, которая касается всех государств, имеющих выходы в интернет-пространство» [9, с. 8].

Существенный вклад в понимание современных вызовов национальной безопасности вносит анализ О.А. Колоткиной трансформации субъектного состава правоотношений в цифровую эпоху. Автор обращает внимание на появление новых видов субъектов, имеющих цифровую форму, включая субъектов с искусственным интеллектом.

О.А. Колоткина справедливо отмечает, что «пока государство не обеспечит эффективную политику в сфере цифровых технологий, не закрепит законодательно базовые категории, связанные с цифровой деятельностью и видами национальной безопасности, данные инновации будут работать против государства» [9, с. 8].

По нашему мнению, концепция О.А. Колоткиной имеет существенное теоретическое и практическое значение для понимания трансформации национальной безопасности в условиях цифровизации. Однако представляется необходимым дополнить ее анализом механизмов международного сотрудничества в сфере кибербезопасности и разработкой конкретных правовых инструментов противодействия новым цифровым угрозам. Особенно актуальным видится развитие правовых механизмов защиты критической информационной инфраструктуры и персональных данных граждан.

С точки зрения Г.Г. Шинкаревой и А.М. Берман, в современных условиях цифровые технологии стали одним из ключевых факторов, определяющих уровень национальной безопасности государства. Авторы

подчеркивают, что цифровизация и национальная безопасность представляют собой взаимосвязанные и взаимозависимые явления.

Особую ценность в работе представляет анализ роли цифровизации как инструмента обеспечения национальной безопасности. Авторы отмечают, что «информационно-коммуникационные технологии определяют динамику развития мировой экономики и многие содержательные аспекты отношений между государствами» [21, с. 257].

Принципиально важным является вывод авторов о том, что «цифровые технологии являются 'двигателем' государственных инновационных процессов, ориентированных на формирование цифровой экономики и обеспечение национальной безопасности и суверенности государства» [21, с. 257].

Заслуживает внимания анализ авторами потенциальных угроз национальной безопасности, связанных с цифровизацией. В частности, Г.Г. Шинкарецкая и А.М. Берман выделяют проблемы криптовалюты, трансформации рынка труда и киберугроз как ключевые вызовы современности.

Значимым представляется вывод авторов о том, что «необходимость обеспечения кибербезопасности является глобальной проблемой, а не проблемой какого-либо отдельно взятого государства, т.к. сегодня с киберугрозами сталкивается каждое государство» [21, с. 257].

Авторы справедливо подчеркивают, что «до тех пор, пока государством не будет выстроена и обеспечена эффективная политика в сфере цифровых технологий, технологии не смогут в должной степени выполнять свои функции и служить национальным интересам» [21, с. 257].

Критически осмысливая концепцию Г.Г. Шинкарецкой и А.М. Берман, следует отметить ее фундаментальный характер и значительный вклад в понимание диалектической взаимосвязи процессов цифровизации и обеспечения национальной безопасности. Особую ценность представляет выделение авторами не только потенциальных угроз цифровой

трансформации, но и ее возможностей для укрепления национальной безопасности. Вместе с тем, исследование могло бы выиграть от более детального анализа конкретных правовых и организационных механизмов государственного регулирования процессов цифровизации. В частности, актуальным представляется исследование вопросов баланса между необходимостью государственного контроля в цифровой сфере и сохранением пространства для инновационного развития, а также разработка конкретных правовых инструментов защиты критической информационной инфраструктуры.

Проведенный анализ научных подходов к пониманию сущности национальной безопасности и роли цифровизации в ее обеспечении позволяет сделать вывод о многоаспектном характере данного феномена. Национальная безопасность представляет собой комплексное явление, включающее различные виды безопасности и требующее системного подхода к ее обеспечению. При этом цифровизация выступает одновременно как фактор укрепления национальной безопасности и как источник новых угроз и вызовов, что требует выработки сбалансированного подхода к регулированию цифровой трансформации общества.

В современных условиях особую актуальность приобретает необходимость совершенствования правового регулирования процессов цифровизации в контексте обеспечения национальной безопасности. Требуется разработка эффективных механизмов противодействия киберугрозам, защиты критической информационной инфраструктуры и персональных данных граждан. При этом важно соблюсти баланс между обеспечением национальной безопасности и созданием благоприятных условий для инновационного развития и цифровой трансформации экономики и общества. Решение этих задач возможно только при условии комплексного подхода, учитывающего как национальные интересы России, так и необходимость международного сотрудничества в сфере кибербезопасности.

1.2 Правовой статус и организационная структура Министерства цифрового развития, связи и массовых коммуникаций РФ

В современных условиях стремительной цифровизации всех сфер общественной жизни особую значимость приобретает эффективное государственное управление в области информационных технологий, связи и массовых коммуникаций. Ключевым органом, определяющим государственную политику в данной сфере, является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России). Понимание правового статуса и организационной структуры данного ведомства имеет принципиальное значение для осмысления механизмов государственного регулирования цифровой трансформации российского общества и экономики.

В соответствии с действующим законодательством, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, электросвязи и почтовой связи, массовых коммуникаций и средств массовой информации.

Правовой статус Минцифры России определяется Положением, утвержденным Постановлением Правительства РФ от 02.06.2008 № 418, согласно которому «Министерство является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, электросвязи и почтовой связи, массовых коммуникаций и средств массовой информации» [18].

Особое значение имеет то, что Министерство выступает в качестве почтовой администрации Российской Федерации и выполняет функции

администрации связи Российской Федерации при осуществлении международной деятельности в области связи. Кроме того, Минцифры России является уполномоченным федеральным органом исполнительной власти в сфере использования электронной подписи.

Существенным элементом правового статуса Министерства является осуществление координации и контроля деятельности находящейся в его ведении Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), а также подведомственных Министерству организаций.

Важно отметить, что в структуре Министерства предусмотрено наличие до 19 департаментов по основным направлениям деятельности. При этом «структурными подразделениями Министерства являются департаменты по основным направлениям деятельности Министерства. В состав департаментов включаются отделы» [18].

Принципиальным является то, что Министерство в установленной сфере деятельности не вправе осуществлять функции по контролю и надзору, а также функции по управлению государственным имуществом, кроме случаев, устанавливаемых указами Президента РФ и постановлениями Правительства РФ. Данные ограничения не распространяются на полномочия Министра по управлению имуществом, закрепленным за Министерством и подведомственными организациями.

В рамках международной деятельности Министерство осуществляет взаимодействие с органами государственной власти иностранных государств и международными организациями в установленной сфере деятельности, а также участвует в реализации государственной политики Российской Федерации в области международной информационной безопасности.

Финансовое обеспечение деятельности Министерства осуществляется за счет средств федерального бюджета. При этом Министерство является юридическим лицом, имеет печать с изображением Государственного герба Российской Федерации, иные печати, штампы и бланки установленного

образца, а также счета, открываемые в соответствии с законодательством Российской Федерации.

Следует подчеркнуть особую роль Министерства в реализации национальной программы «Цифровая экономика Российской Федерации», в рамках которой оно выступает ключевым координатором процессов цифровой трансформации государственного управления и экономики страны.

Важным аспектом правового статуса Министерства является его полномочие по разработке и реализации мер поддержки субъектов малого и среднего предпринимательства в сфере информационных технологий, включая разработку и выполнение соответствующих ведомственных целевых программ.

В системе органов исполнительной власти Министерство занимает особое положение как центр компетенций по вопросам развития информационного общества и формирования цифровой экономики, что подтверждается расширением его полномочий в сфере регулирования использования информационных технологий в государственном управлении и экономике.

Организационная структура Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации представляет собой сложную иерархическую систему, во главе которой находится Министр цифрового развития, связи и массовых коммуникаций – Шадаев Максут Игоревич [11].

Основной функциональный каркас Министерства составляют девятнадцать профильных департаментов, которые можно систематизировать по ключевым направлениям деятельности. В сфере цифрового развития и технологий функционируют Департамент развития цифровых компетенций и образования, Департамент развития отрасли информационных технологий, Департамент развития искусственного интеллекта и больших данных, Департамент развития облачных сервисов и Департамент развития технологий цифровой идентификации. Инфраструктурное направление представлено Департаментом реализации инфраструктурных проектов, Департаментом

развития инфраструктуры электронного правительства и Департаментом развития новых телекоммуникационных сервисов. В области коммуникаций и медиа действуют Департамент развития массовых коммуникаций и международного сотрудничества, Департамент государственной поддержки развития медиа и Департамент государственной поддержки периодической печати и книжной индустрии. Вопросами безопасности и регулирования занимаются Департамент обеспечения кибербезопасности и Департамент государственного регулирования рынка телекоммуникаций. Экономический блок включает Департамент экономики и финансов, Департамент цифровой трансформации и координации бюджетных расходов и Департамент стимулирования спроса на радиоэлектронную продукцию. Административно-правовое обеспечение осуществляют Правовой департамент и Административный департамент. Отдельно следует выделить Департамент развития сервисов и клиентского опыта, отвечающий за повышение качества предоставляемых услуг.

Значительную роль в структуре Министерства играют подведомственные органы, среди которых ключевое место занимает Роскомнадзор, осуществляющий контрольно-надзорные функции в сфере связи, информационных технологий и массовых коммуникаций.

Министерство осуществляет координацию деятельности двадцати пяти подведомственных организаций, которые можно разделить на три основные категории.

К первой категории относятся научно-исследовательские институты и организации общей направленности: ФГБУ «ЦЭКИ», ФГАУ НИИ «Восход», ФГБУ «Связист», ФГБУ НИИ «Интеграл», ФКУ «Государственные технологии», ФГУП «Почта Крыма», ФГУП РСВО, ФГУП ГЦСС, ФГБУ НИИР и ФГБУ ЦМС имени А.С. Попова.

Вторую категорию составляют ведущие отраслевые образовательные учреждения, осуществляющие подготовку специалистов в сфере телекоммуникаций и информационных технологий: ФГБОУ ВО МТУСИ,

ФГБОУ ВО СПбГУТ, ФГБОУ ВО ПГУТИ, ФГБОУ ВО СибГУТИ и ФГБОУ ДПО «Академия медиаиндустрии».

В третью категорию входят организации, обеспечивающие информационную и техническую поддержку отрасли, включая ведущие медиахолдинги и технические центры: ФГУП «ТТЦ «Останкино», ФГУП РТРС, ФГУП ВГТРК, ФГБУ «РГМЦ», ФГУП МИА «Россия сегодня», ФГБУ «Редакция «Российской газеты», ФГУП «Космическая связь», ФГУП «Ново-Петровский завод «Оргтехсвязь», ФГУП Издательство «Транспорт» и ФГБУ «Центр МИР ИТ» [11].

Для более глубокого понимания организационно-правовых аспектов функционирования Минцифры России целесообразно обратиться к научным исследованиям в данной области.

С точки зрения Е.Я. Велиховой, организационно-правовая структура органов в сфере связи в Российской Федерации имеет иерархический характер, где центральное место занимает Министерство связи и массовых коммуникаций РФ, обладающее всей полнотой нормотворческих полномочий в данной сфере.

Анализируя компетенцию Минкомсвязи России, Е.Я. Велихова отмечает его ключевую роль в выработке и реализации государственной политики в сфере телекоммуникаций. По мнению автора, «Министерство связи и массовых коммуникаций Российской Федерации является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативному правовому регулированию в сфере информационных технологий» [5, с. 50].

Особое внимание в работе уделяется подведомственным Минкомсвязи органам. В частности, Роскомнадзор осуществляет контрольно-надзорные функции, а Россвязь отвечает за управление государственным имуществом и оказание государственных услуг в сфере связи. При этом автор подчеркивает необходимость четкого разграничения полномочий между данными структурами.

Заслуживает внимания позиция Е.Я. Велиховой относительно правового статуса Государственной комиссии по радиочастотам (ГКРЧ). Автор указывает, что «ГКРЧ обладает административной правосубъектностью, является носителем властных полномочий по реализации технических задач регулирования использования радиочастотного спектра» [5, с. 50].

Примечательно, что Е.Я. Велихова предлагает конкретные меры по совершенствованию системы регулирования в сфере связи. В частности, она считает целесообразным наделить Роскомнадзор дополнительными полномочиями по мониторингу правоприменительной практики и выработке предложений по совершенствованию законодательства.

Значимым представляется вывод автора о том, что «структура органов в сфере связи в Российской Федерации построена следующим образом: во главе находится Министерство связи и массовых коммуникаций, которое обладает всей полнотой нормотворчества в сфере связи» [5, с. 50].

Исходя из проведенного автором анализа, представляется обоснованным ее предложение о необходимости создания специальной рабочей группы в структуре Роскомнадзора для проведения регулярного мониторинга правоприменительной практики в сфере связи.

Проанализировав научную позицию Е.Я. Велиховой, следует отметить комплексный подход автора к исследованию организационно-правовой структуры органов в сфере связи. Предложенные меры по совершенствованию компетенции Роскомнадзора представляются обоснованными, поскольку направлены на повышение эффективности правового регулирования в телекоммуникационной сфере. Вместе с тем полагаем, что помимо расширения полномочий контрольно-надзорных органов требуется также совершенствование механизмов их взаимодействия с иными органами государственной власти в целях обеспечения комплексного подхода к регулированию телекоммуникационной отрасли.

Таким образом, анализ правового статуса и организационной структуры Министерства цифрового развития, связи и массовых коммуникаций РФ

позволяет сделать вывод о комплексном характере данного органа исполнительной власти, играющего ключевую роль в процессах цифровой трансформации государственного управления и экономики страны. Обладая широкими полномочиями в сфере выработки государственной политики и нормативно-правового регулирования, Министерство эффективно координирует деятельность подведомственных структур и организаций, обеспечивая системный подход к развитию информационно-коммуникационной инфраструктуры России.

Сложная иерархическая структура Министерства, включающая профильные департаменты по основным направлениям деятельности и разветвленную сеть подведомственных организаций, позволяет решать масштабные задачи цифровизации различных отраслей экономики и социальной сферы. При этом четкое разграничение полномочий между структурными подразделениями и подведомственными органами, а также эффективные механизмы их взаимодействия способствуют достижению стратегических целей государственной политики в области цифрового развития, связи и массовых коммуникаций.

1.3 Полномочия и функции Министерства цифрового развития, связи и массовых коммуникаций РФ в сфере обеспечения национальной безопасности

В эпоху интенсивного технологического развития и масштабной цифровой трансформации общества вопросы обеспечения национальной безопасности в информационном пространстве становятся критически важными для сохранения суверенитета и защиты национальных интересов государства. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации выступает ключевым регулятором в сфере информационной безопасности, реализуя комплексный подход к противодействию современным киберугрозам и обеспечению устойчивости

критической информационной инфраструктуры страны. В условиях возрастающих рисков информационного противоборства и технологической зависимости особую значимость приобретает анализ полномочий и функций Министерства в контексте обеспечения национальной безопасности России.

В системе обеспечения национальной безопасности Российской Федерации Министерство цифрового развития, связи и массовых коммуникаций (Минцифры России) играет существенную роль как федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, электросвязи и информационной безопасности [18].

Одним из ключевых направлений деятельности Министерства в сфере обеспечения национальной безопасности является защита информационного пространства России. Министерство устанавливает «требования к информационной безопасности информационных систем, в том числе информационных систем персональных данных, информационно-телекоммуникационных сетей и других сетей связи» [18].

В области защиты критической информационной инфраструктуры Минцифры России разрабатывает и внедряет «требования к функционированию систем управления сетями связи при возникновении угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети «Интернет» и сети связи общего пользования» [18].

Особое внимание уделяется обеспечению безопасности при трансграничном информационном обмене. Министерство устанавливает «требования к линиям связи, пересекающим государственную границу Российской Федерации, и к средствам связи, к которым подключаются указанные линии связи» [18].

В сфере биометрической идентификации Минцифры России осуществляет регулирование и контроль за обработкой биометрических

персональных данных, согласовывая с ФСБ России порядок их обработки, включая сбор и хранение, а также требования к параметрам биометрических персональных данных [18].

Существенным направлением деятельности Министерства является обеспечение технологического суверенитета страны через развитие отечественного программного обеспечения и стимулирование импортозамещения в сфере информационных технологий. Минцифры России реализует комплекс мер по поддержке российских IT-компаний, создающих критически важное программное обеспечение и разрабатывающих инновационные решения в области информационной безопасности.

Министерство активно участвует в реализации государственной политики Российской Федерации в области международной информационной безопасности, что является важным аспектом обеспечения национальной безопасности в условиях глобальной цифровизации [18].

В рамках реализации национальной программы «Цифровая экономика» Министерство координирует работу по созданию устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств. Особое внимание уделяется внедрению современных технологий защиты информации и обеспечению безопасности критической информационной инфраструктуры.

В части обеспечения устойчивости функционирования критической информационной инфраструктуры Минцифры России устанавливает требования для операторов связи по обеспечению устойчивого функционирования средств связи, взаимодействующих со средствами связи других операторов, в том числе находящихся за пределами территории Российской Федерации [18].

Министерство осуществляет взаимодействие с федеральным органом исполнительной власти в области обороны по вопросам совместной

эксплуатации и восстановления единой сети электросвязи в интересах обеспечения обороны и безопасности Российской Федерации [18].

В чрезвычайных ситуациях Минцифры России организует выполнение мероприятий по управлению и восстановлению единой сети электросвязи Российской Федерации, проводит тренировки с операторами связи и органами исполнительной власти субъектов РФ для определения готовности сетей связи к угрозе возникновения чрезвычайной ситуации [18].

Важным аспектом деятельности Минцифры России является развитие системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Министерство активно взаимодействует с Национальным координационным центром по компьютерным инцидентам, обеспечивая своевременное реагирование на угрозы информационной безопасности и координацию действий по их нейтрализации.

В рамках обеспечения безопасности критической информационной инфраструктуры Министерство по согласованию с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, устанавливает требования к сетям и средствам связи для проведения мероприятий в целях реализации возложенных на них задач [18].

Министерство играет ключевую роль в обеспечении кибербезопасности государственных информационных систем, устанавливая по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, требования о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет» [18].

В условиях развития цифровых технологий и появления новых форм киберугроз Минцифры России постоянно совершенствует нормативно-правовую базу и механизмы защиты информационной инфраструктуры. Министерство регулярно актуализирует требования к обеспечению

безопасности и устойчивости функционирования сетей связи, учитывая современные тенденции развития информационных технологий и новые виды угроз.

В сфере обеспечения безопасности точек обмена трафиком Минцифры России по согласованию с Федеральной службой безопасности Российской Федерации устанавливает требования к обеспечению их функционирования, включающие требования к обеспечению устойчивого функционирования технических и программных средств связи, сооружений связи [18].

Особое внимание Министерство уделяет вопросам организационно-технического обеспечения устойчивого функционирования сети связи общего пользования, устанавливая соответствующий порядок и требования к защите сетей связи и информационных систем операторов связи от несанкционированного доступа к ним и передаваемой по ним информации [18].

В области обеспечения безопасности при использовании электронной подписи Министерство выступает в качестве головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров и устанавливает по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности перечень угроз безопасности, актуальных при идентификации заявителя [18].

Важным аспектом деятельности Министерства является обеспечение защиты сведений, составляющих государственную тайну, в процессе своей деятельности, а также контроль и координация деятельности подведомственной федеральной службы и организаций в указанной области массовых коммуникаций РФ, закрепленных в Постановлении Правительства РФ от 02.06.2008 № 418, демонстрирует системный подход государства к решению задач обеспечения национальной безопасности в цифровой среде. Широкий спектр полномочий Министерства охватывает все ключевые аспекты информационной безопасности: от защиты персональных данных

граждан до обеспечения устойчивости функционирования критической информационной инфраструктуры страны.

По нашему мнению, существующая система полномочий Минцифры России создает необходимую правовую основу для эффективного противодействия современным вызовам и угрозам в информационной сфере. Особенно важным представляется наличие механизмов межведомственного взаимодействия и координации усилий с другими органами государственной власти в области обеспечения безопасности. Вместе с тем, динамичный характер развития информационных технологий и появление новых форм киберугроз требуют постоянного совершенствования нормативно-правовой базы и расширения инструментария противодействия современным вызовам национальной безопасности.

На основе проведенного в первой главе исследования можно заключить, что в современных условиях стремительной цифровой трансформации общества национальная безопасность приобретает новое содержательное наполнение, где цифровизация выступает одновременно как фактор укрепления безопасности и как источник новых угроз. Комплексный анализ научных подходов к пониманию сущности национальной безопасности демонстрирует необходимость системного подхода к её обеспечению, учитывающего многоаспектный характер современных вызовов в информационной сфере.

Министерство цифрового развития, связи и массовых коммуникаций РФ занимает ключевое место в системе обеспечения национальной безопасности России, обладая широкими полномочиями в сфере выработки государственной политики и нормативно-правового регулирования цифровой трансформации. Сложная иерархическая структура Министерства, включающая профильные департаменты и разветвленную сеть подведомственных организаций, позволяет эффективно координировать процессы цифровизации различных отраслей экономики и социальной сферы,

обеспечивая при этом защиту национальных интересов в информационном пространстве.

Анализ полномочий и функций Минцифры России в сфере обеспечения национальной безопасности свидетельствует о комплексном подходе к решению задач защиты информационного пространства страны, включая обеспечение устойчивости критической информационной инфраструктуры, защиту персональных данных граждан и противодействие киберугрозам. При этом динамичный характер развития информационных технологий и появление новых форм угроз требуют постоянного совершенствования нормативно-правовой базы и механизмов межведомственного взаимодействия для эффективного обеспечения национальной безопасности в цифровую эпоху.

Глава 2 Роль Министерства цифрового развития в обеспечении информационной безопасности государства

2.1 Государственная политика в сфере цифровой безопасности и роль Министерства в её реализации

Геополитическая напряженность и технологическое противостояние между странами выводят вопросы цифрового суверенитета и информационной безопасности на принципиально новый уровень значимости. Необходимость защиты национальных интересов России в цифровом пространстве требует выстраивания комплексной системы противодействия киберугрозам и развития отечественных технологических решений. Ключевая роль в реализации этих стратегических задач принадлежит Министерству цифрового развития, связи и массовых коммуникаций РФ, которое формирует и проводит государственную политику, направленную на обеспечение технологической независимости страны, защиту критической информационной инфраструктуры и создание условий для безопасного развития цифровой экономики.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, было определено как «федеральный орган исполнительной власти, ответственный за реализацию национальной программы «Цифровая экономика Российской Федерации» [17]. В рамках данной программы министерство осуществляет функции по реализации федеральных проектов «Информационная безопасность», «Цифровые технологии» и «Цифровое государственное управление» [17].

Важным аспектом деятельности министерства является координация работы с различными участниками системы цифровой безопасности. Министерство взаимодействует с автономной некоммерческой организацией «Цифровая экономика», которая «осуществляет мониторинг развития цифровой экономики и цифровых технологий, формирует прогнозы их

развития и готовит предложения по основным направлениям развития» цифровой безопасности [17].

Особое внимание уделяется формированию эффективной системы управления реализацией программы цифровой безопасности. Министерство обеспечивает информационное взаимодействие всех участников системы, осуществляет мониторинг реализации федеральных проектов и координирует работу проектного офиса по реализации программы [17].

В целях обеспечения прозрачности и эффективности реализации политики цифровой безопасности министерство организует подготовку ежемесячных отчетов о ходе реализации федеральных проектов. Эти отчеты содержат «достоверную информацию о достижении общественно значимых результатов, показателей и контрольных точек» [17].

Существенным элементом работы министерства является взаимодействие с региональными органами власти в сфере цифровой безопасности. Министерство координирует реализацию «региональных проектов, обеспечивающих достижение показателей и результатов федеральных проектов программы» [17].

В рамках своих полномочий министерство осуществляет подготовку изменений в нормативные правовые акты, направленные на совершенствование системы цифровой безопасности. При этом все изменения проходят обязательное согласование с заинтересованными органами и организациями [17].

Важной функцией министерства является обеспечение межведомственной координации в сфере цифровой безопасности. Министерство организует работу с федеральными органами исполнительной власти, участвующими в реализации программы, обеспечивает согласование их действий и решение возникающих разногласий [17].

Отдельное внимание уделяется вопросам финансового обеспечения мероприятий по цифровой безопасности. Министерство участвует в «планировании бюджетных ассигнований на реализацию программы» и

осуществляет контроль за эффективным использованием выделенных средств [17].

В целях повышения эффективности реализации политики цифровой безопасности министерство обеспечивает создание и функционирование «информационной системы проектной деятельности», которая используется для мониторинга реализации программы и федеральных проектов [17].

Министерство также отвечает за формирование системы оценки эффективности реализации политики цифровой безопасности. Эта система включает в себя «регулярный мониторинг достижения показателей, анализ результатов реализации программы и подготовку предложений по ее совершенствованию» [17].

С точки зрения Е.А. Поповой и З.С. Мартемьяновой, современная государственная политика в области цифровой безопасности неразрывно связана с общей стратегией цифровой трансформации общества. Авторы подчеркивают, что количественные изменения в сфере цифровизации привели к качественным переменам, заметным всем участникам социально-экономических процессов.

Особое внимание исследователи уделяют вопросам нормативно-правового регулирования цифровой безопасности. Ключевым документом они считают Доктрину информационной безопасности, утвержденную Указом Президента РФ в 2016 году. По их мнению, «данная Доктрина сформирована для обеспечения национальной безопасности государства в эпоху информационных изменений» [16, с. 165].

В работе отмечается системный подход государства к обеспечению цифровой безопасности через создание специализированных институтов развития. Авторы указывают на важную роль Агентства стратегических инициатив и Фонда развития интернет-инициатив в реализации государственной политики цифровизации.

Значимым аспектом исследования является анализ международного опыта в сфере цифровой безопасности. Е.А. Попова и З.С. Мартемьянова

приводят примеры успешных практик Китая, Израиля и Белоруссии, подчеркивая необходимость адаптации зарубежного опыта к российским реалиям.

Авторы акцентируют внимание на существующих угрозах: «важно обратить внимание на возможные угрозы в виде информационной безопасности, технологической зависимости, ограничение правового института, отсутствие механизма регулирования изменений» [16, с. 165].

В контексте развития цифровой безопасности исследователи подчеркивают необходимость формирования цифрового сознания и создания условий для его развития. По их мнению, это является одной из ключевых задач государственной политики в данной сфере.

Особую ценность представляет выявленная авторами взаимосвязь между эффективностью государственной политики в сфере цифровой безопасности и качеством нормативно-правовой базы. Они подчеркивают необходимость своевременного реагирования регулятора на технологические изменения.

Критически осмысливая исследование авторов, следует отметить его значительный вклад в понимание современных процессов цифровой трансформации государственного управления. Позиция Е.А. Поповой и З.С. Мартемьяновой относительно необходимости создания комплексной системы обеспечения цифровой безопасности представляется обоснованной и своевременной. Особенно важным видится акцент авторов на взаимосвязи технологических и образовательных компонентов в обеспечении цифровой безопасности государства. При этом открытым остается вопрос о конкретных механизмах интеграции предложенных авторами решений в существующую систему государственного управления, что может стать предметом дальнейших исследований.

В условиях возрастающих геополитических вызовов особую актуальность приобретают вопросы практической реализации мер по обеспечению информационной безопасности государственных структур и

финансового сектора, что требует детального рассмотрения существующих рисков и механизмов их минимизации.

С точки зрения А.В. Баркова и А.С. Киселева, текущая санкционная политика в отношении России создает беспрецедентные риски для информационной безопасности государственных структур и банковского сектора. Авторы подчеркивают критическую важность совершенствования защиты информационных систем в условиях возросших киберугроз.

Исследователи указывают на системные проблемы в существующей инфраструктуре. В частности, они отмечают, что «в настоящее время в единой сети электросвязи Российской Федерации отсутствует телекоммуникационная инфраструктура, отвечающая требованиям по устойчивости и информационной безопасности» [4, с. 26].

А.В. Барков и А.С. Киселев акцентируют внимание на необходимости перехода на отечественное программное обеспечение и оборудование. По их оценке, использование зарубежных решений создает критические уязвимости в системе национальной безопасности, позволяя иностранным структурам получать доступ к конфиденциальной информации.

Важным аспектом исследования является анализ роли биометрических технологий в обеспечении безопасности. Авторы рассматривают успешный опыт внедрения систем распознавания лиц в различных сферах, отмечая необходимость создания единой государственной биометрической базы данных.

Особое внимание уделяется банковскому сектору как одному из наиболее технологически развитых. «Роль банковской системы в современной рыночной экономике сложно преуменьшить, а все изменения, происходящие в ней, затрагивают всю экономику» [4, с. 26].

Отдельного внимания заслуживает вопрос кадрового обеспечения информационной безопасности банковского сектора. По мнению авторов, существует острая необходимость в создании специализированных образовательных программ, учитывающих специфику работы с

биометрическими данными и современными системами защиты информации. Важно обеспечить постоянное повышение квалификации специалистов в соответствии с развитием технологий и появлением новых угроз.

Исследователи также отмечают необходимость создания единой системы сертификации специалистов по информационной безопасности в банковской сфере. Такая система позволит стандартизировать требования к компетенциям сотрудников и обеспечить высокий уровень защиты информации во всем банковском секторе. При этом важно учитывать международные стандарты и лучшие практики в данной области.

Исследователи предлагают конкретные изменения в законодательство, направленные на расширение возможностей использования биометрических данных в целях обеспечения безопасности. В частности, они рекомендуют дополнить ФЗ «Об информации» положениями о праве государственных органов на сбор и обработку биометрических данных.

А.В. Барков и А.С. Киселев подчеркивают необходимость баланса между обеспечением безопасности и защитой прав граждан. Они признают существование рисков нарушения приватности, но считают их оправданными в контексте национальной безопасности.

Стоит отметить глубину и системность подхода авторов к проблеме информационной безопасности государственных структур и банковского сектора. Предложенная концепция создания единой биометрической базы данных заслуживает внимания, однако требует серьезной доработки в части обеспечения конституционных прав граждан. Важно учитывать не только технические аспекты внедрения подобных систем, но и социально-правовые последствия их использования. Представляется целесообразным разработать многоуровневую систему контроля за обработкой биометрических данных с участием как государственных органов, так и институтов гражданского общества.

Проанализировав конкретные механизмы обеспечения информационной безопасности, целесообразно рассмотреть более широкий

контекст влияния цифровизации на национальную безопасность и конкурентоспособность страны в глобальном масштабе.

С точки зрения Е.В. Логиновой, цифровизация российской экономики и общества является ключевым фактором обеспечения национальной безопасности через повышение глобальной конкурентоспособности страны. Автор подчеркивает, что «цифровизация станет источником долгосрочного экономического роста, повысит качество жизни населения, обеспечит конкурентоспособность страны и национальную безопасность» [10, с. 23].

Исследователь акцентирует внимание на том, что отставание России в темпах и масштабах цифровизации от передовых стран несет существенные риски для национальной безопасности. В частности, «ее роль в мировой экономике будет догоняющей, обеспечение национальной безопасности в России будет под вопросом, она будет лишена перспектив инновационного развития» [10, с. 23].

Особое внимание Е.В. Логинова уделяет роли государственной политики в развитии цифровой экономики. Автор отмечает важность принятия национальной программы «Цифровая экономика Российской Федерации», которая направлена на решение ключевых проблем цифровой безопасности.

По мнению Е.В. Логиновой, приоритетными направлениями государственной политики должны стать: либерализация рынка программного обеспечения, стимулирование межсистемной конкуренции, создание открытой экосистемы инноваций и развитие систем непрерывного образования.

Автор подчеркивает необходимость повышения эффективности платформ электронного правительства и расширения спектра электронных государственных услуг. При этом Е.В. Логинова отмечает, что «Россия демонстрирует достаточно высокие результаты, занимая 32 место из 193 возможных» [10, с. 23] в рейтинге развития электронного правительства.

Важным аспектом в работе является анализ цифровых экстерналий. Е.В. Логинова выделяет как положительные эффекты (повышение эффективности, социальная интеграция, развитие конкуренции), так и отрицательные (усугубление цифрового неравенства, рост естественных монополий).

Существенным аспектом государственной политики в сфере цифровой безопасности, по мнению Е.В. Логиновой, является развитие механизмов государственно-частного партнерства. Автор подчеркивает, что эффективное взаимодействие государства и бизнеса позволяет не только привлечь дополнительные ресурсы для развития цифровой инфраструктуры, но и обеспечить более гибкое реагирование на возникающие угрозы. Особую роль в этом процессе играют технологические компании, обладающие передовыми разработками в области информационной безопасности.

Особенностью позиции автора является акцент на необходимости систематического мониторинга изменений, происходящих под влиянием цифровых технологий, для своевременной корректировки мер государственной политики в сфере обеспечения национальной безопасности.

По нашему мнению, позиция Е.В. Логиновой относительно роли государственной политики в обеспечении цифровой безопасности представляется обоснованной и актуальной. Особенно важным видится предложенный автором комплексный подход к оценке цифровых параметров развития общества и их влияния на национальную безопасность. При этом следует отметить, что предложенные механизмы государственного регулирования могли бы быть дополнены более конкретными инструментами реализации обозначенных приоритетов.

Анализ государственной политики в сфере цифровой безопасности и роли Министерства цифрового развития в её реализации позволяет сделать вывод о системном подходе российского государства к решению данного комплекса задач. Создана необходимая нормативно-правовая база, определены ключевые институты развития, выстроена эффективная система межведомственного взаимодействия. Особое внимание уделяется вопросам

технологического суверенитета, развитию отечественного программного обеспечения и защите критической информационной инфраструктуры. При этом государственная политика учитывает необходимость баланса между обеспечением безопасности и защитой прав граждан, что отражается в комплексном подходе к регулированию использования современных цифровых технологий.

Особое значение в современных условиях приобретает задача обеспечения безопасности критической информационной инфраструктуры на региональном уровне.

Необходимо создание эффективной системы мониторинга и реагирования на инциденты, учитывающей специфику различных отраслей и территорий. При этом важно обеспечить баланс между централизованным управлением и автономностью региональных систем безопасности, что позволит повысить устойчивость всей национальной системы цифровой безопасности

Вместе с тем, динамичный характер цифровой трансформации и появление новых вызовов требуют постоянного совершенствования механизмов обеспечения цифровой безопасности.

Приоритетными направлениями дальнейшего развития государственной политики в данной сфере должны стать: укрепление технологического суверенитета страны, развитие отечественных программных решений, совершенствование системы подготовки специалистов в области информационной безопасности, а также расширение международного сотрудничества в борьбе с киберугрозами. Особое значение приобретает необходимость постоянного мониторинга эффективности принимаемых мер и их своевременной корректировки с учетом меняющейся ситуации в глобальном цифровом пространстве.

2.2 Реализация национальных проектов Министерством в сфере цифровизации как инструмент обеспечения национальной безопасности

В контексте обеспечения национальной безопасности Российской Федерации особую значимость приобретает реализация комплекса национальных проектов в сфере цифровизации, которые претерпели существенную трансформацию и реструктуризацию в период 2024-2025 годов. Правительством Российской Федерации был утвержден масштабный Единый план по достижению национальных целей развития до 2030 года с перспективой до 2036 года, что свидетельствует о стратегическом характере цифровой трансформации государства.

В парадигме современной теории государственного управления цифровая трансформация рассматривается как многоаспектный процесс, детерминирующий качественные изменения в социально-экономической системе государства. Имплементация цифровых технологий в систему государственного управления становится не просто технологическим императивом, но и фундаментальным условием обеспечения национального суверенитета в условиях глобальной цифровой конкуренции.

Фундаментальным элементом цифровой трансформации выступает государственная программа «Информационное общество», реализация которой осуществляется в два этапа: первый охватил период 2011-2021 годов, а второй рассчитан на 2022-2030 годы. Данная программа служит базисом для множества федеральных проектов, в том числе проекта «Информационная доступность для инвалидов и маломобильных групп населения», реализуемого в период 2022-2025 годов под руководством Министерства цифрового развития, связи и массовых коммуникаций [14].

Особого внимания заслуживает тот факт, что с 2025 года начинается реализация нового национального проекта «Экономика данных и цифровая трансформация государства», который приходит на смену национальной

программе «Цифровая экономика Российской Федерации», действовавшей с 1 октября 2018 года по 31 декабря 2024 года. Данная трансформация отражает эволюцию подходов к цифровизации государственного управления и экономики.

В рамках нового национального проекта предусмотрена реализация целого ряда федеральных проектов, рассчитанных на период 2025-2030 годов. Ключевым среди них является федеральный проект «Инфраструктура доступа к информационно-телекоммуникационной сети Интернет», направленный на обеспечение повсеместного доступа к цифровым сервисам [14].

Значительное внимание уделяется развитию социальной сферы через федеральный проект «Цифровые платформы в отраслях социальной сферы», который предусматривает комплексную цифровизацию социальных услуг и сервисов в период 2025-2030 годов. Параллельно реализуется федеральный проект «Искусственный интеллект», перешедший из предыдущей программы в обновленном формате [14].

Методологическая база реализации национальных проектов в сфере цифровизации базируется на системном подходе, интегрирующем технологические, организационные и социальные аспекты цифровой трансформации. Данный подход позволяет обеспечить синергетический эффект от взаимодействия различных компонентов цифровой экосистемы государства.

Особую роль в обеспечении национальной безопасности играет федеральный проект «Цифровое государственное управление», получивший продолжение в новом национальном проекте. Его реализация направлена на создание целостной системы цифрового государственного управления, что является критически важным для обеспечения суверенитета в цифровую эпоху.

Стратегическое значение имеет федеральный проект «Отечественные решения», рассчитанный на 2025-2030 годы, который направлен на обеспечение технологической независимости страны через развитие

собственных цифровых решений и платформ. Этот проект тесно связан с федеральным проектом «Прикладные исследования и перспективные разработки», также реализуемым в период 2025-2030 годов [14].

В условиях возрастающих киберугроз особую актуальность приобретает федеральный проект «Инфраструктура кибербезопасности», запланированный на 2025-2030 годы. Данный проект является логическим продолжением федерального проекта «Информационная безопасность», действовавшего до конца 2024 года [14].

Кадровое обеспечение цифровой трансформации реализуется через федеральный проект «Кадры для цифровой трансформации», пришедший на смену проекту «Кадры для цифровой экономики». Параллельно продолжается реализация федерального проекта «Развитие кадрового потенциала ИТ-отрасли», рассчитанного на период 2022-2030 годов [14].

Следует отметить, что до 31 декабря 2024 года действовал особый порядок публикации сведений о реализации ряда стратегически важных государственных программ, включая программы «Космическая деятельность России», «Развитие атомного энергопромышленного комплекса» и «Развитие электронной и радиоэлектронной промышленности» [14].

В контексте институциональной теории цифровая трансформация государственного управления может рассматриваться как процесс формирования новых институциональных механизмов, обеспечивающих эффективное функционирование государства в цифровую эпоху. Этот процесс характеризуется высокой степенью сложности и взаимозависимости различных элементов системы государственного управления.

Важным элементом цифровой трансформации выступает федеральный проект «Государственная статистика», реализуемый в период 2025-2030 годов, который направлен на создание современной системы статистического учета и анализа данных. Этот проект имеет критическое значение для принятия обоснованных управленческих решений на всех уровнях государственной власти [14].

До конца 2024 года действовал федеральный проект «Цифровые технологии», который заложил основу для дальнейшего развития отечественных цифровых решений и технологий. Его задачи были частично интегрированы в новые федеральные проекты, начавшие свою реализацию с 2025 года [14].

Особого внимания заслуживает федеральный проект «Обеспечение доступа в Интернет за счет развития спутниковой связи», реализация которого осуществлялась в период 2022-2024 годов. Данный проект заложил основу для дальнейшего развития спутниковых технологий связи и обеспечения доступности интернета на всей территории страны [14].

Методическое обеспечение реализации государственных программ осуществляется на основе рекомендаций, утвержденных Приказом Минэкономразвития России от 23 декабря 2024 года № 813, что обеспечивает единый подход к мониторингу и оценке эффективности проводимых мероприятий [14].

Федеральный проект «Развитие цифровых и информационных проектов на территории субъектов Российской Федерации», рассчитанный на период 2022-2030 годов, обеспечивает координацию цифровой трансформации на региональном уровне, что особенно важно для обеспечения единого цифрового пространства страны.

Парадигмальный сдвиг в понимании роли цифровых технологий в обеспечении национальной безопасности отражается в трансформации концептуальных подходов к реализации национальных проектов. Происходит переход от технократической модели цифровизации к комплексной модели цифровой трансформации, учитывающей социальные, экономические и геополитические аспекты.

Значимым аспектом является передача курирования федерального проекта «Искусственный интеллект» от Минэкономразвития России к Минцифры России с 1 сентября 2024 года, что свидетельствует о

консолидации управления процессами цифровой трансформации в рамках единого ведомства.

В рамках обеспечения национальной безопасности особую роль играет преемственность реализуемых проектов и программ. Так, федеральный проект «Цифровое государственное управление» получил продолжение в обновленном формате в составе национального проекта «Экономика данных и цифровая трансформация государства» [14].

Комплексный характер цифровой трансформации подтверждается наличием взаимосвязанных проектов в различных сферах, от развития инфраструктуры до подготовки кадров, что обеспечивает системный подход к решению задач цифровизации и укрепления национальной безопасности [14].

Важно отметить, что реализация национальных проектов в сфере цифровизации осуществляется в соответствии с Распоряжением Правительства РФ от 06.10.2021 № 2816-р, утвердившим перечень инициатив социально-экономического развития Российской Федерации до 2030 года, что обеспечивает согласованность различных направлений государственной политики.

Анализ структуры и содержания национальных проектов в сфере цифровизации позволяет сделать вывод о комплексном подходе к обеспечению цифрового суверенитета и национальной безопасности России через развитие собственных технологий, подготовку кадров и создание современной цифровой инфраструктуры.

Теоретико-методологический анализ реализации национальных проектов в сфере цифровизации позволяет выявить существенную трансформацию подходов к обеспечению национальной безопасности в цифровую эпоху. Формируется новая парадигма цифрового суверенитета, основанная на принципах технологической независимости и информационной самодостаточности.

В контексте анализа трансформации национальных проектов следует отметить, что переход от национальной программы «Цифровая экономика

Российской Федерации» к национальному проекту «Экономика данных и цифровая трансформация государства» отражает качественное изменение подходов к цифровизации государственного управления [14].

Существенным аспектом обеспечения национальной безопасности является интеграция различных направлений цифровой трансформации в единую систему. Так, проект «Информационная инфраструктура», действовавший до конца 2024 года, органично трансформировался в более широкий проект «Цифровые платформы в отраслях социальной сферы», что демонстрирует расширение масштабов цифровизации [14].

Особое внимание в рамках обеспечения национальной безопасности уделяется мониторингу эффективности реализуемых проектов. Методические рекомендации, утвержденные Минэкономразвития России, обеспечивают единообразный подход к оценке результативности государственных программ и федеральных проектов в сфере цифровизации.

Важным элементом обеспечения национальной безопасности является развитие региональной составляющей цифровой трансформации. Федеральный проект «Развитие цифровых и информационных проектов на территории субъектов Российской Федерации» создает необходимую основу для равномерного развития цифровой инфраструктуры на всей территории страны.

Следует подчеркнуть значимость преемственности в реализации проектов цифровой трансформации. Так, опыт реализации федерального проекта «Кадры для цифровой экономики» был учтен при разработке проекта «Кадры для цифровой трансформации», что обеспечивает непрерывность процесса подготовки специалистов для цифровой экономики [14].

С позиций системного анализа, архитектура национальных проектов в сфере цифровизации представляет собой сложную адаптивную систему, характеризующуюся высокой степенью взаимозависимости компонентов и способностью к самоорганизации в условиях динамично меняющейся внешней среды.

В рамках обеспечения технологического суверенитета особую роль играет федеральный проект «Прикладные исследования и перспективные разработки», который создает научно-технологический задел для развития отечественных цифровых решений. Данный проект тесно связан с проектом «Отечественные решения», формируя комплексный подход к технологической независимости [14].

Значительное внимание уделяется вопросам информационной безопасности, что отражено в трансформации соответствующего федерального проекта в более масштабный проект «Инфраструктура кибербезопасности». Это свидетельствует о возрастающей роли защиты информационного пространства в системе национальной безопасности.

Комплексный характер цифровой трансформации подтверждается включением в новый национальный проект федерального проекта «Государственная статистика», что обеспечивает формирование единой системы сбора и анализа данных для принятия управленческих решений на всех уровнях государственной власти [14].

Важным аспектом обеспечения национальной безопасности является развитие спутниковых технологий связи, что нашло отражение в федеральном проекте «Обеспечение доступа в Интернет за счет развития спутниковой связи». Данное направление имеет стратегическое значение для обеспечения связности территории страны.

Особого внимания заслуживает консолидация управления процессами цифровой трансформации в рамках Министерства цифрового развития, связи и массовых коммуникаций, что способствует повышению эффективности реализации национальных проектов и обеспечению национальной безопасности в цифровой сфере.

В контексте современной теории национальной безопасности цифровая трансформация государственного управления приобретает характер стратегического императива, определяющего способность государства эффективно реагировать на современные вызовы и угрозы. Формирование

целостной системы цифрового государственного управления становится ключевым фактором обеспечения национального суверенитета в условиях глобальной цифровизации.

Методологическая рефлексия процессов цифровой трансформации позволяет констатировать формирование новой парадигмы государственного управления, базирующейся на принципах цифрового суверенитета, технологической независимости и информационной безопасности. Данная парадигма находит свое практическое воплощение в системе национальных проектов и программ цифровизации.

Интегративный характер реализуемых национальных проектов в сфере цифровизации отражает комплексный подход к решению задач обеспечения национальной безопасности, учитывающий многоаспектность современных вызовов и необходимость формирования адекватных механизмов реагирования на них.

Резюмируя вышеизложенное, следует подчеркнуть, что реализация национальных проектов в сфере цифровизации представляет собой сложный многоаспектный процесс, детерминирующий качественные изменения в системе обеспечения национальной безопасности Российской Федерации. Комплексный характер реализуемых проектов, их взаимосвязанность и направленность на достижение стратегических целей развития государства позволяют говорить о формировании новой парадигмы цифрового государственного управления, ориентированной на обеспечение технологического суверенитета и национальной безопасности в условиях глобальных цифровых трансформаций.

Представим выводы по второй главе исследования. Анализ роли Министерства цифрового развития в обеспечении информационной безопасности государства позволяет сделать вывод о формировании комплексной системы управления цифровой трансформацией страны. Министерство выступает ключевым координатором реализации государственной политики в сфере цифровой безопасности, обеспечивая

эффективное взаимодействие между федеральными органами исполнительной власти, региональными структурами и институтами развития. Особое внимание уделяется мониторингу реализации федеральных проектов и своевременной корректировке принимаемых мер с учетом динамично меняющейся ситуации в глобальном цифровом пространстве.

Принципиальное значение в деятельности Министерства приобретает реализация масштабного комплекса национальных проектов в сфере цифровизации, претерпевших существенную трансформацию в период 2024-2025 годов. Переход от национальной программы «Цифровая экономика Российской Федерации» к национальному проекту «Экономика данных и цифровая трансформация государства» отражает качественное изменение подходов к цифровизации государственного управления. Новая архитектура проектов обеспечивает системное развитие цифровой инфраструктуры, отечественных технологических решений и кадрового потенциала отрасли, что создает прочную основу для укрепления национальной безопасности в цифровую эпоху.

Стратегическим направлением работы Министерства является обеспечение технологического суверенитета страны через развитие собственных цифровых решений и платформ. Особое внимание уделяется проектам в сфере искусственного интеллекта, информационной безопасности и развития спутниковых технологий связи. Важным аспектом деятельности выступает создание эффективной системы защиты критической информационной инфраструктуры при одновременном соблюдении баланса между обеспечением безопасности и защитой прав граждан, что находит отражение в комплексном подходе к регулированию использования современных цифровых технологий.

В условиях возрастающих геополитических вызовов и технологического противостояния между странами Министерство цифрового развития демонстрирует способность к оперативной адаптации механизмов реализации национальных проектов. Формируется новая парадигма цифрового

суверенитета, основанная на принципах технологической независимости и информационной самодостаточности. Особую значимость приобретает развитие межведомственного взаимодействия и координация усилий различных участников системы цифровой безопасности, включая научные организации, бизнес-структуры и институты гражданского общества.

В целом, анализ деятельности Министерства цифрового развития свидетельствует о системном подходе к решению задач обеспечения национальной безопасности в цифровую эпоху. Реализуемые национальные проекты создают необходимую технологическую и организационную базу для противодействия современным киберугрозам и укрепления позиций России в глобальном цифровом пространстве. При этом особое внимание уделяется развитию человеческого капитала и созданию условий для инновационного развития отечественной цифровой индустрии, что имеет стратегическое значение для обеспечения долгосрочной конкурентоспособности страны.

Глава 3 Проблемные аспекты и направления модернизации системы обеспечения информационной безопасности Министерством цифрового развития в составе национальной безопасности страны

3.1 Основные проблемы по обеспечению информационной безопасности, как составляющей национальной

Комплексный анализ вызовов информационной безопасности как неотъемлемого компонента национальной безопасности государства приобретает особую значимость в контексте системной трансформации социально-экономических отношений под влиянием цифровых технологий. Формирование единого информационного пространства, рост взаимозависимости критической инфраструктуры от цифровых систем управления, а также появление новых форм информационного противоборства требуют научного переосмысления существующих подходов к обеспечению безопасности государства в цифровую эпоху. В этой связи актуализируется необходимость детального исследования ключевых проблем в сфере информационной безопасности, выявления системных уязвимостей и определения перспективных направлений совершенствования механизмов защиты национальных интересов в условиях цифровой трансформации общества.

С точки зрения Е.А. Калужина, взаимосвязь информационной и национальной безопасности России в современных условиях требует пристального внимания. По мнению исследователя, особую ценность в эпоху стремительного технологического развития представляет информация, при этом ее разнообразие варьируется от персональных данных до государственной тайны.

Рассматривая ключевые проблемы, Е.А. Калужин указывает на доминирование зарубежных разработчиков на отечественном рынке средств

информатизации и защиты информации. Как подчеркивает автор: «их продукция не проходит должного контроля и вполне вероятно имеет не декларированные возможности, использование которых может нанести значительный материальный ущерб организациям» [8, с. 90].

В своих рассуждениях Е.А. Калужин акцентирует внимание на киберпреступности на внутреннем рынке. По его наблюдениям, наибольшую опасность представляют атаки на банковский сектор, причем целью злоумышленников чаще становятся не сами финансовые учреждения, а их клиенты.

В размышлениях Е.А. Калужина значительное место занимает человеческий фактор. Исследователь отмечает: «зачастую угрозы реализуются непреднамеренно в результате некомпетентных действий со стороны персонала» [8, с. 90], что может привести к значительным убыткам организации.

Особое внимание Е.А. Калужин уделяет проблеме защиты персональных данных граждан. По его мнению: «работодатели и организации, предоставляющие услуги, зачастую пренебрегают мерами защиты, что влечет несанкционированное использование полученной информации» [8, с. 90].

В качестве решения выявленных проблем Е.А. Калужин предлагает комплексный подход, включающий стимулирование отечественных производителей средств защиты информации и модернизацию программно-аппаратных комплексов.

С точки зрения исследователя, важнейшим направлением является повышение компетентности персонала в области информационной безопасности и установление строгих внутренних правил с соответствующими мерами ответственности.

Е.А. Калужин настаивает на необходимости создания эффективной системы защиты персональных данных, предлагая два пути решения: формирование собственной службы безопасности или привлечение специализированных организаций.

По нашему мнению, позиция Е.А. Калужина относительно комплексного подхода к обеспечению информационной безопасности представляется весьма обоснованной. Особенно важным видится акцент автора на необходимости развития отечественного производства средств защиты информации, что в современных геополитических условиях приобретает стратегическое значение. Однако считаем необходимым дополнить предложенные меры усилением международного сотрудничества в сфере кибербезопасности при сохранении информационного суверенитета страны.

Расширяя проблематику информационной безопасности от технологических аспектов к более широкому социально-правовому контексту, интересную перспективу анализа предлагают З.И. Алиева и З.М. Хасбулатова. С точки зрения З.И. Алиевой и З.М. Хасбулатовой, в современном обществе информационная безопасность занимает ведущее положение в структуре национальной безопасности России, что обусловлено повсеместным внедрением информационных технологий во все сферы жизни. Авторы подчеркивают особую динамику состояния информационной безопасности в период 2020-2022 годов, когда массовый переход на удаленный формат работы сделал этот вопрос приоритетным в повестке национальной безопасности.

По мнению З.И. Алиевой и З.М. Хасбулатовой, одной из ключевых проблем является международный терроризм, использующий современные технологии для подрыва государственных систем безопасности. «Речь идет не только о коммуникации между членами террористических группировок, но и об их деятельности в рамках информационного поля и сети «Интернет», направленной на подрыв государственных систем безопасности» [3, с. 44].

Исследователи акцентируют внимание на проблеме защиты персональных данных пользователей в социальных сетях. «Прежде всего, нарушается право на неприкосновенность частной жизни, личные и семейные тайны, защиту чести и доброго имени, когда пользователь размещает свои

фотографии в сети, а мошенник использует эти фотографии в своих целях» [3, с. 44].

З.И. Алиева и З.М. Хасбулатова подчеркивают значимость факторов, влияющих на формирование бюджета информационной безопасности. Авторы отмечают, что приоритетными направлениями являются защита персональных данных, критической информационной структуры и государственных информационных систем.

С точки зрения исследователей, особую актуальность приобретает проблема обеспечения государственного суверенитета в информационном пространстве. «Основной задачей правового регулирования данного вида общественных отношений является не ограничение доступа к всемирной сети «Интернет», а создание необходимых условий для обеспечения национальной безопасности государства» [3, с. 44].

З.И. Алиева и З.М. Хасбулатова указывают на необходимость совершенствования нормативно-правовой базы в сфере информационной безопасности. По их мнению, темпы развития общественных отношений в сфере информационных технологий значительно превышают реакцию законодателя на эти изменения.

Авторы подчеркивают уязвимость российского общества в связи с его переходным состоянием и глубоким разрывом в уровне социально-экономического развития регионов. «Обществу ещё только предстоит выработать порядок и нормы безопасного информационного взаимодействия, безопасного, как для индивида, так и для общества в целом» [3, с. 44].

По нашему мнению, позиция З.И. Алиевой и З.М. Хасбулатовой относительно комплексного подхода к обеспечению информационной безопасности представляется весьма обоснованной и актуальной. Особенно важным видится акцент авторов на необходимости баланса между обеспечением государственного суверенитета в информационном пространстве и защитой конституционных прав граждан. Вместе с тем, считаем целесообразным дополнить предложенные меры разработкой

механизмов международного сотрудничества в сфере противодействия киберугрозам, учитывая их трансграничный характер.

Углубляя понимание системных вызовов цифровой эпохи и их влияния на трансформацию правовой системы, существенный вклад в исследование проблематики информационной безопасности вносят работы Т.А. Поляковой и соавторов. С точки зрения Т.А. Поляковой и соавторов, вопросы цифрового развития государства и общества, их влияние на трансформацию системы права носят глобальный характер, затрагивая как международно-правовое обеспечение, так и изменения в национальном законодательстве.

По мнению Т.А. Поляковой, А.В. Минбалева и И.С. Бойченко, особую актуальность приобретает проблема правовой оценки цифровизации и цифровых процессов в контексте формирования государственной политики. Авторы подчеркивают: «глобальная цифровая трансформация создает широкий спектр вызовов и угроз, рисков для национальных экономик государств, их хозяйствующих субъектов и граждан» [15, с. 35].

Исследователи акцентируют внимание на том, что технология блокчейн, несмотря на свою надежность, также несет определенные риски информационной безопасности. Среди них авторы выделяют: «потеря ключей доступа может привести к неблагоприятным последствиям и угрозе потери информации, выявлены возможности злоупотребления правами администраторов, угроза получения доступа третьих лиц» [15, с. 35].

Т.А. Полякова, А.В. Минбалева и И.С. Бойченко указывают на необходимость унификации терминологии в сфере цифровизации, отмечая использование термина «цифровое» более чем в 600 федеральных законах и около 2000 актах Правительства Российской Федерации.

Авторы обращают особое внимание на проблему защиты персональных данных при их трансграничной передаче, особенно в контексте вступления в силу в США закона CLOUD Act. Как отмечается в исследовании: «права организаций-поставщиков облачных сервисов на защиту прав на

конфиденциальность данных пользователей могут быть серьезно ограничены международными соглашениями» [15, с. 35].

С точки зрения исследователей, существенную угрозу представляет цифровое неравенство населения и неготовность к предоставлению гражданам услуг с использованием ИКТ на всей территории государства.

Т.А. Полякова, А.В. Минбалеев и И.С. Бойченко подчеркивают важность международного сотрудничества в сфере информационной безопасности, отмечая: «отсутствие согласованной политики по обеспечению информационной безопасности государств в цифровой сфере является важным препятствием для достижения синергетических эффектов» [15, с. 35].

Изучение научных взглядов Т.А. Поляковой, А.В. Минбалеева и И.С. Бойченко на проблематику информационной безопасности в цифровую эпоху позволяет выделить несколько значимых аспектов. Исследователи справедливо указывают на необходимость комплексного подхода к противодействию современным киберугрозам, учитывающего как технологическую специфику цифровой среды, так и международно-правовой контекст. Предложенные авторами механизмы международного сотрудничества и унификации терминологии представляются перспективными инструментами обеспечения информационной безопасности. Однако требуется дальнейшая проработка практических аспектов реализации межгосударственного взаимодействия в данной сфере, включая создание эффективных платформ обмена информацией о киберугрозах и координации совместных действий по их нейтрализации.

Переходя от глобальных аспектов цифровизации к специфике национального регулирования информационной безопасности, важно обратиться к исследованию А.К. Дубеня. С точки зрения А.К. Дубеня, в современных условиях информационно-коммуникационных технологий проблема информационной безопасности приобретает особую актуальность в обеспечении национальной безопасности государства. Автор подчеркивает, что законодатель оперативно реагирует на возникающие в этой сфере вызовы,

уделяя информационной безопасности особое внимание в системе национальной безопасности.

Как отмечает А.К. Дубень, принятые документы стратегического планирования свидетельствуют об укреплении суверенитета государства в информационном поле. При этом автор акцентирует внимание на том, что «информационная безопасность является сложным правовым явлением с точки зрения информационного права, поскольку затрагивает все сферы общественной жизни и обеспечивает развитие государства в целом» [6, с. 56].

По мнению исследователя, особое значение имеют национальные интересы в сфере информационной безопасности, которые представляют собой общие ориентиры для органов публичной власти. А.К. Дубень подчеркивает, что «состояние информационной безопасности зависит не только от деятельности законодателя или правоприменителя, но и от правомерного и ответственного поведения граждан и организаций» [6, с. 56].

Важным аспектом, на который обращает внимание А.К. Дубень, является расширение полномочий государства в регулировании общественных отношений в информационной сфере. Автор отмечает, что это связано с социально-экономическими предпосылками и необходимостью технологической и юридической защиты цифровых данных.

Исследователь подчеркивает значимость совершенствования правового регулирования информационной безопасности, которое «должно иметь системный, комплексный характер, устраняя неоднозначность ключевых понятий и их дефиниций» [6, с. 56].

С точки зрения А.К. Дубеня, существенным фактором развития национальной политики государства выступает информационная составляющая. Автор акцентирует внимание на том, что «роль информационной безопасности и ее место в системе национальной безопасности определяется государственной информационной политикой» [6, с. 56].

А.К. Дубень приходит к выводу, что информационная политика Российской Федерации является регулятором публичных и частных правоотношений, через которые реализуются стратегические задачи государства. При этом автор подчеркивает необходимость совершенствования как публично-правовых, так и частноправовых норм.

По нашему мнению, исследование А.К. Дубеня существенно обогащает теоретическое понимание проблем информационной безопасности в контексте национальной безопасности государства. Автор предлагает убедительную аргументацию необходимости системного подхода к совершенствованию правового регулирования, при этом его позиция о взаимозависимости государственной деятельности и гражданской ответственности представляется особенно актуальной в современных условиях. Глубокое понимание информационной безопасности как комплексного правового феномена позволило исследователю выявить ключевые направления развития государственной политики в данной сфере. При этом работа могла бы получить дополнительное развитие за счет более предметного рассмотрения конкретных правовых механизмов, способных обеспечить баланс между публичными и частными интересами в информационной сфере. Также было бы полезным дополнить теоретические выводы анализом практических шагов по внедрению предложенных автором концепций в действующую систему правового регулирования информационной безопасности.

С точки зрения С.С. Морозовой и Ю.Г. Смирновой, в постковидный период цифровизация достигла беспрецедентного влияния на все сферы жизни государства и общества, что создает новые вызовы для обеспечения информационной безопасности как составляющей национальной безопасности.

По мнению исследователей, особую актуальность приобретает проблема правового регулирования в условиях цифровой трансформации, поскольку темпы развития цифровой среды значительно преобладают над готовностью

правовой системы адаптироваться к новой реальности. Как отмечают авторы: «цифровизация задает новые тренды: вместо отчетности все чаще используются аналитические и прогнозные разработки» [13, с. 129].

С.С. Морозова и Ю.Г. Смирнова акцентируют внимание на пересечении и наложении правовых норм разной отраслевой принадлежности, что создает существенные проблемы в контексте отношений права и научно-технического развития. Особенно остро стоит вопрос отсутствия системной модернизации правовых норм в условиях цифровизации.

Принципиально важным, по мнению исследователей, является рассмотрение права на безопасность в цифровую эпоху в двух парадигмах: «безопасности цифры» и «безопасности от цифры» [13, с. 129]. Авторы подчеркивают необходимость гармоничного совмещения обеспечения традиционных прав и свобод человека с процессами цифровизации.

Значимым достижением российской практики обеспечения информационной безопасности, по мнению авторов, является высокое место России в рейтинге Global Cybersecurity Index 2020 года (5-е место из 193 стран). При этом исследователи отмечают, что именно правовой аспект получил наивысшую оценку.

С.С. Морозова и Ю.Г. Смирнова выделяют ключевые особенности правового регулирования цифрового управления и безопасности в РФ, среди которых особое внимание уделяется проблеме «расплывчатости виртуальных границ цифрового пространства, усложняющей процесс законотворческой деятельности» [13, с. 129].

Авторы подчеркивают необходимость усиления контроля со стороны органов государственной власти над реализацией политики в сфере обеспечения кибербезопасности и законодательного закрепления распределения полномочий между соответствующими государственными структурами.

По нашему мнению, предложенный С.С. Морозовой и Ю.Г. Смирновой анализ проблем обеспечения информационной безопасности отличается

глубиной и системностью подхода. Особенно ценным представляется выделение авторами дуальности парадигм безопасности в цифровую эпоху. Вместе с тем, можно отметить, что исследователями недостаточно раскрыты практические механизмы преодоления выявленных противоречий между темпами цифровизации и возможностями правового регулирования, что открывает перспективы для дальнейших исследований в данной области.

Проведенный анализ научных исследований позволяет выделить несколько ключевых проблемных узлов в сфере обеспечения информационной безопасности как составляющей национальной безопасности. Во-первых, это технологическая зависимость от зарубежных решений в области информационной безопасности, создающая критические уязвимости для национальной безопасности. Во-вторых, существенное отставание нормативно-правовой базы от темпов развития цифровых технологий и появления новых форм киберугроз. В-третьих, проблема обеспечения баланса между необходимостью государственного контроля в цифровой сфере и защитой конституционных прав граждан.

Особую озабоченность вызывает рост киберпреступности, особенно в финансовом секторе, а также усиление угроз международного кибертерроризма. При этом ситуация осложняется человеческим фактором - недостаточным уровнем цифровой грамотности населения и специалистов, а также несовершенством механизмов защиты персональных данных. Требуется решения проблема цифрового неравенства регионов и отсутствия единой политики в сфере информационной безопасности на международном уровне.

Решение выявленных проблем требует комплексного подхода, включающего развитие отечественных технологий защиты информации, совершенствование нормативно-правовой базы с учетом современных вызовов, повышение цифровой грамотности населения и формирование культуры информационной безопасности. Принципиальное значение имеет укрепление международного сотрудничества в сфере противодействия киберугрозам при сохранении информационного суверенитета страны. Только

системный подход к решению этих задач позволит обеспечить необходимый уровень защищенности национальных интересов России в цифровую эпоху.

3.2 Совершенствование нормативно-правового регулирования и организационных механизмов обеспечения информационной безопасности

В современных условиях геополитической турбулентности и стремительного развития информационных технологий вопросы совершенствования нормативно-правового регулирования и организационных механизмов обеспечения информационной безопасности приобретают первостепенное значение для национальной безопасности России. Комплексный анализ научных исследований в данной области позволяет выявить ключевые направления и проблемные аспекты развития системы информационной безопасности как на национальном, так и на международном уровне.

С точки зрения В.М. Редкоуса, современное развитие государственного управления в Российской Федерации во многом обусловлено проведением специальной военной операции, что актуализировало вопросы обеспечения национальной безопасности и противодействия угрозам безопасности страны. Автор подчеркивает, что «речь идет уже не просто об угрозах безопасности России, а о фундаментальных угрозах, которые из года в год шаг за шагом грубо и бесцеремонно создаются безответственными политиками на Западе в отношении нашей страны» [19, с. 145].

В.М. Редкоус акцентирует внимание на том, что совершенствование правового регулирования в области информационной безопасности требует установления четкого правового положения уполномоченных должностных лиц и структурных подразделений, ответственных за обеспечение информационной безопасности в органах и организациях.

Существенным вкладом в развитие правового регулирования, по мнению В.М. Редкоуса, стало принятие Постановления Правительства РФ от 15 июля 2022 г. № 1272, утвердившего типовые положения о заместителе руководителя и структурном подразделении, ответственных за информационную безопасность.

Особое внимание автор уделяет анализу полномочий ответственного лица, подчеркивая, что «его указания и поручения в части обеспечения информационной безопасности являются обязательными для исполнения всеми государственными служащими, муниципальными служащими и работниками органа (организации)» [19, с. 145].

В.М. Редкоус детально рассматривает основные направления деятельности структурного подразделения, отмечая важность «исключения или существенного снижения негативных последствий (ущерба) в отношении органа (организации) вследствие нарушения функционирования информационных систем» [19, с. 145].

Значимым аспектом в работе В.М. Редкоуса является анализ взаимодействия подразделения с различными структурами, включая ФСБ России, Федеральную службу по техническому и экспортному контролю и Министерство цифрового развития, связи и массовых коммуникаций РФ.

Автор поднимает методологическую проблему соотношения прав и обязанностей подразделения, отмечая, что «фактически функции подразделения выступают как его обязанности» [19, с. 145], хотя это не вполне корректно с точки зрения юридической техники.

В.М. Редкоус подчеркивает необходимость расширения сравнительно-правовых исследований для выявления новых правовых средств, способствующих обеспечению информационной безопасности России.

По нашему мнению, позиция В.М. Редкоуса представляется обоснованной и своевременной, особенно в части необходимости четкого определения правового статуса должностных лиц и подразделений, ответственных за информационную безопасность. Вместе с тем, считаем

целесообразным дополнить предложенный автором подход разработкой механизмов оценки эффективности деятельности указанных структур и должностных лиц.

Если В.М. Редкоус концентрирует внимание на внутригосударственных аспектах обеспечения информационной безопасности, то А.К. Дубень расширяет исследовательский фокус, рассматривая данную проблематику через призму военно-технического сотрудничества и международных отношений.

С точки зрения А.К. Дубеня, в современных условиях геополитической нестабильности и мирового кризиса процессы цифровизации и развития информационных технологий продолжают активно влиять на все сферы жизнедеятельности человека. Автор подчеркивает, что «увеличение количества центров мирового экономического и политического развития, укрепление позиций новых глобальных и региональных стран-лидеров приводят к изменению структуры мирового порядка» [7, с. 43].

По мнению А.К. Дубеня, особую актуальность приобретает правовое обеспечение информационной безопасности в сфере военно-технического сотрудничества, которое становится одной из движущих констант при сохранении суверенитета и обеспечения национальной безопасности России. Автор отмечает, что «информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, военной и других составляющих безопасности РФ» [7, с. 43].

Значимым аспектом исследования А.К. Дубеня является анализ правового режима информации в военно-технической области. Автор указывает на необходимость более детального установления перечня информации, являющейся объектом внешнеторговых сделок с иностранными государствами.

А.К. Дубень подчеркивает важность совершенствования законодательства в контексте принятия Указа Президента РФ от 1 мая 2022 г. № 250, согласно которому «с 1 января 2025 г. органам и организациям

запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие недружественные действия» [7, с. 43].

Существенное внимание А.К. Дубень уделяет вопросам укрепления интеграционного взаимодействия России с другими странами в сфере военно-технического сотрудничества по обеспечению информационной безопасности. Автор считает это направление стратегически важным для укрепления как международной информационной безопасности, так и национальной безопасности России.

А.К. Дубень обращает особое внимание на необходимость формирования предпосылок к заключению соглашений о взаимной защите секретной информации в сфере военно-технического сотрудничества с более подробным описанием перечня такой информации и механизма разрешения споров.

В качестве важного направления совершенствования правового регулирования А.К. Дубень выделяет необходимость «формирования благоприятной информационной среды, исключая риски использования информации ограниченного доступа в военно-технической области против интересов России» [7, с. 43].

По нашему мнению, позиция А.К. Дубеня представляется актуальной и обоснованной, особенно в части необходимости совершенствования правового регулирования военно-технического сотрудничества в сфере информационной безопасности. Однако считаем целесообразным дополнить предложенный автором подход разработкой конкретных механизмов мониторинга эффективности принимаемых мер по обеспечению информационной безопасности в рамках военно-технического сотрудничества.

Развивая тему международного взаимодействия в сфере информационной безопасности, В.А. Авдеев и О.А. Авдеева смещают акцент на проблематику противодействия киберпреступности как одной из ключевых

угроз современности. С точки зрения В.А. Авдеева и О.А. Авдеевой, в современных условиях глобализации и развития технико-информационных ресурсов особую актуальность приобретает проблема оптимизации средств обеспечения информационной безопасности. Авторы подчеркивают, что «последовательной модификации заслуживают нормы национального законодательства, учитывающие особенности политико-правового и социально-экономического характера развития отечественной государственности» [1, с. 3].

В.А. Авдеев и О.А. Авдеева обращают внимание на стремительный рост преступлений в сфере информационной безопасности. По их наблюдениям, «показатели преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, характеризуются устойчивым ростом» [1, с. 3], что подтверждается статистическими данными увеличения доли таких преступлений с 4,4% в 2017 году до 24,96% в 2020 году.

Особое значение авторы придают международному сотрудничеству в сфере противодействия киберпреступности. Они отмечают важность российской инициативы 2016 года по разработке проекта Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности, подчеркивая его универсальный характер.

В.А. Авдеев и О.А. Авдеева акцентируют внимание на том, что «разрешение проблемы по преодолению угрозы кибербезопасности в условиях современных глобализационных процессов предопределило повышенный интерес к созданию механизма, предусматривающего недопустимость использования информационно-коммуникационных технологий как средства воздействия» [1, с. 3].

Существенным вкладом авторов является выделение новых угроз кибербезопасности, включающих неправомерный доступ в электронной форме к информации, воздействие на информацию и ее перехват, создание и распространение вредоносных программ, а также незаконный оборот устройств.

В.А. Авдеев и О.А. Авдеева подчеркивают необходимость формирования правового механизма, направленного на повышение качества и устойчивости элементов государственного управления в отношении финансовой системы, а также укрепление государственно-частного партнерства.

Значимым аспектом исследования является вывод авторов о том, что «повышение эффективности мер по обеспечению международной кибербезопасности детерминирует установление единообразного подхода к квалификации совершаемых в области высоких технологий противоправных деяний» [1, с. 3].

По нашему мнению, позиция В.А. Авдеева и О.А. Авдеевой представляется глубоко обоснованной и актуальной, особенно в части необходимости комплексного подхода к обеспечению информационной безопасности на национальном и международном уровнях. Вместе с тем считаем целесообразным дополнить предложенные авторами меры разработкой механизмов оперативного реагирования на новые виды киберугроз, учитывая стремительное развитие информационных технологий.

От анализа конкретных угроз информационной безопасности логично перейти к рассмотрению системных вопросов совершенствования организационного механизма национальной системы обеспечения информационной безопасности, которым посвящено исследование Н.А. Молчанова и Е.К. Матевосовой.

По мнению Н.А. Молчанова и Е.К. Матевосовой, качество государственных преобразований в современном мире напрямую зависит от состояния информационной безопасности как на национальном, так и на международном уровне. Авторы подчеркивают, что формирование новых угроз и рисков в условиях глобализации определяет приоритетные направления государственной политики в информационной сфере.

С точки зрения Н.А. Молчанова и Е.К. Матевосовой, особую актуальность приобретает проблема защиты информационных систем органов

государственной власти и социально значимых организаций. Как отмечают исследователи, «информационные системы органов государственной власти, а также организаций, деятельность которых имеет социально-экономическую значимость превращаются сегодня в театр военных действий с применением информационного оружия массового поражения» [12, с. 164].

Авторы обращают особое внимание на необходимость совершенствования организационного механизма национальной системы обеспечения информационной безопасности. При этом подчеркивается важность комплексного подхода к нормативному регулированию с учетом различных сценариев развития информационного общества.

Принципиальная позиция Н.А. Молчанова и Е.К. Матевосовой заключается в том, что «мероприятия по обеспечению безопасности информационной инфраструктуры зачастую не имеют комплексной основы» [12, с. 164]. Исследователи указывают на необходимость научной обоснованности реализуемой государственной политики в данной области.

Важным аспектом в работе авторов является анализ международного сотрудничества в сфере информационной безопасности. Н.А. Молчанов и Е.К. Матевосова подчеркивают, что «единый международный правовой режим обеспечения информационной безопасности еще находится в стадии своего формирования» [12, с. 164].

Исследователи акцентируют внимание на необходимости создания структурно единой и функционально взаимосвязанной системы обеспечения информационной безопасности на всех уровнях государственного управления. При этом особо подчеркивается роль права в предотвращении глобального информационного хаоса.

Авторы указывают на важность совершенствования нормативной правовой базы в области обеспечения информационной безопасности с учетом рекомендаций Совета Безопасности Российской Федерации. По их мнению, «выработка единственно верных вневременных подходов - это бесполезная и невыполнимая задача» [12, с. 164].

По нашему мнению, позиция авторов относительно необходимости постоянного совершенствования механизмов обеспечения информационной безопасности представляется обоснованной и актуальной. Особенно важным является их акцент на комплексном подходе к решению данной проблемы и необходимости научного обоснования принимаемых решений. Соглашаясь с исследователями, считаем необходимым подчеркнуть, что в современных условиях требуется более активная работа по формированию международно-правовых механизмов обеспечения информационной безопасности.

Проведенный анализ научных исследований позволяет констатировать, что совершенствование нормативно-правового регулирования и организационных механизмов обеспечения информационной безопасности требует комплексного подхода, учитывающего как внутригосударственные аспекты (включая четкое определение правового статуса уполномоченных должностных лиц и структурных подразделений), так и международное измерение (в частности, развитие военно-технического сотрудничества и противодействие киберпреступности). Особую значимость приобретает необходимость оперативного реагирования на новые виды информационных угроз при одновременном укреплении системы государственного управления в данной сфере.

В условиях возрастающей геополитической напряженности и технологической конкуренции принципиальное значение имеет дальнейшее совершенствование правового регулирования информационной безопасности с учетом как национальных интересов России, так и необходимости развития международного сотрудничества в данной сфере. При этом важно обеспечить научную обоснованность принимаемых решений, эффективность механизмов их реализации и возможность оперативной адаптации нормативной базы к новым вызовам и угрозам информационной безопасности.

Представим выводы по третьей главе исследования. На основе проведенного анализа можно заключить, что современное состояние системы обеспечения информационной безопасности как составляющей национальной

безопасности характеризуется рядом существенных проблем, требующих комплексного решения. К ним относятся технологическая зависимость от зарубежных решений в области информационной безопасности, отставание нормативно-правовой базы от темпов развития цифровых технологий, сложности в обеспечении баланса между государственным контролем в цифровой сфере и защитой конституционных прав граждан, а также рост киберпреступности и усиление угроз международного кибертерроризма. Ситуация осложняется недостаточным уровнем цифровой грамотности населения, несовершенством механизмов защиты персональных данных и проблемой цифрового неравенства регионов.

Совершенствование системы обеспечения информационной безопасности требует комплексного подхода, включающего как развитие отечественных технологий защиты информации и модернизацию нормативно-правовой базы, так и укрепление международного сотрудничества в сфере противодействия киберугрозам при сохранении информационного суверенитета страны. Особую значимость приобретает необходимость четкого определения правового статуса уполномоченных должностных лиц и структурных подразделений, ответственных за информационную безопасность, развития военно-технического сотрудничества и формирования эффективных механизмов противодействия новым видам информационных угроз. При этом принципиальное значение имеет обеспечение научной обоснованности принимаемых решений и возможности оперативной адаптации нормативной базы к новым вызовам цифровой эпохи.

Заключение

На основе проведенного исследования можно заключить, что в современных условиях стремительной цифровой трансформации общества национальная безопасность приобретает новое содержательное наполнение, где цифровизация выступает одновременно как фактор укрепления безопасности и как источник новых угроз. Комплексный анализ научных подходов к пониманию сущности национальной безопасности демонстрирует необходимость системного подхода к её обеспечению, учитывающего многоаспектный характер современных вызовов в информационной сфере.

Министерство цифрового развития, связи и массовых коммуникаций РФ занимает ключевое место в системе обеспечения национальной безопасности России, обладая широкими полномочиями в сфере выработки государственной политики и нормативно-правового регулирования цифровой трансформации. Сложная иерархическая структура Министерства, включающая профильные департаменты и разветвленную сеть подведомственных организаций, позволяет эффективно координировать процессы цифровизации различных отраслей экономики и социальной сферы, обеспечивая при этом защиту национальных интересов в информационном пространстве.

Анализ полномочий и функций Минцифры России в сфере обеспечения национальной безопасности свидетельствует о комплексном подходе к решению задач защиты информационного пространства страны, включая обеспечение устойчивости критической информационной инфраструктуры, защиту персональных данных граждан и противодействие киберугрозам. При этом динамичный характер развития информационных технологий и появление новых форм угроз требуют постоянного совершенствования нормативно-правовой базы и механизмов межведомственного взаимодействия для эффективного обеспечения национальной безопасности в цифровую эпоху.

Анализ роли Министерства цифрового развития в обеспечении информационной безопасности государства позволяет сделать вывод о формировании комплексной системы управления цифровой трансформацией страны. Министерство выступает ключевым координатором реализации государственной политики в сфере цифровой безопасности, обеспечивая эффективное взаимодействие между федеральными органами исполнительной власти, региональными структурами и институтами развития. Особое внимание уделяется мониторингу реализации федеральных проектов и своевременной корректировке принимаемых мер с учетом динамично меняющейся ситуации в глобальном цифровом пространстве.

Принципиальное значение в деятельности Министерства приобретает реализация масштабного комплекса национальных проектов в сфере цифровизации, претерпевших существенную трансформацию в период 2024-2025 годов. Переход от национальной программы «Цифровая экономика Российской Федерации» к национальному проекту «Экономика данных и цифровая трансформация государства» отражает качественное изменение подходов к цифровизации государственного управления. Новая архитектура проектов обеспечивает системное развитие цифровой инфраструктуры, отечественных технологических решений и кадрового потенциала отрасли, что создает прочную основу для укрепления национальной безопасности в цифровую эпоху.

Стратегическим направлением работы Министерства является обеспечение технологического суверенитета страны через развитие собственных цифровых решений и платформ. Особое внимание уделяется проектам в сфере искусственного интеллекта, информационной безопасности и развития спутниковых технологий связи. Важным аспектом деятельности выступает создание эффективной системы защиты критической информационной инфраструктуры при одновременном соблюдении баланса между обеспечением безопасности и защитой прав граждан, что находит

отражение в комплексном подходе к регулированию использования современных цифровых технологий.

В условиях возрастающих геополитических вызовов и технологического противостояния между странами Министерство цифрового развития демонстрирует способность к оперативной адаптации механизмов реализации национальных проектов. Формируется новая парадигма цифрового суверенитета, основанная на принципах технологической независимости и информационной самодостаточности. Особую значимость приобретает развитие межведомственного взаимодействия и координация усилий различных участников системы цифровой безопасности, включая научные организации, бизнес-структуры и институты гражданского общества.

В целом, анализ деятельности Министерства цифрового развития свидетельствует о системном подходе к решению задач обеспечения национальной безопасности в цифровую эпоху. Реализуемые национальные проекты создают необходимую технологическую и организационную базу для противодействия современным киберугрозам и укрепления позиций России в глобальном цифровом пространстве. При этом особое внимание уделяется развитию человеческого капитала и созданию условий для инновационного развития отечественной цифровой индустрии, что имеет стратегическое значение для обеспечения долгосрочной конкурентоспособности страны.

На основе проведенного анализа можно заключить, что современное состояние системы обеспечения информационной безопасности как составляющей национальной безопасности характеризуется рядом существенных проблем, требующих комплексного решения. К ним относятся технологическая зависимость от зарубежных решений в области информационной безопасности, отставание нормативно-правовой базы от темпов развития цифровых технологий, сложности в обеспечении баланса между государственным контролем в цифровой сфере и защитой конституционных прав граждан, а также рост киберпреступности и усиление угроз международного кибертерроризма. Ситуация осложняется

недостаточным уровнем цифровой грамотности населения, несовершенством механизмов защиты персональных данных и проблемой цифрового неравенства регионов.

Совершенствование системы обеспечения информационной безопасности требует комплексного подхода, включающего как развитие отечественных технологий защиты информации и модернизацию нормативно-правовой базы, так и укрепление международного сотрудничества в сфере противодействия киберугрозам при сохранении информационного суверенитета страны. Особую значимость приобретает необходимость четкого определения правового статуса уполномоченных должностных лиц и структурных подразделений, ответственных за информационную безопасность, развития военно-технического сотрудничества и формирования эффективных механизмов противодействия новым видам информационных угроз. При этом принципиальное значение имеет обеспечение научной обоснованности принимаемых решений и возможности оперативной адаптации нормативной базы к новым вызовам цифровой эпохи.

Список используемой литературы и используемых источников

1. Авдеев В.А., Авдеева О.А. Основные направления совершенствования правовой политики по обеспечению в условиях глобализации информационной безопасности // Российская юстиция. 2021. № 3. С. 2 - 4.
2. Акаев У.Ю. Национальная безопасность: понятие, виды, формы обеспечения // Образование. Наука. Научные кадры. 2020. №3. С. 94-95.
3. Алиева З. И., Хасбулатова З. М. Информационная безопасность как составная часть национальной безопасности Российской Федерации: конституционно-правовой аспект // Юридический вестник Дагестанского государственного университета. 2022. №3. С. 39-45.
4. Барков А.В., Киселев А.С. О правовом обеспечении безопасности информационно-телекоммуникационной инфраструктуры банков и государственных структур // Банковское право. 2022. № 4. С. 20 - 27.
5. Велихова Е.Я. Регулирующие органы в сфере телекоммуникаций и их воздействие на телекоммуникационные отношения в Российской Федерации и зарубежных странах // Право и экономика. 2016. № 2. С. 45 - 51.
6. Дубень А.К. Информационная безопасность в системе национальной безопасности: актуальные проблемы информационного права // Вопросы безопасности. 2023. №1. С. 51-57.
7. Дубень А.К. Отдельные аспекты правового обеспечения информационной безопасности в Российской Федерации // Закон и право. 2022. №7. С. 39-44.
8. Калужин Е. А. Проблемы информационной безопасности как составной части национальной безопасности России // Инфраструктурные отрасли экономики: проблемы и перспективы развития. 2015. №10. С. 89-91
9. Колоткина О.А. Вопросы обеспечения национальной безопасности государства в условиях цифровизации // Государственная власть и местное самоуправление. 2021. № 7. С. 7 - 10.

10. Логинова Е.В. Цифровые параметры обеспечения национальной безопасности современной России // Национальная безопасность / nota bene. 2019. №6. С. 11-24.
11. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. – Москва. – URL: <https://digital.gov.ru/ru/ministry/structure/> (дата обращения: 04.02.2025).
12. Молчанов Н.А., Матевосова Е.К. Доктрина информационной безопасности Российской Федерации (новелла законодательства) // Актуальные проблемы российского права. 2017. № 2. С. 159 - 165.
13. Морозова С.С., Смирнова Ю.Г. Особенности правового регулирования цифрового управления и безопасности в современной России // ПОЛИТЭКС. 2023. №1. С. 123-132.
14. Перечень государственных программ, национальных и федеральных проектов, приоритетных программ и проектов в Российской Федерации. 2024// СПС «КонсультантПлюс»
15. Полякова Т.А., Минбалеев А. В., Бойченко И.С. Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде // Вестник Академии права и управления. 2018. №3 (52). С. 32-36.
16. Попова Е.А., Мартемьянова З.С. Государственная политика в области цифровой трансформации общества // Государственное и муниципальное управление. Ученые записки. 2018. №3. С. 162-166.
17. Постановление Правительства РФ от 02.03.2019 № 234 (ред. от 01.08.2024) «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» (вместе с «Положением о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации») // СПС «КонсультантПлюс».
18. Постановление Правительства РФ от 02.06.2008 № 418 (ред. от 15.03.2024) «О Министерстве цифрового развития, связи и массовых

коммуникаций Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2024) // СПС «КонсультантПлюс».

19. Редкоус В.М. Некоторые вопросы совершенствования правового регулирования в области обеспечения информационной безопасности // Аграрное и земельное право. 2022. №9 (213). С.143-146.

20. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации // СПС «КонсультантПлюс».

21. Шинкарецкая Г.Г., Берман А.М. Цифровизация и проблема обеспечения национальной безопасности // Образование и право. 2020. №5. С. 254-258.