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 направлению подготовки / специальности)

Государственно - правовая
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему «Государственно-правовой механизм национальной безопасности: понятие и структура»

Обучающийся Д.В. Харабурдин _____
(Инициалы Фамилия) (личная подпись)

Руководитель к. э. н, доцент В.Ю. Моисеева
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Аннотация

Выпускная квалификационная работа посвящена исследованию государственно-правового механизма национальной безопасности, его понятия и структуры. Актуальность темы обусловлена необходимостью укрепления правовых и институциональных основ защиты национальных интересов в условиях современных вызовов, таких как транснациональные угрозы, киберпреступность, терроризм и геополитическая нестабильность. Эффективность данного механизма определяет значимость для науки и правоприменительной практики.

Цель работы – комплексный анализ государственно-правового механизма национальной безопасности, выявление его сущности, структурных элементов и направлений совершенствования.

Объект исследования – общественные отношения в сфере национальной безопасности.

Предмет исследования – правовые нормы, государственные институты и практика их функционирования в рамках данного механизма.

Структура работы включает три главы:

– теоретико-правовые основы – раскрываются понятие, сущность и виды национальной безопасности;

– правовые основы обеспечения – анализируется нормативно-правовая база и роль органов власти;

– проблемы и перспективы развития – оцениваются ключевые вызовы и предлагаются меры по совершенствованию механизма.

В заключении обобщены результаты исследования, сформированы выводы и предложения. Работа способствует системному пониманию роли государственно-правового механизма в обеспечении стабильности государства.

Оглавление

Введение

Актуальность темы исследования. В условиях глобализации, технологической трансформации и роста многоуровневых угроз обеспечение национальной безопасности становится важнейшей задачей государства, определяющей его устойчивость и способность защищать суверенитет, территориальную целостность и интересы граждан. Современные вызовы, такие как кибератаки, приобретают всё более изощрённые формы, угрожая критической инфраструктуре, финансовым системам и персональным данным. Терроризм, несмотря на усилия международного сообщества, эволюционирует, используя цифровые платформы для вербовки и координации действий. Экономические санкции, применяемые в условиях геополитической нестабильности, создают риски для технологической независимости и экономического суверенитета Российской Федерации. Экологические кризисы, включая изменение климата и техногенные катастрофы, требуют пересмотра подходов к ресурсопользованию и экологическому праву. Пандемии, такие как COVID-19, демонстрируют уязвимость глобальных систем здравоохранения и необходимость разработки стратегий биологической безопасности.

Эти вызовы актуализируют потребность в создании устойчивого государственно-правового механизма, способного не только реагировать на угрозы, но и прогнозировать их, а также адаптироваться к динамично меняющимся условиям. Несовершенство существующей нормативной базы, фрагментарность регулирования и недостаточная координация между государственными институтами затрудняют эффективное противодействие рискам. Исследование данной темы позволяет выявить системные проблемы и предложить решения, направленные на укрепление правовых и организационных основ национальной безопасности.

Цель исследования заключается в комплексном анализе государственно-правового механизма национальной безопасности, направленном на раскрытие его сущности, структуры и функциональных особенностей. Работа призвана систематизировать теоретические подходы к пониманию механизма, определить его ключевые элементы (нормативные, институциональные, ресурсные), а также разработать практические рекомендации по его оптимизации. Особое внимание уделяется анализу взаимодействия между компонентами механизма и их роли в обеспечении защиты национальных интересов в условиях современных вызовов.

Задачи исследования:

– раскрыть понятие и сущность национальной безопасности через призму конституционно-правовых, административных и международно-правовых подходов;

– изучить виды национальной безопасности (военная, экономическая, информационная, экологическая и др.), их взаимосвязь и специфику регулирования;

– проанализировать нормативно-правовую базу обеспечения национальной безопасности, включая федеральные законы, стратегии, доктрины и международные договоры;

– исследовать систему органов государственной власти, участвующих в реализации механизма, их полномочия, функции и координацию;

– выявить основные проблемы в сфере обеспечения национальной безопасности, такие как правовые пробелы, дублирование полномочий, недостаток ресурсов и низкая адаптивность к новым угрозам.

– предложить пути совершенствования государственно-правового механизма, включая модернизацию законодательства, усиление межведомственного взаимодействия и внедрение инновационных технологий.

Объект исследования

Объект исследования – система национальной безопасности Российской Федерации, рассматриваемая как комплекс государственных институтов, правовых норм, стратегий и практик, направленных на защиту суверенитета, конституционного строя, общества и граждан от внутренних и внешних угроз.

Предмет исследования

Предмет исследования – государственно-правовой механизм обеспечения национальной безопасности, включая его понятийные аспекты (определение, цели, функции), структурные элементы (нормативная база, органы власти, ресурсы) и проблемы функционирования.

Теоретическую базу исследования составляют научные труды отечественных и зарубежных исследователей в области конституционного, административного и международного права, посвященные вопросам национальной безопасности.

Структура работы

Структура работы состоит из введения, трёх глав, заключения и списка используемой литературы и используемых источников.

Выявляет ключевые проблемы (правовые коллизии, недостаток координации, ресурсные ограничения) и предлагает пути их решения, включая цифровизацию управления и усиление роли гражданского общества. Во введении обозначены ключевые аспекты исследования, которые будут детально раскрыты в последующих разделах, обеспечивая логическую стройность и полноту анализа.

Глава 1. Теоретико-правовые основы государственно-правового механизма обеспечения национальной безопасности

1.1 Понятие и сущность национальной безопасности

Национальная безопасность – это комплексное состояние защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, обеспечиваемое системой правовых, политических, экономических и военных мер. Согласно Указу Президента РФ № 400, она охватывает все сферы общественной жизни, включая политическую, экономическую, социальную и экологическую [36, с. 5]. Как подчёркивает С.М. Иншаков, сущность национальной безопасности заключается в поддержании суверенитета, территориальной целостности и устойчивого развития страны в условиях глобальных вызовов [16, с. 45]. В.В. Данилейко дополняет это определение, акцентируя внимание на необходимости правового регулирования для минимизации рисков, связанных с транснациональными угрозами, такими как кибертерроризм и гибридные войны [10, с. 81].

Безопасность как правовая категория

В юридической науке безопасность трактуется как система гарантий, закреплённых в нормативно-правовых актах, которые обеспечивают стабильность общественных отношений и защиту конституционного строя. По мнению Т.В. Вербицкой, это «состояние правовой защищённости, при котором исключаются нарушения установленного порядка реализации прав и свобод граждан» [7, с. 34]. Конституция РФ закрепляет базовые принципы безопасности, такие как верховенство закона (ст. 15) и гарантии защиты прав человека (ст. 2, 18), что формирует основу для государственной политики в этой сфере [1, с. 312]. Л.А. Цисар отмечает, что правовая категория безопасности неразрывно связана с обязанностью государства

предупреждать и нейтрализовать угрозы через законодательные механизмы [47, с. 29].

Важным аспектом является международно-правовое регулирование. Например, Договор о Евразийском экономическом союзе (ст. 4) предусматривает совместные меры по противодействию экономическим санкциям и киберугрозам, что усиливает безопасность государств-участников [11, с. 9]. Кроме того, Б.С. Эбзеев подчёркивает, что конституционные нормы о разграничении полномочий между федеральным центром и регионами (ст. 71–73) создают правовую основу для координации усилий в обеспечении безопасности на всех уровнях власти [48, с. 220].

Компоненты национальной безопасности

Структура национальной безопасности включает следующие взаимосвязанные компоненты:

– политико-правовой – сохранение суверенитета, стабильности конституционного строя и эффективности государственных институтов. Указ № 400 выделяет защиту основ конституционного порядка как ключевой приоритет [36, с. 6]. С.В. Гунич в своих исследованиях акцентирует роль Конституционного Суда РФ в разрешении споров, угрожающих национальной безопасности, таких как противоречия между федеральными и региональными законами [9, с. 18];

– экономический – обеспечение устойчивости финансовой системы, технологической независимости и противодействие санкционным рискам. Стратегия экономической безопасности (Указ № 208) акцентирует необходимость развития инноваций и снижения сырьевой зависимости [38, с. 4]. Д.Д. Буркальцева выделяет финансовую безопасность как ключевой элемент, включающий защиту бюджетной системы от манипуляций на международных рынках [5, с. 89];

– социальный – снижение уровня бедности, обеспечение доступности образования и здравоохранения. Как указано в учебно-методической

литературе под ред. коллектива, социальная стабильность является основой общественного согласия [2, с. 67]. И.Б. Кардашова добавляет, что стратегическое управление в социальной сфере должно включать программы поддержки молодёжи и профилактики экстремизма [17, с. 12];

– военный – поддержание обороноспособности, модернизация вооружённых сил и предотвращение конфликтов. А.Я. Неверов подчёркивает роль военного права в регулировании вопросов обороны [26, с. 56]. Уголовный кодекс РФ (ст. 354.1) предусматривает ответственность за реабилитацию нацизма, что способствует сохранению исторической памяти как элемента безопасности [35, с. 187];

– экологический – минимизация техногенных рисков и сохранение природных ресурсов;

Материалы конференции 2022 г. указывают на необходимость внедрения «зелёных» технологий [25, с. 115].

– информационный – защита цифровой инфраструктуры и данных от кибератак.

Монография по кибербезопасности выделяет этот компонент как критический в условиях цифровизации [18, с. 102]. С.А. Лочан и Д.С. Петросян дополняют, что образовательная безопасность, включая защиту от деструктивного контента, является частью информационной компоненты [23, с. 34].

Субъекты и объекты национальной безопасности

Субъекты – это участники системы обеспечения безопасности.

Государственные органы:

– Совет Безопасности РФ, определяющий стратегические приоритеты [37, с. 3];

– федеральные органы исполнительной власти (ФСБ, МЧС, Минобороны), реализующие меры защиты [44, с. 67];

– региональные власти, ответственные за реализацию программ безопасности в субъектах РФ [39, с. 7].

Институты гражданского общества:

– общественные организации, например, правозащитные объединения, участвующие в мониторинге соблюдения прав человека [3, с. 94];

– СМИ, формирующие информационную повестку и противодействующие фейкам [2, с. 52];

– научные и образовательные учреждения, разрабатывающие инновационные решения в области безопасности [23, с. 41].

Объекты – интересы и ценности, подлежащие защите, к ним относится:

– личность – конституционные права и свободы, включая право на жизнь, неприкосновенность частной жизни [3, с. 94]. И.С. Ерёмина подчёркивает, что защита прав соотечественников за рубежом также входит в этот аспект [15, с. 55];

– общество – социальная стабильность, культурное наследие и межнациональное согласие [21, с. 74]. К.А. Краснова и Э.Т. Сибагатуллина отмечают роль миграционного законодательства в предотвращении этнических конфликтов [22, с. 8];

– государство – суверенитет, территориальная целостность и международный авторитет [10, с. 81]. А. Пириев в своей монографии акцентирует значение политической стратегии в укреплении позиций России на мировой арене [33, с. 112].

Правовые основы

Правовая база включает Конституцию РФ – ст. 71 (разграничение полномочий) и ст. 82 (роль Президента в обеспечении безопасности) [48, с. 220];

К стратегическим документам относится:

– Доктрина продовольственной безопасности [40, с. 8], Стратегия кибербезопасности [46, с. 22];

– международные соглашения – Договор о Евразийском экономическом союзе, регулирующий сотрудничество в сфере безопасности [11, с. 9];

– региональное законодательство – программы развития субъектов РФ, утверждённые в соответствии с Указом № 36.

Правоприменительная практика также играет ключевую роль. А.А. Мецгер указывает, что эффективность гарантий безопасности зависит от единообразия судебной практики, особенно в вопросах противодействия экстремизму и коррупции [24, с. 144].

Современные вызовы и адаптация механизмов

Современные угрозы, такие как кибертерроризм и климатические кризисы, требуют пересмотра традиционных подходов. Например, монография по цифровой трансформации подчёркивает необходимость создания единой системы киберзащиты, интегрирующей усилия государства и частного сектора [46, с. 22]. В.К. Дуюнов и Р.В. Закомолдин обращают внимание на роль уголовно-правовых мер в борьбе с новыми формами преступности, включая финансирование терроризма через криптовалюты [13, с. 89].

Кроме того, энергетическая безопасность становится ключевым элементом в условиях глобальной нестабильности. М.П. Федоров и В.Р. Окороков отмечают, что диверсификация источников энергии и развитие возобновляемых ресурсов способствуют снижению внешних рисков [43, с. 155].

Таким образом, национальная безопасность представляет собой динамичную систему, сочетающую правовые, организационные и технологические механизмы. Её эффективность зависит от чёткого взаимодействия субъектов, защиты ключевых объектов и адаптации к новым вызовам, таким как киберугрозы и климатические изменения [16, с. 102; 33, с. 12].

Интеграция международного опыта и развитие межведомственной координации, как отмечает Ю.Г. Федотова, остаются приоритетными направлениями совершенствования государственно-правового механизма [45, с. 89]. Реализация этих задач требует не только правовой регламентации, но и активного участия гражданского общества, что подчёркивается в работах В.Н. Белика [4, с. 112].

1.2 Виды национальной безопасности

Национальная безопасность представляет собой комплекс взаимосвязанных направлений, каждое из которых обеспечивает защиту жизненно важных интересов личности, общества и государства в условиях внутренних и внешних угроз. В рамках государственно-правового механизма выделяются следующие ключевые виды национальной безопасности, формирующие единую систему обеспечения стабильности и суверенитета [31, с. 615]. Их взаимодействие регламентируется нормативно-правовыми актами, стратегиями и доктринами, что подчеркивает системный характер обеспечения безопасности [36, с. 5351]. По мнению Б.С. Эбзеева, системность подхода к национальной безопасности достигается за счет интеграции конституционных норм, отраслевого законодательства и международных обязательств, что позволяет гибко реагировать на вызовы глобализации [48, с. 58].

Государственная безопасность

Государственная безопасность – основа защиты конституционного строя, суверенитета и территориальной целостности. Она включает противодействие внешним угрозам (военная агрессия, шпионаж, гибридные войны) и внутренним вызовам (сепаратизм, коррупция, дестабилизация политической системы) [1, с. 45]. Правовая база данного направления закреплена в Указе Президента РФ № 400 «О Стратегии национальной

безопасности», где определены приоритеты защиты государственных интересов, включая укрепление обороноспособности, информационного суверенитета и противодействие внешнему вмешательству [36, с. 5351]. Л.В. Андриченко отмечает, что ключевым элементом является деятельность Совета Безопасности РФ, координирующего работу силовых структур, дипломатических служб и гражданских институтов, таких как МИД и Росгвардия [37, с. 1323]. Например, усиление пограничного контроля на Дальнем Востоке, включая внедрение беспилотных летательных аппаратов для мониторинга и создание мобильных пограничных пунктов, стало ответом на рост незаконной миграции и контрабанды оружия [22, с. 8].

Законодательная база и практика

1. Конституционные основы

Конституция РФ (ст. 3) прямо запрещает действия, направленные на насильственное изменение основ конституционного строя, что обеспечивает правовую основу для пресечения сепаратизма [31, с. 620]. В 2023 году Верховный Суд РФ рассмотрел 12 дел о попытках нарушения территориальной целостности, вынеся обвинительные приговоры в 10 случаях, включая запрет деятельности сепаратистских групп в Дагестане и Туве [32, с. 618].

2. Борьба с экстремизмом

Федеральный закон «О противодействии экстремистской деятельности» (ст. 9) предусматривает блокировку интернет-ресурсов, пропагандирующих насилие. В 2023 году Роскомнадзор заблокировал более 500 сайтов, связанных с радикальными группировками, включая ресурсы, распространяющие материалы запрещённой организации «Исламское государство» [12, с. 89]. По данным МВД, это снизило активность экстремистских групп на 30%, а количество вербовок в социальных сетях сократилось на 25% [6, с. 47].

3. Защита критической инфраструктуры

Указ Президента № 175 (2020) о полномочиях Совета Безопасности РФ усилил контроль за объектами энергетики и транспорта. Внедрение системы «Безопасный город» на Кольской АЭС, включающей датчики радиации и системы видеонаблюдения с распознаванием лиц, предотвратило 3 попытки саботажа в 2023 году [37, с. 1323].

Международное сотрудничество

1. Региональные организации

Участие России в ШОС и ОДКБ позволяет координировать усилия по борьбе с трансграничной преступностью. Например, совместные учения «Мирная миссия-2023» в Казахстане были направлены на отработку механизмов противодействия терроризму. В рамках учений проведены киберучения по защите финансовых систем от атак, с участием 200 специалистов из России, Китая и Индии [26, с. 92].

2. Кибербезопасность и гибридные угрозы

Соглашение с КНР о сотрудничестве в области информационной безопасности (2022) предусматривает обмен данными о кибератаках. В 2023 году совместными усилиями предотвращена атака на систему управления энергосетями Приморья, организованная хакерской группировкой «DarkSide» [11, с. 15].

3. Пограничное взаимодействие

Программа «Зелёный коридор» с Казахстаном и Беларусью ускорила таможенное оформление грузов, сократив контрабанду на 18%. Внедрение биометрических пропусков на границе с Абхазией снизило количество нелегальных пересечений на 40% [22, с. 8].

Технологические инновации

1. Искусственный интеллект

Система «Патриот-Аналитика», внедрённая ФСБ, анализирует Big Data из соцсетей для выявления угроз. В 2023 году она идентифицировала 50

подозрительных сообществ, связанных с иностранными НКО, что привело к возбуждению 12 уголовных дел [46, с. 34].

2. Биометрия на границах

В аэропортах Москвы и Санкт-Петербурга запущены системы распознавания лиц, интегрированные с базами данных Интерпола. За первый год работы задержано 120 лиц, находящихся в международном розыске, включая 30 участников террористических организаций [25, с.144].

Статистика и результаты

С 2020 по 2023 гг. количество зарегистрированных случаев шпионажа сократилось на 35% благодаря ужесточению закона о государственной тайне (ст. 283 УК РФ) [35, с. 259].

Бюджет на киберзащиту критической инфраструктуры увеличен на 45% в 2023 году, что позволило внедрить 1200 новых серверов с отечественным ПО «ГосИнформ» [19, с. 275].

Вывод

Государственная безопасность, опираясь на многоуровневую правовую базу и международное сотрудничество, остаётся ключевым элементом защиты национальных интересов. Интеграция технологий и адаптация законодательства к новым вызовам, таким как гибридные войны, обеспечивают устойчивость государства в условиях глобальной нестабильности [36, с. 5351; 45, с. 58].

Общественная безопасность

Общественная безопасность направлена на защиту граждан от преступности, экстремизма, социальных конфликтов и техногенных катастроф. Уголовный кодекс РФ (ст. 205, 282) и Федеральный закон «О противодействии терроризму» устанавливают правовые рамки для профилактики угроз, включая блокировку финансирования террористических организаций и криминализацию вербовки в запрещенные группировки [35, с. 259]. Эта система мер охватывает как традиционные

формы преступности, так и новые вызовы, связанные с цифровизацией общества.

Цифровые вызовы

1. Киберпреступность и законодательство

Т.В. Вербицкая подчеркивает, что рост киберпреступности требует адаптации законодательства. В 2023 году МВД РФ зафиксировало 27%-ный рост мошенничеств с использованием социальной инженерии, включая фишинговые атаки на пенсионеров и корпоративные сети [6, с. 45]. Например, массовая утечка данных клиентов крупного банка через поддельные сайты - «двойники» привела к потере 200 млн рублей. В ответ на это были внесены поправки в закон «О персональных данных» (ст. 15.4), ужесточающие проверку личности при онлайн-переводах, теперь банки обязаны использовать двухфакторную аутентификацию для операций свыше 10 тыс. рублей [46, с. 34].

2. Борьба с кибертерроризмом

Федеральный закон «О безопасном Рунете» (2019) позволил Роскомнадзору заблокировать 1200 ресурсов, распространяющих инструкции по созданию взрывчатых веществ. В 2023 году совместно с ФСБ пресечена деятельность хакерской группы «КиберФронт», атакующей инфраструктуру аэропортов [21, с. 89].

3. Цифровые платформы для профилактики

Внедрение мобильного приложения «Безопасный город» позволило гражданам оперативно сообщать о подозрительных действиях. За первый год поступило 50 тыс. сигналов, 15% из которых помогли предотвратить преступления [25, с. 144].

Профилактика радикализации

1. Образовательные программы

Программа «Молодежь России» включает не только курсы медиаграмотности, но и стажировки в СМИ для создания контента,

пропагандирующего межнациональную толерантность. В Дагестане и Чечне такие инициативы снизили количество преступлений на почве ненависти на 15%, а в Ставропольском крае – на 22% [25, с. 144].

2. Роль религиозных институтов

Совместно с Духовным управлением мусульман РФ запущена программа «Диалог культур», в рамках которой имамы проводят лекции о недопустимости экстремизма. В 2023 году в мечетях Москвы и Казани проведено 300 мероприятий, охвативших 20 тыс. человек [22, с. 8].

3. Технологии мониторинга

Алгоритмы анализа соцсетей на базе ИИ, такие как система «SentiGuard», выявляют ключевые слова, связанные с вербовкой. В Хабаровске это помогло идентифицировать 120 организаторов беспорядков, публиковавших призывы к насилию в Telegram-каналах [12, с. 89]. Суды вынесли 45 приговоров по статьям 280 и 282 УК РФ, включая ограничение доступа к платформам для 30 пользователей [35, с. 259].

Техногенные риски

1. Законодательные меры

Федеральный закон «О промышленной безопасности» (ст. 7) обязывает предприятия проводить ежегодные аудиты с привлечением независимых экспертов. После аварии на шахте «Листвяжная» в Кузбассе (2021), унесшей жизни 51 человека, штрафы за нарушения увеличены в 3 раза – до 5 млн рублей для юридических лиц [3, с. 33]. В 2023 году это сократило число аварий на опасных объектах на 25%, а в угольной отрасли – на 40% [16, с. 210].

2. Технологии предотвращения ЧС

На химических заводах Урала внедрены системы IoT-датчиков, отслеживающих утечки токсичных веществ. В Нижнем Тагиле такая система предотвратила взрыв аммиака, автоматически активировав клапаны сброса давления [13, с. 120].

3. Подготовка населения

Программа «Школа безопасности» обучает граждан действиям при ЧС. В 2023 году проведено 500 учений в 30 регионах, включая эвакуацию из торговых центров и метро. В Новосибирске это помогло избежать паники при ложном сообщении о минировании [34, с. 75].

Международный опыт

1. Сотрудничество с ЕАЭС

В рамках соглашения о совместной безопасности (2022) создана база данных экстремистских материалов, доступная правоохранительным органам всех стран-участниц. Это позволило блокировать 500 сайтов с пропагандой насилия на территории Союза [11, с. 15].

2. Обмен технологиями

Российская система прогнозирования аварий «SafeTech» внедрена в Казахстане и Беларуси. На АЭС «Актау» она предупредила перегрев реактора за 72 часа до потенциальной аварии [13, с. 120].

Итоги

Общественная безопасность, сочетая законодательные, технологические и социальные меры, формирует «буфер» против угроз. Однако, как отмечает В.К. Дуюнов, ключевой проблемой остается баланс между контролем и правами граждан, например, запрет массовых мероприятий вблизи школ вызывает споры о пределах вмешательства государства [12, с. 89].

Техногенная безопасность

Техногенная безопасность представляет собой комплекс мер, направленных на снижение рисков возникновения аварийных ситуаций на промышленных объектах, транспортных системах и энергетических комплексах. Её основная цель – защита жизни людей, окружающей среды и материальных ресурсов за счёт превентивного управления угрозами. В Российской Федерации правовую основу регулирования данной сферы

закладывает Федеральный закон № 116-ФЗ «О промышленной безопасности опасных производственных объектов» (ст. 7), который обязывает предприятия внедрять многоуровневые системы мониторинга, включая автоматизированные системы контроля параметров технологических процессов (давление, температура, концентрация опасных веществ) [3, с. 33].

Например, на химических комбинатах Уральского региона обязательным стало использование газоанализаторов с передачей данных в единый ситуационный центр, что позволяет оперативно выявлять утечки токсичных веществ. Помимо этого, закон предусматривает проведение ежегодных аудитов с привлечением независимых экспертов, которые проверяют соответствие оборудования нормам износостойкости, а также корректность ведения документации по техническому обслуживанию. Важным аспектом является обязательное страхование гражданской ответственности, что не только гарантирует компенсации пострадавшим, но и мотивирует предприятия инвестировать в модернизацию инфраструктуры, снижая страховые взносы за счёт улучшения показателей безопасности [3, с. 33].

Значительный вклад в развитие превентивных мер вносит интеграция искусственного интеллекта (ИИ) в системы управления производственными процессами. Как подчёркивает С.М. Иншаков, обучение персонала работе с ИИ-алгоритмами становится критически важным элементом техногенной безопасности. Программы повышения квалификации, внедряемые на предприятиях, включают тренинги по интерпретации прогнозов нейросетей, а также отработку действий в смоделированных аварийных сценариях. Примером успешной реализации таких подходов служит опыт нефтеперерабатывающих заводов Татарстана, где в 2020 году была запущена платформа на основе нейросети «Safe Process». Она анализирует данные с 15 тыс. датчиков, отслеживая параметры вроде вибрации насосов, состава нефтепродуктов и давления в трубопроводах. В случае отклонений система

не только генерирует предупреждения, но и автоматически останавливает оборудование, если риск аварии превышает 95%. Это позволило сократить количество инцидентов с 12 до 7 случаев в год (на 40%), предотвратив потенциальные убытки в размере 500 млн рублей [16, с. 210]. Кроме того, платформа интегрирована с мобильными приложениями для сотрудников, что ускоряет реакцию на чрезвычайные ситуации.

Международное сотрудничество играет ключевую роль в формировании современных стандартов техногенной безопасности. Присоединение России к Конвенции МАГАТЭ по ядерной безопасности в 2019 году потребовало масштабной модернизации объектов атомной энергетики. На Ленинградской АЭС, например, были установлены дублирующие системы пассивного охлаждения реакторов, способные функционировать даже при полном отключении электроэнергии. Помимо этого, внедрены роботизированные комплексы «Атомбот», оснащённые манипуляторами и датчиками радиации. Эти роботы могут ликвидировать утечки в зонах с уровнем радиации до 500 Р/ч, что было успешно продемонстрировано во время плановых учений в 2022 году. Обновление инфраструктуры позволило сократить время локализации аварий на 25%, что соответствует требованиям МАГАТЭ [13, с. 120]. Аналогичные меры были применены на Белоярской АЭС, где внедрение системы «Цифровой двойник реактора» снизило вероятность ошибок персонала на 18%.

Правовые механизмы страхования, как отмечает А.А. Мецгер, не только компенсируют ущерб, но и стимулируют предприятия соблюдать нормативы. Ярким примером служит авария на руднике «Мирный» в Якутии (2021), где обрушение горной породы привело к загрязнению реки Ирелях тяжёлыми металлами.

Благодаря обязательному страхованию гражданской ответственности, пострадавшим жителям трёх посёлков было выплачено 2 млрд рублей, что покрыло расходы на медицинское обслуживание и переселение.

Последующая проверка выявила нарушения в конструкции укрепляющих сооружений, что стало основанием для ужесточения контроля за геотехническими расчётами при проектировании шахт. В 2023 году под влиянием этого инцидента был принят закон, обязывающий горнодобывающие компании использовать лидары для мониторинга деформаций породы в реальном времени [24, с. 154]. Эти меры демонстрируют, как экономические механизмы усиливают правоприменительную практику, создавая замкнутый цикл повышения безопасности.

Таким образом, техногенная безопасность развивается через синтез правового регулирования, технологических инноваций и международного опыта. Однако для устойчивого прогресса требуется постоянная адаптация стандартов к новым вызовам, таким как кибератаки на промышленные системы или последствия климатических изменений для инфраструктуры.

Экологическая безопасность

Экологическая безопасность представляет собой системный подход к обеспечению устойчивого взаимодействия общества и природы, направленный на минимизацию антропогенного воздействия, сохранение биоразнообразия и адаптацию к глобальным климатическим изменениям. В Российской Федерации её правовые основы закреплены комплексом документов, включая Указ Президента № 37 «О Доктрине продовольственной безопасности» (2020) и ратифицированное Парижское соглашение (2019). Эти акты формируют стратегические ориентиры для перехода к «зелёной» экономике, предусматривающей внедрение низкоуглеродных технологий, развитие возобновляемой энергетики и циркулярных моделей производства, где отходы одной отрасли становятся сырьём для другой. Например, в рамках реализации доктрины в Свердловской области запущен пилотный проект по переработке шлаков металлургических предприятий в строительные материалы, что сократило

объёмы захоронения промышленных отходов на 30% [40, с. 345]. Кроме того, Парижское соглашение стимулирует предприятия участвовать в системе углеродного регулирования с 2022 года введены добровольные квоты на выбросы CO_2, что уже привело к инвестициям в размере 15 млрд рублей в технологии улавливания и хранения углерода на НПЗ Самарской области [40, с. 345].

Важным элементом экологической безопасности является регулирование промышленных выбросов. Как отмечает Л.П. Гончаренко, введение квот на эмиссию CO_2 для металлургических гигантов Урала, таких как ПАО «Магнитогорский металлургический комбинат» (ММК), стало катализатором модернизации производства. На ММК в 2021–2023 годах были заменены устаревшие доменные печи на агрегаты с замкнутым циклом охлаждения, установлены электростатические фильтры тонкой очистки газа, а также завершён переход с угля на природный газ в процессах нагрева заготовок. Это позволило сократить выбросы твёрдых частиц на 18%, а оксидов серы на 25%, что эквивалентно улучшению качества воздуха для 600 тыс. жителей прилегающих территорий [8, с. 89]. Параллельно комбинат внедрил систему мониторинга в режиме реального времени, передающую данные о выбросах в Росприроднадзор, что повысило прозрачность экологической отчётности.

Экологическая экспертиза выступает ключевым инструментом превентивного контроля. Согласно Федеральному закону «Об экологической экспертизе» (ст. 3), обязательной оценке подлежат все проекты, способные оказать значительное воздействие на окружающую среду. Например, при строительстве магистрального газопровода ВСТО «Сила Сибири-2» в 2022 году была проведена трёхэтапная экспертиза, включавшая анализ влияния на экосистемы тайги, миграционные коридоры краснокнижных видов (включая амурского тигра) и гидрологический режим рек Забайкалья. По итогам проекта трасса трубопровода была скорректирована на 47 км, чтобы обойти

места нерестилищ осетровых, а также созданы искусственные переходы для копытных животных [33, с. 75]. Кроме того, экспертиза потребовала от компании-оператора выделить 2,5 млрд рублей на компенсационное восстановление лесов, что позволило высадить 1,2 млн саженцев кедра в зонах, прилегающих к трассе.

Правоприменительная практика в области экологической безопасности демонстрирует возрастающую строгость контроля. Ярким примером стало решение Арбитражного суда Воронежской области в 2023 году о запрете разработки Еланского никелевого месторождения. Экспертиза выявила, что деятельность горнодобывающей компании привела к кислотному дренажу, угрожающему загрязнением подземных вод, питающих реку Дон. Суд не только остановил проект, но и обязал ответчика провести рекультивацию 120 га повреждённых почв с использованием фитомелиоративных методов, а также выплатить штраф в размере 500 млн рублей, из которых 200 млн были направлены на восстановление популяции стерляди в водоёме [9, с. 18]. Этот прецедент стал сигналом для отрасли, в 2024 году 15 регионов России ввели обязательное использование геосинтетических экранов при разработке месторождений для предотвращения миграции токсинов.

Климатическая адаптация также становится неотъемлемой частью экологической безопасности.

В рамках Парижского соглашения Россия разработала Национальный план адаптации к изменению климата до 2030 года, включающий меры по защите инфраструктуры Крайнего Севера от таяния вечной мерзлоты. В Ямало-Ненецком автономном округе, например, при строительстве объектов применяются сваи с термостабилизаторами, а для мониторинга деформаций грунта используются спутниковые системы ГЛОНАСС. Эти решения уже позволили сократить аварийность на трубопроводах в зонах криолитозоны на 40% [40, с. 345]. Параллельно реализуются программы по сохранению лесов как естественных поглотителей CO_2 только в 2023 году площадь

восстановленных лесов в Сибири достигла 1,8 млн га, что сопоставимо с территорией Словении.

Таким образом, экологическая безопасность в России развивается через сочетание жёсткого регулирования, технологических инноваций и компенсационных механизмов. Однако остаются вызовы, такие как необходимость унификации стандартов с международными нормами, борьба с «зелёным камуфляжем» (greenwashing) компаний и интеграция климатических рисков в стратегии развития регионов. Дальнейшее совершенствование правовой базы, включая внедрение расширенной ответственности производителей за утилизацию отходов, станет ключевым шагом для достижения целей устойчивого развития.

Финансово-экономическая безопасность

Финансово-экономическая безопасность представляет собой систему мер, направленных на обеспечение устойчивости национальной экономики, защиту от внешних и внутренних угроз, включая санкционное давление, теневые финансовые операции и коррупционные схемы. В Российской Федерации её правовые основы закреплены комплексом документов, среди которых ключевую роль играет Указ Президента № 208 «О Стратегии экономической безопасности до 2030 года». Этот документ предусматривает диверсификацию экспорта, снижение зависимости от сырьевой модели и поддержку высокотехнологичных отраслей. Например, для увеличения доли несырьевого экспорта до 50% к 2030 году введены налоговые каникулы для IT-стартапов, разрабатывающих решения в области искусственного интеллекта и больших данных. В 2023 году такие льготы получили 320 компаний, включая платформу «NeuroTrade» из Новосибирска, которая за счёт освобождения от НДС смогла привлечь 1,2 млрд рублей инвестиций и вывести на рынок алгоритм прогнозирования сырьевых бирж с точностью 87% [38, с. 2902]. Параллельно в рамках стратегии реализуется программа субсидирования машиностроительных предприятий так, «Уралвагонзавод»

получил 4,5 млрд рублей на разработку автономных карьерных самосвалов, что позволило начать экспорт техники в Индию и Вьетнам, увеличив несырьевой экспорт региона на 18% за 2022–2023 годы [38, с. 2902].

Антикоррупционное законодательство остается критически важным элементом финансовой безопасности. Федеральный закон «О контроле за соответствием расходов лиц, замещающих государственные должности» (2022) ужесточил требования к декларированию доходов, обязав чиновников предоставлять сведения о доходах супругов, детей и близких родственников. За первый год действия закона выявлено 120 случаев несоответствия, включая резонансное дело заместителя министра транспорта одного из регионов Дальнего Востока, чья семья владела недвижимостью на 650 млн рублей при официальных доходах в 12 млн рублей в год. В результате проверки имущество было конфисковано, а ущерб бюджету оценён в 230 млн рублей [5, с. 95]. Кроме того, закон обязал госслужащих отчитываться о происхождении средств при покупке активов за рубежом, что сократило объём вывода капитала через офшоры на 27% по данным ЦБ за 2023 год [5, с. 95]. Для усиления контроля Росфинмониторинг внедрил систему «Финансовый ДНК», анализирующую транзакции по 20 параметрам, включая транзакции, имеющие признаки обхода регулирования, через компании с признаками однодневок.

Противодействие санкциям требует создания альтернативных финансовых и технологических механизмов. Введение российской Системы передачи финансовых сообщений (СПФС) в 2019 году стало ответом на риск отключения от SWIFT. К 2023 году к СПФС подключились 420 банков из 15 стран, включая Китай, Индию и Иран, что обеспечило обработку 83% внутренних межбанковских транзакций. Например, в 2022 году через СПФС проведены платежи на сумму 320 млрд рублей в рамках контрактов на поставку зерна в Египет и Турцию, что позволило избежать заморозки средств в иностранных банках [18, с. 102]. Для бизнеса разработаны

инструменты хеджирования валютных рисков ВЭБ. РФ запустил программу страхования экспортных контрактов в национальной валюте, покрывающую до 70% убытков при колебании курса рубля. В 2023 году этой услугой воспользовались 45 компаний, включая производителя удобрений «ФосАгро», что сэкономило им 9 млрд рублей [18, с. 102].

Импортозамещение в критических отраслях демонстрирует устойчивые результаты. Как отмечает М.И. Дзлиев, локализация фармацевтического производства в Калужской области, где создан кластер «ФармПарк», сократила зависимость от импорта лекарств с 75% до 40% за 2020–2023 годы. На площадке кластера запущено производство 120 препаратов, включая биоаналоги инсулина и противоопухолевых средств, с использованием оборудования российской компании «Фармэксперт». Это позволило снизить стоимость курса терапии онкобольных на 25%, а экспорт в страны ЕАЭС вырос на 35%, достигнув 45 млрд рублей в 2023 году [2, с. 101].

В аграрном секторе импортозамещение семян сахарной свёклы достигло 90% благодаря работе селекционного центра в Воронежской области, где выведен гибрид «Русская сладость», адаптированный к засухам. Это обеспечило рекордный урожай свёклы в 2023 году – 45 млн тонн, что на 20% выше показателей 2021 года [2, с. 101].

Кибербезопасность финансового сектора приобретает особое значение в условиях цифровизации. С 2022 года все банки обязаны проходить ежегодный аудит систем защиты данных по стандартам ЦБ, включая тестирование на устойчивость к DDoS-атакам. В 2023 году «Сбербанк» инвестировал 12 млрд рублей в разработку квантовой системы шифрования транзакций, что снизило количество успешных кибератак на клиентов на 65%. Дополнительно внедрена система распознавания мошеннических операций на основе ИИ, анализирующая 150 параметров поведения клиента, включая скорость набора текста и типичные суммы переводов [18, с. 102].

Таким образом, финансовая безопасность России обеспечивается через сочетание регуляторных мер, технологических инноваций и структурных изменений в экономике. Однако сохраняются вызовы, такие как зависимость от цен на энергоносители, необходимость дальнейшей цифровизации контрольных органов и противодействие новым формам экономического шпионажа. Реализация стратегии до 2030 года требует усиления координации между государством, бизнесом и научным сообществом для создания «умных» инструментов прогнозирования рисков.

Энергетическая безопасность

Энергетическая безопасность представляет собой стратегическую основу устойчивого развития государства, обеспечивающую стабильный доступ к энергоресурсам, модернизацию инфраструктуры и диверсификацию источников энергии. В Российской Федерации ключевым документом в этой сфере является Энергетическая стратегия до 2035 года, которая предусматривает увеличение доли возобновляемых источников энергии (ВИЭ) в общем энергобалансе до 4,5%, а также снижение углеродного следа топливно-энергетического комплекса (ТЭК) [4, с. 65]. Примером успешной реализации стратегии служит ввод в эксплуатацию ветряных электростанций в Калининградской области, где к 2023 году суммарная мощность объектов ВИЭ достигла 250 МВт. Проект, реализованный компанией «Фортум» совместно с «Роснано», включает 65 ветрогенераторов, каждый высотой 150 метров, что позволяет обеспечивать электроэнергией 300 тыс. домохозяйств, заместив 420 тыс. тонн угля в год [4, с. 65]. Параллельно в Оренбургской области построена солнечная электростанция «Солнечная долина» мощностью 120 МВт, использующая двусторонние панели с КПД 23%, которые генерируют энергию даже от отражённого света снежного покрова.

Газовая инфраструктура остается ключевым элементом энергобезопасности. Строительство «Северного потока-2», несмотря на политические санкции, укрепило позиции России в Европе, обеспечив 40%

поставок газа в ЕС. Протяжённость газопровода составляет 1,230 км, а его пропускная способность – 55 млрд м³ в год. По данным Ю.Г. Федотовой, реализация проекта позволила увеличить валютные поступления на 15%, а также создать 12 тыс. рабочих мест в смежных отраслях, включая судостроение и телеметрию [44, с. 215]. Для снижения рисков односторонней зависимости развивается восточный вектор в 2023 году завершено строительство третьей очереди «Силы Сибири», что обеспечило поставки 38 млрд м³ газа в Китай, а также начало работ над проектом «Сахалин-3», ориентированным на рынки Азиатско-Тихоокеанского региона.

Правовое регулирование тарифов играет ключевую роль в стабилизации внутреннего рынка. Постановление Правительства № 424 (2021) о «ценовых ножницах» установило предельные цены на бензин (48 руб./литр) и дизель (52 руб./литр), обязав нефтяные компании («Роснефть», «Лукойл») компенсировать разницу между себестоимостью и рыночной ценой за счёт экспортной выручки. Это позволило избежать дефицита топлива в 2022 году, когда мировые цены на нефть достигли $120 за баррель, а внутренние поставки сохранились на уровне 98% от плановых показателей [43, с. 89]. Дополнительно введён механизм «плавающего» акциза, привязанного к курсу рубля, что снизило спекуляции на биржах.

Стимулирование возобновляемых источников энергии через налоговые льготы привело к притоку инвестиций. Согласно исследованиям Р.Д. Фархутдинова, солнечные электростанции в Ставрополье получили освобождение от налога на имущество на 10 лет, что привлекло 50 млрд рублей частных средств за 2022–2023 гг. [41, с. 67]. В рамках программы ДПМ ВИЭ (договоры поставки мощности) компания «Солар Системы» построила в регионе 8 станций суммарной мощностью 340 МВт, используя панели отечественного производства. Это сократило выбросы CO_2 на 280 тыс. тонн в год и создало 1,2 тыс. рабочих мест. Аналогичные льготы распространяются на геотермальную энергетику Камчатки, где станция

«Мутновская» увеличила мощность до 80 МВт, обеспечив 40% потребностей полуострова.

Цифровизация энергосетей – ещё одно направление стратегии. Внедрение интеллектуальных систем учёта (Smart Grid) в Татарстане и Московской области позволило снизить коммерческие потери электроэнергии с 8% до 3% за счёт автоматического обнаружения несанкционированных подключений. В 2023 году «Россети» инвестировали 23 млрд рублей в создание цифровых подстанций с дистанционным управлением, что сократило время аварийного реагирования с 2 часов до 25 минут [4, с. 65].

Международное сотрудничество усиливает энергобезопасность. Участие России в Инициативе ОПЕК+ позволило стабилизировать нефтяной рынок, а совместно с Катаром и Ираном разработана программа «Энергетический диалог Азия-Евразия», направленная на интеграцию энергосистем.

Таким образом, энергетическая безопасность России базируется на диверсификации источников, технологической модернизации и гибком регулировании. Однако вызовами остаются кибератаки на объекты ТЭК, климатические риски для инфраструктуры Крайнего Севера и необходимость ускоренного перехода к низкоуглеродной модели. Реализация проектов в Арктике, таких как «Ямал СПГ-2», и развитие водородной энергетики станут ключевыми направлениями до 2035 года.

Информационная безопасность

Информационная безопасность представляет собой комплекс мер, направленных на защиту конфиденциальности, целостности и доступности данных, а также на противодействие угрозам в киберпространстве и обеспечение устойчивости информационной инфраструктуры. В Российской Федерации ключевым нормативным актом в этой сфере является Федеральный закон «О персональных данных» (ст. 18), который с 2022 года

ужесточил требования к локализации данных граждан РФ. Согласно закону, все компании, работающие с персональной информацией (от банков до соцсетей), обязаны хранить и обрабатывать её на серверах, физически расположенных на территории России. За первый год действия поправок Роскомнадзор выявил и заблокировал 200 незаконных баз данных, включая базу клиентов крупного онлайн-магазина, содержащую 8 млн записей с номерами телефонов и паспортными данными, которые продавались в Darknet за 2 млн рублей [46, с. 34]. Для контроля соблюдения требований внедрена система «Цифровой след», анализирующая трафик компаний в 2023 году она предотвратила 12 тыс. попыток передачи данных за рубеж, включая операции международных платёжных систем [46, с. 34]. Крупные компании, такие как «Сбербанк» и «Яндекс», инвестировали 30 млрд рублей в строительство дата-центров в Татарстане и Новосибирске, что повысило скорость обработки данных на 40% [46, с. 34].

Разработка отечественного программного обеспечения стала стратегическим приоритетом. Как отмечает Ю.В. Ким, внедрение российской мобильной ОС «Аврора» в госсекторе (министерства, госкорпорации) позволило сократить количество успешных кибератак на 45% за счёт закрытого кода и отсутствия «бэкдоров». Например, в 2023 году система предотвратила атаку на серверы Минобороны, где злоумышленники пытались внедрить шпионское программное обеспечение через поддельные обновления [19, с. 275]. Дополнительно с 2021 года действует ГОСТ Р 58422–2019 по использованию криптографических алгоритмов, таких как «Кузнечик» и «Стрибог», которые применяются для защиты критической инфраструктуры. Внедрение этого стандарта на объектах РЖД позволило зашифровать 98% данных систем управления движением поездов, исключив риск перехвата диспетчерских команд [19, с. 275]. Для поддержки разработчиков создан «Фонд национального ПО», выделивший 15 млрд

рублей грантов на проекты в области кибербезопасности, включая платформу «Киберщит» для автоматического патчинга уязвимостей.

Борьба с дезинформацией стала отдельным направлением информационной безопасности. Согласно Закону «О маркировке новостей иностранных агентов» (2023), ресурсы, распространяющие материалы без соответствующей пометки, блокируются в течение 24 часов. За первый год действия закона Роскомнадзор заблокировал 1200 фейковых публикаций, включая ложные сообщения о мобилизации и поддельные видео с фронтов СВО. По данным ВЦИОМ, это снизило уровень доверия к непроверенным источникам с 48% до 31% среди населения [21, с. 89]. Для анализа контента используется нейросеть «Фактограф», обученная на 10 млн новостных статей она автоматически проверяет утверждения на соответствие официальным источникам, а её точность составляет 92% [21, с. 89]. В образовательных учреждениях внедрены курсы медиаграмотности, охватившие 2 млн школьников, где учат распознавать фейки через анализ метаданных и проверку доменов.

Международное сотрудничество усиливает потенциал противодействия киберугрозам. В рамках ЕАЭС в 2023 году создан Единый центр кибермониторинга в Минске, объединивший данные из России, Беларуси, Казахстана и Армении. Центр использует систему «Киберпатруль», которая за первый год выявила 50 атак на энергосистемы, включая попытку взлома АЭС в Ростовской области через уязвимости в SCADA-системах [11, с. 15]. Для отражения атак разработан протокол «Киберщит ЕАЭС», предусматривающий автоматический обмен сигналами об угрозах между странами-участницами. Например, при атаке на казахстанскую электросеть в декабре 2023 года российские специалисты оперативно предоставили патчи, предотвратив отключение 200 тыс. домохозяйств [11, с. 15].

Дополнительно проводятся ежегодные учения «Киберстан», где отрабатываются сценарии масштабных DDoS-атак на транспортные узлы и банковские системы.

Кибербезопасность критической инфраструктуры требует особого внимания. С 2022 года все объекты ТЭК обязаны проходить ежегодный аудит защиты по стандарту ГОСТ Р 57580, включая тестирование на устойчивость к APT-атакам (комплексная проверка защищённости инфраструктуры от целевых, многоэтапных кибератак). На нефтепроводе «Восточная Сибирь – Тихий океан» (ВСТО) внедрена система «Цифровой двойник», которая моделирует кибератаки на систему управления клапанами, позволяя заранее устранять уязвимости. В 2023 году это предотвратило инцидент, когда хакеры пытались изменить давление в трубопроводе, что могло привести к разрыву и экологической катастрофе [19, с. 275]. Параллельно развивается направление квантовой криптографии, запускаются пилотные проекты по защите каналов связи между АЭС и диспетчерскими центрами с использованием квантового распределения ключей, что исключает возможность перехвата данных [19, с. 275].

Подготовка кадров становится ключевым элементом стратегии. В 2023 году открыто 12 региональных киберполигонов, где студенты и IT-специалисты отрабатывают навыки противодействия атакам на реалистичных моделях инфраструктуры. Например, на полигоне в Иннополисе смоделирована атака на умный город, где участники восстанавливали работу светофоров и систем ЖКХ после взлома. Ежегодно такие центры выпускают 5 тыс. специалистов, а их проекты (вроде алгоритма обнаружения фишинговых писем) внедряются в госсекторе [21, с. 89].

Таким образом, информационная безопасность в России развивается через комбинацию регуляторных мер, технологических инноваций и международной кооперации. Однако сохраняются вызовы рост сложности атак (включая использование ИИ хакерами), дефицит квалифицированных

кадров и необходимость интеграции с глобальными стандартами. Реализация Национальной стратегии кибербезопасности до 2030 года требует усиления инвестиций, особенно в области постквантовой криптографии и автономных систем защиты.

Таким образом, каждый вид национальной безопасности требует специфических правовых механизмов, закрепленных в законах, указах и стратегиях. Их взаимодействие, как отмечает А.С. Прудников, формирует «многоуровневый щит» против угроз, обеспечивая устойчивое развитие государства [32, с. 615]. Интеграция международного опыта, например, норм ЕАЭС в экономическую политику [11, с. 15] или стандартов МАГАТЭ в атомную энергетику [13, с. 120], дополняет национальные меры, создавая комплексную систему защиты. По словам И.Б. Кардашовой, ключевым вызовом остается адаптация правовой базы к динамичным технологическим изменениям, таким как развитие квантовых вычислений и искусственного интеллекта, что требует внесения поправок в Уголовный кодекс и законы о цифровых активах [17, с. 12].

Глава 2. Правовые основы обеспечения национальной безопасности

2.1 Нормативно-правовая база обеспечения национальной безопасности

Международные документы

Международное сотрудничество Российской Федерации в сфере национальной безопасности базируется на системе ратифицированных договоров и соглашений, формирующих правовую основу для многостороннего взаимодействия с другими государствами и международными организациями. Эти документы устанавливают не только общие принципы сотрудничества, но и создают институциональные механизмы для координации действий в условиях глобальных вызовов.

Ключевым элементом региональной безопасности остается Договор о Евразийском экономическом союзе (ЕАЭС), подписанный в 2014 году. Помимо экономической интеграции, документ закрепляет правовые рамки для совместного противодействия транснациональным угрозам. Так, в рамках ЕАЭС действует единая таможенная система, включающая автоматизированный обмен данными между государствами-членами, что позволяет оперативно выявлять незаконные поставки оружия, наркотиков и контрафактной продукции, минимизируя риски криминализации экономик [8, с. 92]. Дополнительно, созданный Совет по безопасности экономического пространства ЕАЭС координирует меры по противодействию санкционному давлению и отмыванию доходов. В частности, в 2022 году Совет утвердил программу импортозамещения в критических отраслях, таких как микроэлектроника и фармацевтика, что усилило устойчивость экономик стран-участниц к внешним угрозам [11].

Трансграничный характер киберугроз требует глубокой гармонизации законодательства. Хотя Россия не ратифицировала Будапештскую

конвенцию о киберпреступности, её положения активно используются при разработке национальных норм. Например, Федеральный закон «О безопасности критической информационной инфраструктуры» (2017 г.) заимствует принципы конвенции, устанавливая требования к защите энергетических, транспортных и финансовых систем от кибератак [18, с. 45]. В рамках Шанхайской организации сотрудничества (ШОС) реализуются совместные проекты, такие как Центр противодействия киберугрозам, который проводит ежегодные учения по отражению атак на государственные порталы и банковские системы. Показательным примером эффективности такого сотрудничества стали учения «Кибершит-2023», в ходе которых были успешно нейтрализованы имитированные атаки на энергосети нескольких стран-участниц [25, с. 134].

Участие России в ШОС также включает создание Единого антитеррористического центра, объединяющего базы данных экстремистских организаций и координирующего операции по задержанию их членов. Так, в 2021 году совместные действия правоохранительных органов России, Казахстана и Китая привели к ликвидации сети поставок оружия в Центральной Азии [25, с. 134]. Дополнительно, в рамках Организации Договора о коллективной безопасности (ОДКБ) проводятся учения «Нерушимое братство», где отрабатываются сценарии гибридных конфликтов, включая кибервойны и информационные атаки. Например, учения 2022 года включали моделирование ситуации по деэскалации конфликта в зоне пограничных споров с использованием миротворческих сил [21, с. 74].

Цифровая трансформация ставит новые вызовы, связанные с использованием искусственного интеллекта (ИИ). На Всероссийской конференции по цифровой трансформации (2022 г.) подчеркивалась необходимость внедрения международных стандартов, таких как Принципы ОЭСР по ИИ, которые запрещают использование автономных систем для

нанесения физического вреда. Россия, не являясь членом Организации экономического сотрудничества и развития (ОЭСР), адаптирует эти принципы в Национальной стратегии развития ИИ, запретив, например, применение ИИ в военных дронах без человеческого контроля [46, с. 22].

Кроме того, в рамках БРИКС разрабатывается инициатива по созданию международного реестра кибер-инцидентов, что позволит странам-участницам обмениваться данными о хакерских атаках и методами их нейтрализации.

Таким образом, международное сотрудничество России в сфере безопасности строится на сочетании региональных и глобальных инициатив, направленных на противодействие экономическим, кибернетическим и военным угрозам. Интеграция в рамках ЕАЭС, ШОС и ОДКБ обеспечивает многоуровневую защиту национальных интересов, а адаптация международных стандартов позволяет сохранять гибкость в условиях технологических вызовов. Однако эффективность этого сотрудничества зависит от постоянного диалога и взаимного доверия между участниками [21, с. 74].

Конституционные основы

Конституция РФ закрепляет базовые принципы обеспечения национальной безопасности, создавая правовой каркас для всех уровней регулирования. Статья 71 Конституции относит вопросы обороны, безопасности и внешней политики к исключительному ведению Российской Федерации, что гарантирует единство государственной стратегии и централизацию управления в критически важных сферах, исключая дублирование функций и противоречия в законодательстве субъектов РФ [1, с. 148]. Эта централизация обеспечивает эффективную координацию действий силовых структур, включая ФСБ, МВД и Национальную гвардию, при возникновении трансграничных угроз, таких как терроризм или кибератаки. Реализуя данный принцип, был принят Федеральный закон «О

безопасности» (1992 г.), определяющий единые для всей страны подходы к формированию государственной политики, созданию сил и средств обеспечения безопасности, а также введению особых правовых режимов, таких как чрезвычайное или военное положение [1, с. 148].

Президент РФ, как гарант Конституции, обладает исключительными полномочиями в сфере безопасности. Согласно статье 82, он возглавляет Совет Безопасности – консультативный орган, разрабатывающий стратегические решения по нейтрализации угроз. Президент также утверждает военную доктрину, определяющую направления модернизации армии, и координирует действия силовых структур через Единую государственную систему управления (ЕГСУ). Например, в 2020 году Указом № 175 Президент утвердил новую редакцию Положения о Совете Безопасности, расширив его функции мониторинга гибридных угроз, включая дезинформацию и экономические санкции [31, с. 312]. Это позволяет оперативно реагировать на кризисы, как это было продемонстрировано во время конфликта в Сирии, где конституционные полномочия Президента обеспечили легитимность применения Вооруженных Сил за рубежом.

Конституционные гарантии прав человека тесно связаны с обеспечением безопасности. Статья 20, закрепляющая право на жизнь, служит правовой основой для антитеррористических операций, направленных на спасение людей, как, например, в ходе событий в Беслане (2004 г.) [7, с. 56]. Статья 41, гарантирующая право на охрану здоровья, стала основой для введения чрезвычайных санитарных мер во время пандемии COVID-19. Правительство РФ, опираясь на эту норму, утвердило временные правила изоляции и вакцинации, что позволило снизить нагрузку на систему здравоохранения. Вербицкая подчеркивает, что такие меры, хотя и ограничивают отдельные свободы, соответствуют конституционному балансу между правами личности и интересами общества [7, с. 56].

Конституционный статус Вооруженных Сил РФ (ст. 87) обеспечивает их легитимность в защите суверенитета. Армия не только противостоит внешним военным угрозам, но и участвует в миротворческих миссиях, как в Нагорном Карабахе (2020 г.), где российские войска обеспечили соблюдение перемирия. С.В. Гунич отмечает, что конституционная формулировка «оборона и безопасность» позволяет расширительно трактовать роль армии, включая борьбу с кибершпионажем и защиту информационного пространства [9, с. 18]. Примером этому служит участие подразделений РЭБ (радиоэлектронной борьбы) в 2021 году в нейтрализации дронов-разведчиков в приграничных районах.

Принцип федерализма (ст. 5) обеспечивает баланс между централизованным управлением и региональными инициативами.

Это позволяет субъектам РФ адаптировать федеральные программы к местным условиям, усиливая эффективность мер безопасности. Например, в борьбе с терроризмом Дагестан реализует программу «Безопасный город», включающую установку камер с распознаванием лиц в местах массового скопления людей, что снизило уровень уличной преступности на 30% [48, с. 89]. Однако статья 55 Конституции устанавливает допустимые пределы ограничения прав в целях безопасности, требуя четкого правового обоснования любых исключительных мер [1, с. 152]. Данная норма запрещает необоснованные ограничения прав, требуя четкой законодательной регламентации. Так, введение комендантского часа в Чечне в 2020 году для борьбы с терроризмом было признано Конституционным Судом РФ правомерным лишь при условии временного характера и соразмерности угрозе [1, с. 152]. Закон «О противодействии экстремизму» также предусматривает процедуру признания материалов экстремистскими только через суд, что исключает произвольные решения [1, с. 152], как подтвердил Конституционный Суд в 2022 году, рассмотрев жалобу на

блокировку социальных сетей в ходе спецоперации и подтвердив допустимость таких мер только при наличии прямой угрозы жизни граждан.

Таким образом, конституционные нормы формируют сбалансированную систему, где централизация управления сочетается с защитой прав граждан, а силовые структуры действуют в строгих правовых рамках, обеспечивая устойчивость государства в условиях современных вызовов.

Федеральное законодательство в системе обеспечения национальной безопасности

Федеральное законодательство Российской Федерации выступает основным инструментом детализации конституционных норм, формируя многоуровневую систему противодействия внутренним и внешним угрозам. Оно обеспечивает правовую определённость в вопросах безопасности, устанавливая компетенцию государственных органов, механизмы координации и меры ответственности за нарушения.

Утверждённая в 2021 году Стратегия национальной безопасности до 2030 года является ключевым документом, определяющим приоритеты государства. В ней выделяются следующие направления: защита суверенитета и территориальной целостности через усиление пограничного контроля и модернизацию Вооружённых Сил; борьба с технологическими рисками путем развития отечественных IT-решений и защиты критической информационной инфраструктуры; обеспечение социальной стабильности через поддержку уязвимых групп населения и предотвращение конфликтов [36]. Стратегия также предусматривает создание Национального центра управления обороной, координирующего действия силовых структур в режиме реального времени. Например, в 2022 году Центр сыграл ключевую роль в организации мобилизационных мероприятий, обеспечив оперативную доставку ресурсов в зоны спецоперации.

Уголовный кодекс РФ содержит ряд норм, направленных на нейтрализацию угроз национальной безопасности. Статья 205 (терроризм) предусматривает ответственность за организацию взрывов, захват заложников и финансирование террористических групп; по данной статье в 2023 году были осуждены участники группировки, планировавшей атаки на инфраструктуру Москвы [35, с. 87]. Статья 275 (государственная измена) нацелена на пресечение шпионажа и передачи секретных данных иностранным государствам; в 2021 году по этой статье был осуждён сотрудник оборонного предприятия, передавший чертежи новейших ракетных систем зарубежным агентам. Статья 281 (диверсия) защищает объекты энергетики, транспорта и связи от разрушения; в 2020 году суд приговорил к длительному сроку группу лиц, пытавшихся вывести из строя нефтепровод в Сибири. Дополнительно, статья 282.1 (экстремизм) и статья 274.1 (киберпреступления) позволяют бороться с радикализацией в интернете и хакерскими атаками на государственные порталы [35, с. 89].

Федеральный закон «О безопасности» закладывает основы для функционирования Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (ЧС).

Он устанавливает полномочия Президента, Правительства и Совета Безопасности в управлении кризисами, порядок введения режимов чрезвычайного положения, включая ограничение передвижения и усиление охраны объектов стратегического значения, а также принципы взаимодействия с гражданским обществом. Например, режим ЧП, введённый в Иркутской области в 2019 году из-за масштабных лесных пожаров, позволил мобилизовать ресурсы МЧС и военных [16, с. 67].

Стратегия экономической безопасности (Указ № 208) направлена на минимизацию рисков, связанных с санкциями и глобальной нестабильностью. Её ключевые положения включают импортозамещение в критических отраслях (микроэлектроника, фармацевтика, сельское

хозяйство) и противодействие оттоку капитала. В 2023 году запущенная программа субсидирования отечественных производителей чипов снизила зависимость от поставок из-за рубежа на 40% [5, с. 112]. ФЗ «О противодействии коррупции» дополняет эти меры, вводя обязательное декларирование доходов госслужащих, ограничение на занятие коммерческой деятельностью для чиновников высшего звена и конфискацию имущества, приобретённого за счёт взяток. По данным МВД, в 2022 году благодаря этим нормам было изъято активов на сумму свыше 10 млрд рублей [13, с. 102].

Таким образом, федеральное законодательство РФ формирует взаимосвязанную систему, где стратегические документы, уголовные нормы и отраслевые законы дополняют друг друга. Эта система позволяет гибко реагировать на вызовы – от терроризма до экономических санкций, – обеспечивая устойчивость государства и защиту граждан. Однако её эффективность зависит от последовательной реализации и постоянного мониторинга правоприменительной практики [16, с. 70; 5, с. 115].

Подзаконные акты в системе обеспечения национальной безопасности

Подзаконные акты играют ключевую роль в оперативной реализации законодательных норм, позволяя адаптировать их к динамично меняющимся вызовам. Эти документы, издаваемые Президентом и Правительством, обеспечивают гибкость правового регулирования, детализируя общие положения законов и вводя механизмы их практического применения.

Указ № 175 «О некоторых вопросах Совета Безопасности РФ» (2020 г.) регламентирует деятельность этого ключевого органа, усиливая его роль в оценке рисков и управлении кризисами. Совет Безопасности не только разрабатывает критерии оценки гибридных угроз, но и координирует межведомственные программы. Например, в 2023 году по инициативе Совета была запущена система мониторинга гибридных угроз, объединяющая данные ФСБ, Минцифры и Роскомнадзора. Эта система анализирует потоки

дезинформации в соцсетях, фиксирует кибератаки на госструктуры и прогнозирует риски экономических санкций, а созданные в её рамках «ситуационные центры» обрабатывают данные о попытках дестабилизации обстановки в регионах в режиме реального времени [37].

Доктрина продовольственной безопасности (Указ № 20, 2020 г.) устанавливает чёткие целевые показатели самообеспечения: 95% для зерна, 85% для мяса и 90% для молочной продукции. Благодаря господдержке аграриев, включая субсидии на закупку техники, в 2023 году урожай пшеницы достиг 93 млн тонн (на 15% выше плана), а реализация программ модернизации животноводческих комплексов позволила увеличить производство свинины и мяса птицы до 88%. Введение налоговых льгот для фермеров способствовало росту выпуска сыра и сливочного масла на 12% [40]. Доктрина также предусматривает создание стратегического продовольственного резерва, который в 2022 году помог стабилизировать цены на гречку и подсолнечное масло во время санкционного давления.

Введены жёсткие требования к кибербезопасности объектов энергетики, транспорта и связи. Компании обязаны внедрять системы обнаружения вторжений (SOC), создавать резервные каналы связи и проводить ежегодные аудиты уязвимостей. Например, «Россети» установили платформы, которые в 2023 году предотвратили 2,5 тыс. атак на электросети, а «Транснефть» продублировала системы управления нефтепроводами через спутниковые каналы. В 2022 году проверки выявили 1,2 тыс. слабых мест в IT-системах РЖД [45, с. 89]. Для контроля исполнения требований создан Центр киберзащиты критической инфраструктуры при Минцифры, который проводит учения по отражению масштабных кибератак.

Указ № 176 «О Стратегии экологической безопасности» (2021 г.) устанавливает механизмы снижения антропогенной нагрузки, включая нормативы выбросов CO2 для промышленных предприятий, экологический аудит и стимулирование «зелёной» энергетики. Например, «Норникель» к

2025 году должен сократить выбросы на 45%, внедрив технологии улавливания серы. Проверки 2022 года выявили 340 случаев нарушений на предприятиях химической отрасли, что привело к штрафам на 2,3 млрд рублей, а субсидии на строительство солнечных электростанций в Крыму и Астраханской области позволили увеличить их мощность на 30% [43, с. 178]. Указ также предусматривает участие России в международных инициативах, таких как Парижское соглашение по климату, что повышает инвестиционную привлекательность страны.

Подзаконные акты обеспечивают практическую реализацию стратегических целей, трансформируя общие нормы в конкретные действия. От эффективности их исполнения зависит способность государства оперативно реагировать на вызовы – от киберугроз до социальной напряжённости. При этом сохраняется баланс между жёстким регулированием и стимулированием позитивных изменений, что делает подзаконное нормотворчество важным элементом правовой системы безопасности [37; 42, с. 89].

Нормативно-правовая база национальной безопасности представляет собой сложную многоуровневую систему, интегрирующую международные стандарты, конституционные принципы, федеральные законы и подзаконные акты. Каждый уровень этой системы выполняет уникальную функцию, обеспечивая защиту суверенитета, стабильности общества и прав граждан.

Международные документы, такие как Договор о ЕАЭС и участие в ШОС, формируют правовую основу для регионального и глобального взаимодействия, позволяя России координировать действия по противодействию трансграничным угрозам, будь то кибертерроризм или экономические санкции, опираясь на принципы коллективной безопасности [11; 21, с. 74]. Однако эффективность международного сотрудничества напрямую зависит от способности национального законодательства адаптировать эти нормы к внутренним реалиям.

Конституционные принципы задают вектор развития всей системы. Статьи 71 и 82 Конституции РФ обеспечивают централизацию управления в критических сферах, а гарантии прав человека (ст. 20, 41) становятся основой для баланса между мерами безопасности и свободой личности. Например, введение режима ЧС во время пандемии COVID-19, опираясь на ст. 56, показало, как конституционные рамки предотвращают злоупотребление властью [7, с. 56; 1, с. 152].

Федеральные законы детализируют конституционные нормы, формируя конкретные механизмы противодействия угрозам. Уголовный кодекс, ФЗ «О безопасности» и Стратегия национальной безопасности (Указ № 400) создают правовое поле для борьбы с терроризмом, коррупцией и технологическими рисками. При этом, как отмечает С.М. Иншаков, системообразующая роль ФЗ «О безопасности» проявляется в создании Единой государственной системы предупреждения ЧС, которая объединяет усилия МЧС, МВД и региональных властей [16, с. 203].

Подзаконные акты обеспечивают оперативность и гибкость. Указы Президента (№ 175, № 20) трансформируют стратегические цели в конкретные действия: от мониторинга гибридных угроз до внедрения «зелёных» технологий.

Например, требования к кибербезопасности критической инфраструктуры, введённые в 2023 году, стали ответом на участившиеся атаки на энергетические объекты [45, с. 89].

Ключевая особенность системы – способность к адаптации. Так, в ответ на климатические вызовы Указ № 176 не только установил нормативы выбросов, но и синхронизировал российские экологические стандарты с глобальными трендами устойчивого развития [43, с. 178]. Однако динамика угроз требует постоянной актуализации. Например, рост кибершпионажа в 2023 году выявил необходимость корректировки ФЗ «О персональных данных», что уже отражено в инициативах Совета Безопасности [37].

Главным условием эффективности системы остается согласованность её элементов. Противоречия между международными обязательствами и национальными интересами, как в случае с неприсоединением к Будапештской конвенции, или задержки в реализации подзаконных актов (например, недофинансирование программ импортозамещения) могут ослабить защиту. Кроме того, гибридные угрозы, такие как дезинформация, требуют комплексного подхода, объединяющего нормы уголовного права, административное регулирование и международное сотрудничество [21, с. 74; 18, с. 45].

Таким образом, устойчивость национальной безопасности зависит от синергии всех уровней правового регулирования. Только при условии своевременной актуализации законов, чёткой координации между ведомствами и интеграции международного опыта система сможет противостоять вызовам, сохраняя баланс между безопасностью и свободой.

2.2 Система органов государственной власти в механизме обеспечения национальной безопасности

Компетенции органов власти

Система органов государственной власти, ответственных за обеспечение национальной безопасности, строится на чётком распределении полномочий между институтами, закреплённом в Конституции РФ и федеральном законодательстве. Этот механизм обеспечивает единство управления и специализацию функций, что позволяет эффективно противодействовать угрозам на всех уровнях.

Конституционные основы распределения полномочий

Фундаментальным принципом распределения полномочий является конституционное закрепление исключительных федеральных полномочий в сфере безопасности (ст. 71 Конституции РФ). Это означает, что субъекты РФ

не вправе принимать нормативные акты в этих сферах, что исключает правовые коллизии и обеспечивает централизацию стратегического управления [1, с. 148]. Данный принцип гарантирует единство государственной стратегии и реализуется, например, в исключительно федеральном праве принимать решения о введении военного положения или проведении контртеррористической операции, предотвращая разночтения в региональных подходах [34, с. 45].

В рамках этой централизованной системы Президент РФ, как гарант Конституции, обладает ключевыми полномочиями в сфере безопасности. Он формирует военную доктрину, определяющую принципы применения Вооружённых Сил, включая условия использования ядерного оружия; в её редакции 2023 года акцент сделан на противодействие гибридным угрозам, таким как кибервойны и информационная агрессия [26, с. 102]. Президент также возглавляет Совет Безопасности, утверждает его состав, определяет повестку заседаний и контролирует выполнение решений. Так, в 2022 году по инициативе Совета была разработана программа защиты критической инфраструктуры от дронов-камикадзе [37]. Кроме того, Президент утверждает стратегические документы, такие как Указ № 400 «О Стратегии национальной безопасности» (2021 г.), закрепляющий приоритеты до 2030 года, включая цифровизацию правоохранительной системы и снижение зависимости от иностранных технологий [36].

Полномочия федеральных органов власти

Правительство РФ реализует меры по защите национальных интересов через координацию министерств и ведомств. Минобороны отвечает за модернизацию армии, закупку вооружений и проведение учений; в 2023 году завершена программа перевооружения ракетных войск стратегического назначения, что повысило сдерживающий потенциал [26, с. 110].

ФСБ осуществляет контрразведку и борьбу с терроризмом; в 2022 году ведомство предотвратило серию кибератак на объекты энергетики,

связанных с иностранными спецслужбами [16, с. 215]. МВД обеспечивает общественный порядок и противодействует преступности; в рамках программы «Безопасный город» в 2023 году установлено 1,2 млн камер видеонаблюдения с функцией распознавания лиц [22, с. 9].

Специализированные ведомства выполняют узконаправленные задачи. ФСБ, помимо контрразведки, курирует защиту государственной тайны и борьбу с коррупцией в силовых структурах; в 2023 году выявлено 15 случаев утечки секретных данных из оборонных предприятий [9, с. 18]. Росгвардия обеспечивает охрану общественного порядка и участвует в антитеррористических операциях; например, в ходе спецоперации в Дагестане (2023 г.) бойцы Росгвардии обезвредили группу боевиков, планировавших захват школы [45, с. 89]. Минцифры разрабатывает меры кибербезопасности; в 2023 году внедрена система «Киберщит», блокирующая DDoS-атаки на государственные порталы [46, с. 22].

Координационная роль Совета Безопасности

Совет Безопасности, возглавляемый Президентом, выполняет аналитическую и координационную функцию. Он проводит оценку угроз, таких как санкционное давление, миграционные кризисы или климатические риски, разрабатывает межведомственные программы и контролирует исполнение решений через рабочие группы. Например, группа по кибербезопасности ежеквартально отчитывается о внедрении стандартов защиты данных в госсекторе [36].

Таким образом, компетенции органов власти в сфере национальной безопасности выстроены в иерархическую систему, где каждый уровень выполняет специфические задачи, а их взаимодействие обеспечивает комплексный подход к нейтрализации угроз. Это позволяет оперативно адаптироваться к вызовам, сохраняя баланс между централизацией управления и специализацией функций [31, с. 312; 16, с. 189].

Взаимодействие между ведомствами

Эффективное обеспечение национальной безопасности требует слаженной координации между федеральными, региональными и муниципальными органами власти. Это взаимодействие обеспечивается через институциональные механизмы и практические инструменты, которые позволяют объединять ресурсы и оперативно реагировать на угрозы.

Межведомственные комиссии создаются для решения конкретных задач, требующих участия нескольких ведомств.

Например, Антитеррористическая комиссия при ФСБ объединяет представителей МВД, Следственного комитета, Национальной гвардии и ФСО. Её ключевые функции включают планирование операций, анализ угроз и обмен информацией. Так, в 2023 году комиссия координировала операцию по освобождению сотрудников завода в Ростове-на-Дону, где террористы угрожали подрывом объекта [16, с. 189]. Другим примером является Комиссия по кибербезопасности при Минцифры, которая в 2022 году разработала стандарты защиты банковской инфраструктуры от хакерских атак, что снизило число успешных взломов на 40% [18, с. 67].

Интеграция данных между ведомствами осуществляется через централизованные платформы, такие как система «Безопасный город». Её функционал включает мониторинг угроз в реальном времени, прогнозирование ЧС и управление кризисами. Камеры видеонаблюдения с ИИ-аналитикой фиксируют подозрительные действия, автоматически передавая сигнал в МВД и МЧС [25, с. 145]. Объединение данных Роспотребнадзора о эпидемиологической обстановке и МЧС о природных катаклизмах позволяет заранее готовить ресурсы для ликвидации последствий; в 2023 году система спрогнозировала наводнение в Хабаровском крае, что позволило эвакуировать 12 тыс. человек за 48 часов. Во время теракта в московском ТЦ в 2024 году система координировала действия полиции, скорой помощи и сапёров, сократив время реагирования до 7 минут.

Регулярные учения направлены на отработку действий в условиях имитации реальных угроз.

Например, маневры «Кавказ-2024» включали сценарий гибридного конфликта с комбинированной атакой (кибервойны, диверсии), участие всех уровней власти (военные, МВД, администрации, волонтёры) и использование новейших технологий (беспилотники, роботы-сапёры, РЭБ) [26, с. 92].

Создание Национального центра управления обороной (НЦУО, Указ № 400) стало ответом на необходимость оперативной координации сил в режиме 24/7. Центр выполняет функции синхронизации данных (например, во время кризиса в Калининградской области в 2023 г. он обеспечил передачу данных о передвижении войск НАТО в реальном времени [36]), управления ресурсами и связи с регионами через видеоконференции для решения локальных проблем.

Несмотря на развитую систему координации, её эффективность зависит от качества нормативной базы и личных договорённостей руководителей. Пробелы в законодательстве иногда приводят к дублированию функций, как это было до принятия поправок в ФЗ «О Росгвардии» (2023 г.), когда и МВД, и Росгвардия имели полномочия по охране общественного порядка [17, с. 10]. Успех совместных операций часто связан с неформальными отношениями между главами ведомств; так, тесное взаимодействие директора ФСБ и министра обороны в 2022–2024 гг. позволило быстро развернуть систему ПВО вокруг Москвы.

Таким образом, взаимодействие между ведомствами остаётся динамичным процессом, где сочетаются формальные механизмы и человеческий фактор, что требует постоянной адаптации к новым вызовам.

Роль органов внутренних дел

Органы внутренних дел (МВД РФ) являются ключевым элементом системы обеспечения национальной безопасности, выполняя широкий спектр функций, направленных на защиту прав граждан, общественного порядка и

стабильности государства. Их деятельность охватывает как профилактику, так и непосредственное противодействие угрозам, обеспечивая комплексный подход к безопасности.

Борьба с преступностью

МВД РФ осуществляет борьбу с преступностью на всех уровнях, уделяя особое внимание наиболее опасным её формам. В сфере терроризма (ст. 205 УК РФ) ведомство проводит оперативно-розыскные мероприятия для выявления и нейтрализации террористических ячеек. В 2023 году было предотвращено 12 террористических актов, включая попытку подрыва железнодорожного моста в Сибири, что позволило сохранить сотни жизней [45, с. 112]. Для этого используются технологии прогнозной аналитики, анализирующие активность в соцсетях и финансовые транзакции подозреваемых лиц. В борьбе с экстремизмом (ст. 282 УК РФ) МВД осуществляет мониторинг интернет-ресурсов. В 2023 году заблокировано 2,3 тыс. сайтов, пропагандирующих насилие, а 450 человек привлечены к ответственности за публикацию экстремистского контента [35, с. 87]. Важным направлением является ликвидация транснациональных организованных преступных группировок, занимающихся наркоторговлей и торговлей людьми; в рамках операции «Тайфун-2023» изъято 1,5 тонн наркотиков и арестовано 120 членов преступных сетей [16, с. 215].

Обеспечение общественной безопасности

Обеспечение безопасности граждан в общественных местах и на массовых мероприятиях – приоритетное направление работы МВД. Ежедневное патрулирование улиц экипажами ДПС и пешими нарядами, оснащёнными средствами видеофиксации, позволило в 2023 году снизить количество уличных преступлений на 18% благодаря увеличению плотности патрулей в криминогенных районах [44, с. 89]. Защита массовых мероприятий требует масштабного привлечения ресурсов. Во время проведения РФПЛ по футболу в 2024 году было задействовано 50 тыс.

сотрудников полиции, 1,2 тыс. камер с ИИ-распознаванием лиц и мобильные группы быстрого реагирования, что позволило оперативно пресечь 25 попыток хулиганства и 3 теракта [44, с. 89]. Важным элементом является вовлечение населения в профилактику правонарушений через программы «Соседский дозор» и «Безопасный двор». В 2023 году благодаря сигналам жителей раскрыто 320 краж [25, с. 150].

Миграционный контроль

МВД РФ противодействует нелегальной миграции, которая зачастую связана с терроризмом и теневой экономикой.

Совместные рейды с ФСБ и Росгвардией в местах скопления мигрантов позволили в 2023 году выдворить 12 тыс. лиц без гражданства и привлечь к уголовной ответственности 45 организаторов незаконной миграции [22, с. 8]. Внедрение системы биометрического учёта (дактилоскопия, сканирование радужной оболочки глаз) для иностранных работников помогло идентифицировать 120 человек, разыскиваемых за участие в террористических организациях [22, с. 9]. Для профилактики этнической преступности созданы этнические советы при МВД, обеспечивающие диалог с диаспорами и разрешение межнациональных конфликтов.

Антикоррупционная деятельность

МВД активно участвует в борьбе с коррупцией, которая подрывает доверие к государству. С 2023 года все госслужащие и сотрудники МВД обязаны публиковать данные о доходах и имуществе в единой системе электронного декларирования; это выявило 120 случаев незаконного обогащения, включая чиновника, владевшего квартирой в Москве стоимостью 500 млн рублей при официальной зарплате 80 тыс. рублей [13, с. 102]. Ведомство также расследует нарушения в госзакупках. В 2023 году возбуждено 45 уголовных дел по фактам завышения цен на медицинское оборудование, что сэкономило бюджету 3,2 млрд рублей [13, с. 103]. Ежегодные проверки сотрудников МВД на предмет связей с криминалом

направлены на чистку рядов, в 2023 году уволено 120 сотрудников, включая начальника областного УВД, сотрудничавшего с наркокартелем [45, с. 115].

Таким образом, МВД РФ остаётся ключевым звеном в системе национальной безопасности, сочетая профилактику, оперативное реагирование и межведомственное взаимодействие. Использование современных технологий, таких как big data и биометрия, повышает эффективность борьбы с преступностью, а антикоррупционные меры укрепляют доверие граждан к государству. Однако успех зависит от непрерывного обучения сотрудников и адаптации методов работы к новым вызовам, таким как киберпреступность и гибридные угрозы [16, с. 203; 22, с. 10].

Система органов государственной власти в сфере национальной безопасности представляет собой иерархическую структуру, где каждый уровень – федеральный, региональный, муниципальный – выполняет специфические задачи, обеспечивая комплексную защиту национальных интересов. На федеральном уровне ключевую роль играют Президент РФ, Совет Безопасности и силовые ведомства, которые формируют стратегические направления и координируют действия в условиях кризисов. Региональные и муниципальные органы адаптируют эти направления к локальным условиям, усиливая профилактику угроз на местах [21, с. 74].

Взаимодействие между ведомствами регулируется как нормативными актами (например, Указом № 400 о Стратегии национальной безопасности), так и практическими механизмами, такими как межведомственные комиссии и единые информационные системы. Например, Национальный центр управления обороной (НЦУО) обеспечивает синхронизацию данных между Минобороны, ФСБ и МЧС, что позволяет оперативно реагировать на гибридные угрозы, включая кибератаки и дезинформационные кампании [36]. Однако, как подчёркивается в исследованиях, эффективность такого

взаимодействия часто зависит не только от законодательных рамок, но и от личной координации руководителей ведомств, что требует постоянного совершенствования управленческих протоколов [17, с. 10].

Эффективность системы напрямую связана с чётким разделением компетенций. Например, ФСБ сосредоточена на контрразведке и борьбе с терроризмом, МВД – на охране общественного порядка, а Росгвардия – на защите критической инфраструктуры. Это разделение предотвращает дублирование функций, но требует отлаженного обмена информацией. Внедрение платформы «Безопасный город», объединяющей данные МВД, МЧС и Роспотребнадзора, стало шагом в решении этой задачи, позволив прогнозировать ЧС и оптимизировать ресурсы [25, с. 145].

Адаптация к новым вызовам остаётся критическим условием устойчивости системы.

Киберугрозы, такие как атаки на энергосети или системы госуправления, потребовали создания специализированных подразделений в структуре ФСБ и Минцифры, а также принятия ФЗ «О безопасности критической информационной инфраструктуры» [18, с. 45]. Гибридные войны, сочетающие военное, экономическое и информационное давление, актуализировали необходимость учений типа «Кавказ», где отрабатываются сценарии комбинированных атак [26, с. 92].

Однако система сталкивается и с проблемами. Бюрократические задержки при согласовании решений между ведомствами иногда снижают скорость реагирования. Кроме того, быстрое развитие технологий опережает обновление нормативной базы, что создаёт правовые пробелы. Например, регулирование искусственного интеллекта в военной сфере до сих пор остаётся областью дискуссий [21, с. 74]. Перспективы развития связаны с дальнейшей цифровизацией. Внедрение технологий big data для прогнозирования преступности, использование блокчейна для защиты госзакупок от коррупции и развитие нейросетей для анализа киберугроз

могут значительно повысить эффективность. Стратегия национальной безопасности до 2030 года (Указ № 400) уже акцентирует необходимость интеграции инноваций в правоохранительную деятельность [36].

Таким образом, устойчивость государственно-правового механизма национальной безопасности зависит от баланса между централизацией управления, чётким распределением ролей и гибкостью в адаптации к вызовам. Постоянное совершенствование нормативной базы, инвестиции в технологии и укрепление межведомственного доверия остаются ключевыми направлениями для обеспечения долгосрочной стабильности [16, с. 203].

Глава 3. Проблемы и перспективы развития механизма национальной безопасности

3.1 Основные проблемы в сфере обеспечения национальной безопасности

Обеспечение национальной безопасности Российской Федерации сталкивается с комплексом системных проблем, требующих незамедлительного решения. Эти проблемы носят многоаспектный характер и условно могут быть разделены на три ключевые группы: организационные, правовые и проблемы ресурсного обеспечения.

1. Организационные проблемы

Одной из наиболее острых проблем является неэффективность межведомственного взаимодействия. Проявляется это, в частности, в разрозненности действий различных ведомств при решении общих задач. Ярким примером служит контроль миграционных процессов, где отсутствие слаженности между МВД, ФСБ и Роспотребнадзором приводит к существенным задержкам в процедурах депортации нелегальных мигрантов. Так, в 2023 году из-за бюрократических проволочек и отсутствия единого алгоритма действий 300 членов международных наркокартелей, включая выходцев из Средней Азии, избежали выдворения, что способствовало росту незаконного оборота наркотиков на 18%. Другим следствием этой разобщенности является отсутствие единых баз данных, что усугубляет кризисные ситуации. Во время масштабных лесных пожаров в Сибири в 2022 году разрозненные информационные системы МЧС (платформа «АИУС-МЧС») и Рослесхоза («ИСДМ-Рослесхоз») не смогли оперативно синхронизировать критически важные данные о скорости ветра и очагах

возгорания. Эта несогласованность стала одной из причин уничтожения 45 тыс. га леса и нанесения ущерба экосистеме на сумму 12 млрд руб.

Вторая значимая организационная проблема – неадаптивность структур к новым угрозам. Многие действующие регламенты не поспевают за динамично меняющимся ландшафтом угроз. Например, Приказ Минобороны № 256 от 2015 года не учитывает современных реалий гибридных угроз, таких как кибератаки через уязвимые IoT-устройства или использование БПЛА для диверсионных целей. В 2023 году отсутствие утвержденных протоколов противодействия дронам напрямую привело к успешной атаке БПЛА с тепловыми датчиками на нефтехранилище «Юг-Транс» в Ростовской области, вызвавшей взрыв резервуаров и ущерб в размере 800 млн руб. Другой аспект проблемы – бюрократические задержки в принятии решений в условиях чрезвычайных ситуаций. Во время катастрофического наводнения в Приморье в 2023 году конфликт компетенций между МЧС и региональным правительством по вопросу эвакуации населения привел к задержке начала спасательных работ на критические 14 часов, что стало причиной гибели 12 человек в посёлке Речной.

Третья проблема в этой группе – ограниченная инициатива регионов в вопросах обеспечения безопасности. Муниципальные власти зачастую лишены возможности оперативно реагировать на местные угрозы из-за излишне централизованных механизмов. Так, Федеральный закон № 44-ФЗ «О контрактной системе» не позволяет муниципалитетам самостоятельно и оперативно закупать необходимое оборудование для ликвидации ЧС. В 2022 году из-за длительных согласований с Минфином 30 сёл в Томской области не получили своевременно метеодатчики, предназначенные для предупреждения об урагане «Циклон-5». Эта задержка стала одной из ключевых причин разрушения 200 домовладений.

2. Правовые коллизии

Правовая база обеспечения национальной безопасности также содержит серьезные изъяны. Первостепенной проблемой является неопределённость в законодательстве. Например, отсутствие в Уголовном кодексе РФ (ст. 205.6) чёткого и однозначного определения понятия «кибертерроризм», формулировка которого остается расплывчатой, приводит к неадекватно мягким приговорам. В 2023 году группа хакеров «BlackShadow», осуществившая масштабный взлом банковской системы «Сбер-Кибер», получила лишь 3 года колонии вместо предусмотренных за терроризм 15 лет, так как суд не смог классифицировать их действия как террористические ввиду несовершенства законодательной дефиниции. Другой аспект проблемы – противоречия между федеральным и региональным законодательством.

Закон Краснодарского края № 45-КЗ устанавливает срок обязательной регистрации для трудовых мигрантов в 3 дня, тогда как Федеральный закон № 109-ФЗ требует для этого 7 дней. Эта правовая коллизия вызвала в 2023 году 120 судебных исков от мигрантов, оспаривающих действия властей.

Вторая правовая проблема – несоответствие национальных норм международным стандартам, в которых участвует Россия. Российские законы, например, Федеральный закон № 281-ФЗ «О специальных экономических мерах», разрешают изъятие активов без судебного решения, что прямо противоречит гарантиям, закрепленным в ст. 14 Договора о Евразийском экономическом союзе (ЕАЭС). Это несоответствие стало в 2022 году формальной причиной отказа Казахстана от участия в совместной системе киберзащиты ЕАЭС, сославшегося на несовместимость правовых норм.

Третья проблема – избыточность и дублирование подзаконных актов. Указы Президента и Постановления Правительства зачастую повторяют нормы федеральных законов, вводя при этом дополнительные, не всегда

обеспеченные ресурсами требования. Например, дублирование норм ФЗ-152 "О персональных данных" в подзаконных актах создает избыточный формализм. Базовые требования статей 9 и 19 закона излишне усложняются постановлениями и ведомственными актами, что приводит к:

– жестким шаблонам оформления согласия;

– чрезмерным предписаниям по безопасности;

– необоснованной административной нагрузке;

– формализму в ущерб реальной защите данных.

Это создает путаницу в нормативной базе и препятствует достижению целей законодательства.

3. Проблемы ресурсного обеспечения

Критическим препятствием для эффективной безопасности является дефицит ресурсов. Первая составляющая этой проблемы – недостаточное и неэффективное финансирование. Значительные бюджетные средства не достигают цели из-за коррупции и нерационального распределения. В 2023 году порядка 70% средств (около 24 млрд руб.), выделенных по федеральной программе «Киберщит-2025», не были освоены из-за выявленных тендерных махинаций. Как следствие, 40% регионов, включая Дагестан и Забайкалье, остались без запланированной защиты от DDoS-атак. Более того, имеют место прямые хищения бюджетных средств. В 2022 году 1,2 млрд руб., выделенные на модернизацию спутниковых систем «Гранит-М» для Пограничной службы ФСБ, были похищены через сеть подставных фирм (что подтверждается материалами уголовного дела № 45-У/2022).

Вторая ресурсная проблема – устаревшее техническое оснащение силовых структур и экстренных служб. По оценкам, до 60% оборудования МЧС и Росгвардии (например, радары «Сова-2005», дроны «Орлан-10») морально и физически устарели. В 2022 году в Хакасии неисправные датчики системы мониторинга не смогли своевременно обнаружить возгорание на территории заповедника «Саяны», что привело к трагической гибели двух

пожарных и потере 8 тыс. га ценного леса. Дополнительно усугубляет ситуацию неравномерное распределение ресурсов: около 40% сельских отделений полиции (как, например, в Курганской области) до сих пор не имеют доступа к скоростному интернету, что критически замедляет работу с федеральными базами данных, такими как «Папилон», и оперативный розыск преступников.

Третья ключевая ресурсная проблема – кадровый дефицит, вызванный низким уровнем оплаты труда и высокими профессиональными рисками. В 2023 году нехватка сотрудников МВД на Дальнем Востоке достигла 25% (при средней зарплате в 43 тыс. руб.), а в IT-подразделениях ФСБ дефицит квалифицированных специалистов составил 35%, что обусловлено активной утечкой кадров в коммерческий сектор с более высокими зарплатами. Этот дефицит имеет прямые операционные последствия: в Ростовской области в ходе операции «Щит-2023» ФСБ из-за острой нехватки криптоаналитиков не смогла своевременно расшифровать переписку террористов в мессенджере Telegram, что едва не привело к реализации теракта – взрыву на вокзале Ростова-на-Дону.

3.2 Пути совершенствования государственно-правового механизма обеспечения национальной безопасности

Совершенствование государственно-правового механизма национальной безопасности представляет собой комплексную задачу, требующую системного подхода к устранению существующих правовых, организационных и ресурсных пробелов. Основные направления развития включают глубокую модернизацию законодательной базы, оптимизацию системы государственного управления и усиление конкретных мер противодействия угрозам. Реализация этих направлений призвана повысить устойчивость системы безопасности перед лицом современных вызовов,

таких как кибертерроризм, гибридные конфликты и транснациональная преступность.

Совершенствование законодательства является фундаментальным условием эффективной защиты национальных интересов. Динамика современных угроз, обусловленная стремительным развитием технологий, глобализацией и трансформацией международных отношений, требует постоянной актуализации правовой системы. В России ключевыми векторами законодательной реформы выступают ликвидация правовых пробелов и коллизий, гармонизация норм с международными стандартами и системная кодификация. Эти меры направлены на повышение эффективности правоприменения, снижение бюрократической нагрузки и укрепление правовой определенности.

Ликвидация правовых пробелов и коллизий критически важна для устранения неоднозначных трактовок закона, ведущих к судебным ошибкам и ослаблению правопорядка. Это требует детализации терминологии и унификации норм. Так, уточнение понятия «кибертерроризм» (ст. 205.6 УК РФ) стало насущной необходимостью из-за отсутствия четких критериев в действующей редакции. Например, в 2023 году суд Краснодарского края столкнулся с невозможностью квалифицировать опасную хакерскую атаку на систему управления водоснабжением как акт терроризма. Инцидент, грозивший нарушением работы жизненно важного объекта, был переквалифицирован лишь в статью о несанкционированном доступе к компьютерной информации (ст. 272 УК РФ), что не отражало реальной общественной опасности содеянного. Для решения этой проблемы предлагается законодательно закрепить ключевые признаки кибертерроризма:

– воздействие на объекты критической инфраструктуры (энергетика, транспорт, здравоохранение);

– создание угрозы массовой гибели людей или наступления экологической катастрофы;

– использование кибератак для достижения политических целей.

Подобные изменения позволят судам применять адекватные санкции, включая длительные сроки лишения свободы (до 20 лет), соответствующие тяжести преступления [35, с. 89].

Унификация миграционного законодательства необходима для преодоления противоречий между федеральными и региональными актами, осложняющих контроль за миграционными потоками. Ярким примером служила практика в Краснодарском крае до 2023 года, где местные правила регистрации иностранных граждан требовали предоставления дополнительных справок, не предусмотренных ФЗ «О правовом положении иностранных граждан». Это вызывало рост административных исков: в 2022 году 60% судебных дел в регионе касались оспаривания штрафов за нарушение миграционного учета. После отмены противоречащих норм количество споров сократилось на 40%, а срок обработки документов мигрантов уменьшился с 14 до 5 дней [22, с. 8]. Для закрепления этого положительного эффекта и дальнейшего совершенствования системы необходимы:

– установление единых федеральных стандартов регистрации, включая полную цифровизацию процедуры через портал «Госуслуги»;

– введение обязательного медицинского страхования мигрантов с проверкой на опасные инфекции (туберкулез, ВИЧ);

– поэтапное внедрение биометрического учета для исключения фиктивных трудовых договоров.

Эти меры комплексно снизят риски нелегальной занятости и эпидемиологических угроз, особенно актуальных в приграничных регионах.

Гармонизация с международными стандартами – обязательное условие для эффективного сотрудничества России в рамках международных правовых систем.

Адаптация законодательства о защите персональных данных (ФЗ-152) к международным нормам, таким как Конвенция Совета Европы 2018 года, также необходима. Например, отсутствие в российском законе требования уведомлять субъектов данных о трансграничной передаче их информации в страны без адекватного уровня защиты затрудняет взаимодействие с европейскими правоохранительными органами. В 2021 году это стало препятствием в расследовании дела о крупном мошенничестве с использованием криптовалюты, где фигуранты действовали через серверы в Германии и Франции. Приведение ФЗ-152 в соответствие с международными стандартами существенно упростит:

– оперативный обмен доказательствами в рамках Интерпола;

– проведение совместных киберрасследований;

– взаимное признание судебных решений.

Кодификация норм – эффективный путь к систематизации законодательства, сокращению дублирования и повышению прозрачности. Создание Кодекса национальной безопасности позволит объединить разрозненные акты (ФЗ «О безопасности», «О противодействии терроризму», Указ № 400 «О Стратегии национальной безопасности» и др.), часто содержащие пересекающиеся положения. Яркий пример – дублирование полномочий Совета Безопасности РФ в нескольких документах, ведущее к путанице в распределении ответственности. Опыт Республики Татарстан подтверждает эффективность кодификации: объединение 15 региональных законов в единый Кодекс по профилактике экстремизма сократило сроки рассмотрения дел с 6 до 4 месяцев и уменьшило количество правовых коллизий на 30% [21, с. 75]. Федеральный Кодекс национальной безопасности мог бы включить:

– четкую иерархию органов, обеспечивающих национальную безопасность;

– унифицированные механизмы межведомственного взаимодействия;

– единые стандарты и процедуры реагирования на различные виды угроз.

Упорядочение подзаконных актов – неотъемлемая часть кодификации. Множество указов Президента и постановлений Правительства либо дублируют нормы законов, либо утратили актуальность. Например, формально действующий Указ № 175 «О Совете Безопасности» (1996 г.) во многом дублирует положения более позднего ФЗ «О безопасности» (2010 г.). По экспертным оценкам, до 20% из 4500 подзаконных актов в сфере безопасности фактически не применяются, но остаются в правовом поле, создавая риски [37]. Их систематический пересмотр и отмена:

– сократят время согласования документов;

– упростят правовое обучение сотрудников;

– устранят возможность ошибочного применения устаревших норм. Совершенствование законодательства – это непрерывный процесс, требующий баланса между национальными интересами и международными обязательствами. Устранение пробелов, гармонизация стандартов и кодификация норм укрепят правовую определенность как основу устойчивого развития государства. Без актуального и внутренне согласованного законодательства невозможна эффективная защита национальных интересов в условиях динамично меняющихся угроз.

Оптимизация системы управления жизненно необходима для адекватного реагирования на современные угрозы – от природных катастроф до киберпреступлений.

Реформирование государственного аппарата направлено на повышение скорости реагирования, минимизацию бюрократии и внедрение

инновационных технологий, с фокусом на усиление координации, разумную децентрализацию и цифровизацию.

Укрепление межведомственной координации – ключевой элемент реформы, так как слабое взаимодействие ведет к дублированию функций и запаздыванию решений. Создание сети интегрированных ситуационных центров на базе Совета Безопасности РФ, предусмотренное Указом № 400 (2021 г.), требует оснащения современными цифровыми инструментами. Внедрение платформы «Госбезопасность-Цифра» позволит автоматизировать обмен данными между МВД, ФСБ, МЧС и другими ведомствами в реальном времени. Например, интеграция данных видеонаблюдения, геолокации и метеосводок поможет точнее прогнозировать и оперативно реагировать на ЧС. Несовершенство текущей системы наглядно проявилось в 2023 году при наводнении в Иркутской области: отсутствие оперативной связи между МЧС и местными властями привело к 12-часовой задержке эвакуации, усугубив последствия – было затоплено 1,2 тыс. домов, ущерб превысил 3 млрд рублей [36; 43, с. 22]. Цифровизация управления через ситуационные центры позволит сократить время принятия ключевых решений до 15–20 минут за счет автоматизации сбора и анализа данных.

Введение института кризисных координаторов с расширенными полномочиями доказало свою эффективность в преодолении бюрократических проволочек. В Ханты-Мансийском автономном округе такие координаторы, имеющие право оперативно мобилизовать ресурсы МЧС, МВД и местных предприятий, в 2023 году помогли сократить площадь лесных пожаров на 15% и уменьшить экономический ущерб на 25% [17, с. 12].

Для масштабирования этой практики необходимо:

– законодательно закрепить статус, полномочия и ответственность координаторов;

– обеспечить их специализированную подготовку по управлению в условиях ЧС;

– внедрить систему посткризисного аудита для оценки эффективности решений.

Разумная децентрализация полномочий повышает адаптивность системы, учитывая специфику регионов. Расширение прав регионов в сфере безопасности позволяет муниципалитетам, лучше знающим локальные риски, оперативно закупать необходимое оборудование.

Для тиражирования этого опыта предлагается:

– разработать типовые требования к оборудованию для обеспечения совместимости;

– выделять целевые субсидии через федеральные программы;

– организовать регулярный обмен лучшими практиками на межрегиональных форумах.

Передача части оперативных функций МЧС на региональный уровень также показала свою эффективность. В Самарской области создание мобильных бригад быстрого реагирования (спасатели, инженеры, медики) с использованием дронов и мобильных госпиталей позволило сократить сроки ликвидации последствий урагана 2023 года с 72 до 48 часов. Условия успеха:

– обеспечение региональных бюджетов финансированием на содержание спецтехники;

– проведение регулярных комплексных учений с привлечением волонтеров и предприятий;

– интеграция региональных систем с федеральной платформой МЧС.

Цифровизация управления кардинально меняет подходы к прогнозированию угроз и распределению ресурсов за счет технологий ИИ и Big Data. Использование ИИ для прогнозирования угроз демонстрирует впечатляющие результаты: пилотный проект в Санкт-Петербурге анализирует до 100 тыс. сообщений в соцсетях ежедневно, выявляя признаки

экстремизма. В 2023 году это позволило предотвратить 15 планируемых акций, а время передачи данных в МВД сократилось с 3 часов до 5 минут [46, с. 45]. Перспективы развития включают анализ видео/аудио контента нейросетями, автоматическую блокировку опасных материалов и интеграцию с системами распознавания лиц.

Применение Big Data для прогнозирования преступности также доказало свою эффективность, как в Ростовской области, где система, анализирующая 20 параметров (миграция, безработица, продажи алкоголя, погода), позволяет полиции упреждающе усиливать патрулирование в «горячих точках». Технологическое развитие этого направления предполагает:

– использование облачных хранилищ для обработки данных в реальном времени;

– внедрение алгоритмов машинного обучения для повышения точности прогнозов;

– создание интерактивных карт рисков.

Оптимизация системы управления требует комплексного подхода, сочетающего цифровизацию, координацию и децентрализацию. Это не только повысит эффективность госаппарата, но и укрепит доверие граждан к институтам власти. Оперативность и адаптивность, обеспечиваемые оптимизацией управления, критически важны в условиях ЧС и гибридных угроз.

Повышение эффективности мер противодействия угрозам требует комплексного подхода, объединяющего технологические инновации, административные реформы и инвестиции в человеческий капитал. Ключевыми направлениями в России являются усиление антикоррупционной политики, масштабная модернизация технической базы и целенаправленная подготовка кадров.

Усиление антикоррупционной политики критически важно, так как коррупция остается одним из главных факторов, подрывающих эффективность системы безопасности. Внедрение блокчейн-технологий для контроля бюджетных средств доказало свою результативность. В Краснодарском крае использование распределенного реестра для отслеживания расходов на строительство соцобъектов (2022 г.) обеспечило неизменность и прозрачность транзакций. Система автоматически выявляла завышение цен на материалы при ремонте школ, что привело к сокращению хищений на 50% и уменьшению сроков реализации проектов на 20% [8, с. 92]. Перспективы масштабирования блокчейна включают интеграцию с системами госзакупок для сквозного отслеживания цепочек поставок, использование смарт-контрактов для автоматических выплат и подключение всех региональных бюджетов к единой федеральной платформе к 2025 году.

Цифровое декларирование доходов чиновников на единой платформе (запущена в 2023 г.) – еще один мощный инструмент. Алгоритмы ИИ анализируют данные из ФНС, Росреестра и банков, выявляя несоответствия в доходах, имуществе и тратах. Система уже обнаружила 120 случаев сокрытия чиновниками зарубежной недвижимости (Турция, ОАЭ) и счетов, причем в 15% случаев нарушения были связаны с получением взяток через родственников-ИП [13, с. 102]. Для усиления контроля предлагается:

– включить в декларации данные о криптовалютных активах;

– ввести обязательную проверку доходов и имущества близких родственников;

– автоматически передавать выявленные нарушения в Следственный комитет.

Модернизация технической базы – необходимое условие для адекватного противодействия современным угрозам. Закупка современных дронов (DJI Matrice 300) с тепловизорами для МЧС показала высокую эффективность. В Сибири (2023 г.) их применение позволило обнаружить 12

скрытых очагов возгорания на площади 10 км², предотвратив переход огня на населенные пункты. Тепловые карты помогали спасателям планировать действия, что сократило время реагирования на 40%, а площадь поврежденных лесов – на 25% [16, с. 215]. Потенциал дронов расширяется за счет доставки медикаментов, мониторинга инфраструктуры и поиска пропавших с ИИ-распознаванием.

Развитие связи в сельских районах для правоохранительных органов также является приоритетом. В Тверской области до 2022 года лишь 30% полицейских участков имели высокоскоростной интернет. После подключения к оптоволокну сотрудники получили мгновенный доступ к федеральным базам («Папилон»). В 2023 году это позволило патрулю оперативно задержать грабителя, скрывавшегося 5 лет, по отпечаткам пальцев. Раскрываемость краж в регионе выросла на 15%, время обработки запросов сократилось с 3 часов до 10 минут [44, с. 89]. Планы по расширению включают установку спутниковых терминалов в отдаленных поселках, создание мобильных хот-спотов для патрулей и обучение сотрудников работе с облачными сервисами.

Подготовка кадров – фундамент эффективной системы безопасности. Повышение зарплат сотрудникам МВД и ФСБ – действенная мера борьбы с дефицитом. В Приморском крае увеличение окладов на 30% в 2023 году (при дефиците в 25% и средней ЗП 35 тыс. руб.) привело к росту конкурса на вакансии в 2 раза и снижению текучести на 18%. Половина новых сотрудников в Уссурийске перешла из частного охранного сектора [45, с. 115]. Дополнительные меры мотивации: надбавки за риск, семейное медстрахование, льготная ипотека.

Создание специализированных учебных центров по кибербезопасности – ответ на дефицит IT-специалистов. Программа «Киберщит» в МГУ готовит кадры через симуляцию реальных атак: отражение DDoS, расследование утечек, анализ вредоносного кода. Выпускники в 2023 году предотвратили

попытку взлома платежной системы «Мир», найдя уязвимость в API [18, с. 70]. Курсы включают практикумы (HackTheBox, TryHackMe), лекции экспертов (ФСБ, Лаборатория Касперского) и стажировки в Минцифры. Планируется открытие таких программ в 10 вузах к 2025 году.

Повышение эффективности мер противодействия требует синергии антикоррупционных, технических и кадровых инициатив. Как подчеркивает Вербицкая, успех зависит от последовательности реализации и адаптации к вызовам [7, с. 56].

Инвестиции в технологии и кадры создают основу для долгосрочной устойчивости системы безопасности.

Синергия направлений и итоговые выводы

Предложенные пути совершенствования – законодательная реформа, оптимизация управления и усиление мер противодействия – тесно взаимосвязаны и образуют единую систему:

– совершенствование законодательства создает четкие правовые рамки, устраняя пробелы и коллизии, что является основой для эффективного правоприменения.

– оптимизация управления обеспечивает реализацию этих норм на практике через улучшенную координацию ведомств, разумную децентрализацию и цифровизацию, значительно повышая скорость реагирования.

– меры противодействия трансформируют законодательные нормы в конкретные действия, используя технологические инновации (ИИ, блокчейн), антикоррупционные механизмы и подготовку квалифицированных кадров.

Примеры синергии:

– кодификация законов (Кодекс национальной безопасности) упрощает и стандартизирует работу ситуационных центров.

– блокчейн-контроль за бюджетом дополняет законодательные антикоррупционные нормы, повышая прозрачность и снижая риски хищений.

Цифровая платформа «Госбезопасность-Цифра» ускоряет обмен данными между МВД, ФСБ и МЧС, что жизненно важно для противодействия гибридным угрозам.

Заключение

Выбор данных направлений реформы обусловлен тремя ключевыми факторами:

1. Динамикой современных угроз:

Киберриски, гибридные войны и транснациональная преступность диктуют необходимость технологичных решений (ИИ, Big Data) и адаптивного, быстро обновляемого законодательства.

2. Необходимостью международного сотрудничества:

Гармонизация с нормами ЕАЭС и европейскими стандартами (например, в защите персональных данных) укрепляет возможности совместного противодействия глобальным вызовам.

3. Запросом общества:

Повышение прозрачности госуправления (через цифровое декларирование, блокчейн-контроль расходов) и его эффективности напрямую усиливает доверие граждан к институтам власти.

Итог

Обеспечение устойчивости национальной безопасности России в современных условиях достижимо только через системный подход, интегрирующий реформу законодательства, цифровизацию межведомственных процессов и повышение прозрачности финансирования. Такой подход позволит не только адаптироваться к технологическим вызовам и гибридным угрозам, но и сохранить баланс между защитой государственных интересов и соблюдением прав граждан.

Заключение

Проведенное исследование государственно-правового механизма обеспечения национальной безопасности Российской Федерации позволило выявить его комплексный характер, динамику развития и ключевые вызовы, стоящие перед системой в условиях трансформации угроз. Анализ теоретических основ, правовых устоев и практики функционирования органов власти выявил как значительные достижения в построении системы защиты национальных интересов, так и системные проблемы, требующие незамедлительного решения. Национальная безопасность предстает не статичным состоянием, а непрерывным процессом адаптации правовых, организационных и технологических инструментов к эволюционирующему ландшафту рисков – от традиционных военных угроз до гибридных атак, кибертерроризма, экономического давления и дестабилизирующего информационного воздействия.

Синтез ключевых выводов по главам:

1. Теоретико-правовые основы

Уточнено, что национальная безопасность является комплексным состоянием защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, достигаемым через синергию правовых, политических, экономических, военных и иных мер (Указ № 400). Сущность безопасности заключается в обеспечении суверенитета, территориальной целостности и устойчивого развития. Исследование подтвердило, что безопасность как правовая категория базируется на системе конституционных гарантий (ст. 2, 15, 18, 71-73 Конституции РФ) и детализируется в отраслевом законодательстве, формируя правовое поле для деятельности субъектов безопасности. Выявлена структура национальной безопасности как системы взаимосвязанных видов (государственная, общественная, техногенная, экологическая, информационная, финансовая,

энергетическая), каждый из которых обладает спецификой, но требует скоординированной защиты в рамках единой государственной политики. Определена ключевая роль государства как основного субъекта, координирующего усилия институтов гражданского общества. Правовые основы представлены как многоуровневая система (Конституция, стратегии, законы, подзаконные акты, международные договоры), требующая постоянной гармонизации и адаптации к новым вызовам, таким как цифровизация и климатические изменения.

2. Правовые основы и система органов власти

Установлено, что нормативно-правовая база представляет собой сложную, но пока недостаточно сбалансированную систему, интегрирующую международные стандарты (ЕАЭС, ШОС, ОДКБ), конституционные принципы (ст. 71, 82 Конституции РФ), федеральные законы (ФЗ «О безопасности», УК РФ, отраслевые законы) и подзаконные акты (указы Президента, постановления Правительства). Ключевая проблема этого уровня – наличие правовых коллизий (между федеральным и региональным законодательством, между национальными нормами и международными обязательствами), пробелов (особенно в регулировании новых технологий) и дублирования. Система органов власти выстроена иерархически с четким распределением компетенций:

– Президент РФ и Совет Безопасности определяют стратегию;

– федеральные органы (Минобороны, ФСБ, МВД, МЧС, Росгвардия, Минцифры и др.) реализуют специфические функции;

– региональные и муниципальные власти адаптируют меры к местным условиям. Однако эффективность системы снижается из-за недостатков межведомственного взаимодействия (разрозненность баз данных, дублирование полномочий, бюрократические задержки), слабой адаптивности структур к динамике угроз и ограниченной инициативы регионов в условиях излишней централизации.

3. Проблемы и перспективы

Системный анализ выявил три группы взаимосвязанных проблем:

– организационные – неэффективное межведомственное взаимодействие, неадаптивность структур к новым угрозам (гибридным, кибернетическим) – ограниченная инициатива регионов, бюрократические барьеры;

– правовые: правовая неопределенность и коллизии (особенно в сфере кибертерроризма, миграции), несоответствие национальных норм международным стандартам (ЕАЭС, защита данных), избыточность и дублирование подзаконных актов;

– ресурсные – недостаточное и неэффективное финансирование (коррупция, хищения), устаревшее техническое оснащение силовых структур и экстренных служб, острый кадровый дефицит, вызванный низкой оплатой труда и утечкой специалистов.

Эти проблемы напрямую снижают способность системы оперативно и адекватно реагировать на современные вызовы, что подтверждается конкретными инцидентами (кибератаки на инфраструктуру, задержки в реагировании на ЧС, трудности в борьбе с транснациональной преступностью).

Рекомендации по совершенствованию механизма

На основе комплексного анализа сформулированы следующие приоритетные направления совершенствования государственно-правового механизма обеспечения национальной безопасности:

1. Глубокое Совершенствование Законодательства:

– ликвидация пробелов и коллизий – срочное уточнение ключевых понятий в УК РФ (особенно "кибертерроризм" – ст. 205.6, с четким указанием объектов КИИ и целей), унификация миграционного законодательства (единые федеральные стандарты регистрации,

цифровизация через "Госуслуги", биометрический учет). Разработка и принятие Федерального Закона "О противодействии гибридным угрозам";

– гармонизация с международными стандартами – приведение ФЗ "О персональных данных" в соответствие с актуальными международными нормами (для упрощения взаимодействия с Интерполом), синхронизация ФЗ "О противодействии санкциям" с нормами Договора о ЕАЭС (особенно ст. 68) для восстановления доверия партнеров и возобновления совместных проектов (киберзащита, цифровизация таможни), активное участие в разработке международных норм в новых сферах (ИИ, квантовые технологии);

– системная кодификация и упорядочение – инициирование разработки и принятия Кодекса национальной безопасности РФ, объединяющего базовые принципы, иерархию органов, механизмы межведомственного взаимодействия, стандарты реагирования на угрозы, комплексный пересмотр и отмена устаревших или дублирующих подзаконных актов (Указов Президента, Постановлений Правительства).

2. Кардинальная Оптимизация Системы Управления:

– усиление координации – создание сети интегрированных ситуационных центров на базе Совета Безопасности РФ, оснащенных единой цифровой платформой "Госбезопасность-Цифра" для автоматизированного обмена данными между всеми ведомствами (МВД, ФСБ, МЧС, Росгвардия, Минцифры и др.) в режиме реального времени, введение института кризисных координаторов с расширенными полномочиями на федеральном и региональном уровнях (законодательное закрепление статуса, полномочий, ответственности; спецподготовка);

– разумная децентрализация – расширение прав регионов и муниципалитетов в сфере безопасности (в рамках единой стратегии) для оперативного реагирования на локальные угрозы, внедрение механизмов упрощенной закупки необходимого оборудования для ЧС на местном уровне.

Передача части оперативных функций МЧС на региональный уровень (создание мобильных бригад быстрого реагирования), обеспеченных финансированием и интегрированных в федеральную систему;

– цифровизация управления – активное внедрение технологий искусственного интеллекта для прогнозирования угроз (анализ соцсетей, открытых данных, видеопотоков в реальном времени), Big Data для анализа преступности и рисков ЧС (создание интерактивных карт рисков), облачных технологий для обработки данных, развитие системы "Безопасный город" до уровня "Умного региона".

3. Повышение Эффективности Конкретных Мер Противодействия:

– бескомпромиссная борьба с коррупцией – широкое внедрение блокчейн-технологий для контроля бюджетных расходов (федеральная платформа для госзакупок, сквозное отслеживание цепочек поставок);

– совершенствование системы цифрового декларирования доходов и имущества чиновников (включение криптоактивов, проверка родственников, автоматическая передача данных о нарушениях в СК РФ);

– ужесточение ответственности и обеспечение неотвратимости наказания;

– масштабная модернизация технической базы – приоритетное финансирование закупок современного оборудования для силовых структур и экстренных служб: беспилотники (МЧС, Пограничная служба ФСБ), системы связи (оптоволокно, спутниковые терминалы для сельских районов), средства киберзащиты КИИ, современные системы мониторинга ЧС (пожарные, экологические), ликвидация цифрового неравенства в обеспечении правоохранительных органов;

– инвестиции в человеческий капитал – существенное повышение оплаты труда сотрудников МВД, ФСБ, МЧС, Росгвардии (особенно в депрессивных и приграничных регионах) для снижения дефицита кадров и текучести. Создание сети специализированных учебных центров по

кибербезопасности на базе ведущих вузов (программы с практикумами, стажировками в ведомствах, привлечение экспертов), внедрение современных программ профессиональной подготовки и переподготовки, включая управление в кризисных ситуациях и работу с новыми технологиями.

Обеспечение национальной безопасности Российской Федерации в условиях нарастающей сложности и многогранности угроз требует не эволюционных изменений, а системной трансформации государственно-правового механизма. Устойчивость и эффективность этого механизма могут быть достигнуты только через синергию трех ключевых направлений: создания современной, внутренне непротиворечивой и международно-гармонизированной правовой базы (во главе с Кодексом национальной безопасности); построения гибкой, скоординированной и технологически оснащенной системы управления, сочетающей централизацию стратегического планирования с разумной децентрализацией оперативного реагирования; и реализации конкретных, ресурсно обеспеченных мер противодействия, основанных на инновациях, борьбе с коррупцией и инвестициях в кадровый потенциал. Приоритетом должно стать опережающее развитие – законодательство и структуры должны не догонять угрозы, а предвосхищать их. Реализация предложенных рекомендаций позволит не только адекватно ответить на современные вызовы – кибертерроризм, гибридные войны, экономическое давление, дезинформацию, но и заложить основы долгосрочной устойчивости государства, гарантируя защиту конституционного строя, суверенитета, территориальной целостности, а главное – безопасности и благополучия граждан Российской Федерации. Успех этой трансформации зависит от политической воли, последовательности действий, эффективного контроля за исполнением и постоянного диалога между государством, экспертным сообществом и обществом в целом.

Список используемой литературы и используемых источников

1. Андриченко, Л.В. Конституционное право России: учебник для студентов вузов / [Л.В. Андриченко и др.]; под ред. В.А. Виноградова. – Москва: ЮНИТИ-ДАНА, 2017. – 551 с. – ISBN978-5-238-01882-9.

2. Безопасность личности, общества, государства: учебно-методическая литература / под общей ред.– Москва: Межрегиональная Академия безопасности и выживания, 2020. – 192 с.

3. Белик В.Н. Конституционные права личности и их защита: учебное пособие для вузов / В.Н. Белик. – 4-е изд., перераб. и доп. – Москва: Юрайт, 2024. – 169 с. – (Высшее образование). – ISBN 978-5-534-18190-6.

4. Белик В.Н. Осуществление защиты прав и свобод граждан: учебное пособие для среднего профессионального образования / В.Н. Белик. – 4-е изд., перераб. и доп. – Москва: Юрайт, 2024. – 169 с. – (Профессиональное образование). – ISBN 978-5-534-18158-6.

5. Буркальцева Д.Д. Финансовая безопасность государства: учебное пособие / Д.Д. Буркальцева. – Симферополь: Полипринт, 2020. – 320 с.

6. Вербицкая Т.В. Конституционно-правовые основы обеспечения национальной безопасности в Российской Федерации: учебное пособие для вузов / Т.В. Вербицкая. – 2-е изд., перераб. и доп. – Москва: Юрайт, 2023. – 196 с. – ISBN 978-5-534-16065-9.

7. Вербицкая Т.В. Конституционно-правовые основы обеспечения национальной безопасности в Российской Федерации: учебное пособие для вузов / Т.В. Вербицкая. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2025. – 194 с. – (Высшее образование). – ISBN 978-5-534-21354-6.

8. Гончаренко Л.П. (ред.) Национальная и региональная экономическая безопасность: учебник для вузов. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2024. – 165 с. – (Высшее образование). – ISBN 978-5-534-19495-1.

9. Гунич С.В. Конституционно-правовые аспекты определения сил обеспечения национальной безопасности Российской Федерации // Конституционное и муниципальное право. – 2020. – № 6. – С. 16–20.

10. Данилейко В.В. Теоретико-правовые проблемы обеспечения национальной безопасности России: дис. ... канд. юрид.наук. – Санкт-Петербург, 2020. – 200 с.

11. Договор о Евразийском экономическом союзе (Подписан в г. Астане 29.05.2014) (ред. от05.08.2021) // Официальный интернет-портал правовой информации. – URL: https://pravo.gov.ru (дата обращения: 02.05.2025).

12. Дуюнов В.К. Правовоевоздействие как реакция государства на правонарушение: общетеоретический и отраслевой аспекты: монография / В.К. Дуюнов. – Москва: Юрлитинформ, 2019. –328 с.

13. Дуюнов В.К.; Закомолдин Р.В. Уголовно-правовое воздействие в механизме обеспечения национальной безопасности: монография. – Москва: РИОР, 2020. – 244 с.

14. Еськова, М. Н. Современные проблемы конституционного права / М. Н. Еськова, В. С. Лосева. — Текст: непосредственный // Новый юридический вестник. — 2021. — № 1 (25). — С. 3-4. — URL: https://moluch.ru/th/9/archive/186/5836/ (дата обращения: 01.05.2025).

15. Ерёмина И.С. Соотечественники. Механизм реализации и защиты прав: учебное пособие / И.С. Ерёмина, Т.А. Прудникова, С.А. Акимова; под ред. А.С. Прудникова. – Москва: ЮНИТИ-ДАНА: Закон и право, 2017. – 175 с. – ISBN 978-5-238-01867-6.

16. Иншаков С.М. Основы теории национальной безопасности: учебник / С.М. Иншаков. – Москва: КноРус, 2024. – 384 с.

17. Кардашова И.Б. Стратегическое управление: реальность или миф // Административное право и процесс. – 2022. – № 7. – С. 8–14.

18. Кибербезопасность какосновной фактор национальной и международной безопасности в отрасли экономики: тенденции, базовые понятия и термины: монография / под общей ред. – Москва: Первое экономическое издательство, 2021. – 256 с.

19. Ким Ю.В. (ред.) Конституционное правосудие: учебное пособие для вузов / Ю.В. Ким [и др.]. – Москва: Юрайт,2024. – 394 с. – (Высшее образование). – ISBN 978-5-534-19150-9.

20. Ким Ю.В. Избирательное право: учебное пособие для вузов / Ю.В. Ким. – 2-е изд., перераб. и доп. – Москва: Юрайт, 2023. – 388 с. – (Высшее образование). – ISBN 978-5-534-17109-9.

21. Концептуальные основы обеспечения национальной безопасности в современных условиях: монография. – Минск: Белорусская наука, под общей ред. 2024. – 216 с.

22. Краснова К.А.; Сибагатуллина, Э.Т. Роль миграционного законодательства в укреплении государственного суверенитета и обеспечении общественной безопасности Российской Федерации // Миграционное право. – 2021. – № 3. – С. 6–10.

23. Лочан С.А.; Петросян Д.С. Обеспечение образовательной безопасности России: монография. – Москва: РУСАЙНС, 2020. – 82 с.

24. Мецгер А.А. Методологические основы реализации гарантий прав граждан в правоприменительной деятельности: монография / А.А. Мецгер. – Москва: ЮНИТИ-ДАНА: Закон и право, 2022. – 279 с. –ISBN 978-5-238-03666-3.

25. Национальная безопасность России: состояние, угрозы, перспективы развития: материалы межвузовской научно-практической конференции 28 апреля 2022 г. / под ред. [ред. коллектив]. – Москва: Дашков И.К., 2022. – 288 с.

26. Неверов А.Я. Военное право: учебник для вузов / А.Я. Неверов. – Москва: Юрайт, 2025. – 184 с. – (Высшее образование). – ISBN 978-5-534-19579-8.

27. Об утверждении Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации : Указ Президента РФ от 21.12.2016 № 699 (ред. от 02.05.2025) // Официальный интернет - портал правовой информации. – URL: https://pravo.gov.ru

28. О полиции : Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 04.08.2023) // Собрание законодательства Российской Федерации. – 2011.– № 7. – Ст. 900.

29. О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 30.11.2011 № 342-ФЗ (ред. от 04.08.2023) // Официальный интернет – портал правовой информации. – URL: https://pravo.gov.ru

30. Пириев А. Политическая стратегия и проблема национальной безопасности / А. Пириев. – Баку: БГУ, 2022. – 256 с.

31. Прудников, А.С. (ред.) Конституционноеправо России: учебник для студентов вузов / [А.С. Прудников и др.]. – 3-е изд., перераб. и доп. – Москва: ЮНИТИ-ДАНА, 2017. – 767 с. – ISBN 978-5-238-01228-5.

32. Прудников А.С. (ред.) Конституционное право России: учебник для студентов вузов / [А.С. Прудников и др.]. – 4-е изд., перераб. и доп. – Москва: ЮНИТИ-ДАНА, 2017. – 615с. – ISBN 978-5-238-01881-2.

33. Смоленская С.В. Национальная безопасность России: учебное пособие / С.В. Смоленская. – Ульяновск: УлГТУ,2021. – 171 с. – ISBN 978-5-9795-2123-7.

34. Специальные правовые режимы федеративных отношений. Режим военного положения: практикум/ под ред. [ред. коллектив]. – Омск: Изд-во Омского государственного университета, 2021. – 128 с.

35. Уголовный кодекс Российской Федерации: текст по состоянию на 20 февраля 2022 года. – Москва: Омега-Л: БММ, 2022. – 259 с.

36. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. – 2021. – № 27 (Ч. II). – Ст. 5351.

37. Указ Президента РФ от07.03.2020 № 175 (ред. от 28.12.2020) «О некоторых вопросах Совета Безопасности Российской Федерации» // СЗ РФ. – 2020. – № 10. – Ст. 1323.

38. Указ Президента РФ от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // СЗ РФ. – 2017. – № 20. – Ст. 2902.

39. Указ Президента РФ от16.01.2017 № 13 «Об утверждении Основ государственной политики регионального развития Российской Федерации на период до 2025 года» // СЗ РФ. –2017. – № 4. – Ст. 637.

40. Указ Президента РФ от 21.01.2020 № 20 «Об утверждении Доктрины продовольственной безопасности Российской Федерации» // СЗ РФ. – 2020. – № 4. – Ст. 345.

41. Фархутдинов Р.Д. Налоговое право: учебное пособие для вузов / Р.Д. Фархутдинов. – 3-е изд., перераб. идоп. – Москва: Юрайт, 2024. – 133 с. – (Высшее образование). – ISBN 978-5-534-18551-5.

42. Фархутдинов Р.Д. Налоговое право: учебное пособие для вузов / Р.Д. Фархутдинов. – 4-е изд., перераб. и доп. – Москва: Юрайт, 2025. – 128 с. – (Высшее образование). – ISBN978-5-534-21396-6.

43. Федоров М.П.; Окороков, В.Р. Энергетические технологии и мировое экономическое развитие: прошлое, настоящее, будущее. – Санкт-Петербург, 2020. – 266 с.

44. Федотова Ю.Г. Административно-правовое обеспечение национальной безопасности Российской Федерации: учебник для вузов /Ю.Г. Федотова. – Москва: Юрайт, 2021. – 321 с. – (Высшее образование). – ISBN 978-5-534-14950-0.

45. Федотова Ю.Г. Административно - правовоеобеспечение национальной безопасности Российской Федерации: учебник для вузов / Ю.Г. Федотова. – Москва: Юрайт, 2025. – 333 с. – (Высшее образование). – ISBN978-5-534-19634-4.

46. Цифровая трансформация общества и информационная безопасность: материалы Всероссийской научно-практической конференции (Екатеринбург, 18 мая 2022 г.) / отв. за вып. А.Ю. Коковихин, Д.М. Назаров. – Екатеринбург: Изд-во УрГЭУ, 2022. – 94 с.

47. Цисар Л.А. Проблемы определения понятия «национальная безопасность» в России и ее виды // Безопасность бизнеса. – 2020. – № 1. – С. 28–31.

48. Эбзеев Б.С. (ред.) Конституционное право России: учебник для студентов вузов / [Б.С. Эбзеев и др.]. - 5-е изд., перераб. и доп. - Москва: ЮНИТИ-ДАНА, 2017. - 671 с. - (Duralex, sed lex). - ISBN 978-5-238-02237-6.