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

Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

40.05.01 Правовое обеспечение национальной безопасности
(код и наименование направления подготовки /специальности)

Государственно-правовая
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему «Правовая защита российского общества от деструктивно-информационно-психологического воздействия как национальный интерес РФ»

Обучающийся Г.Н. Валиев
(Инициалы Фамилия) (личная подпись)

Руководитель канд. юрид. наук, К.П. Федякин
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Аннотация

Современное общество сегодня переживает глубокую трансформацию, вызванную стремительным технологическим прогрессом. Эти изменения ввели новые механизмы распространения информации и психологического воздействия, которые нарушают традиционные каналы коммуникации и изменяют коллективное сознание.

Инновационные технологии и экспериментальные подходы переопределяют способ создания и потребления информации. Как новые стратегии, так и усовершенствованные традиционные методы находятся в активной разработке. Цифровые платформы, включая социальные сети и приложения для обмена мгновенными сообщениями, позволяют людям создавать и делиться контентом в любое время и из любого места. Хотя эта эволюция улучшает коммуникацию, она также создает возможности для целенаправленной манипуляции общественным мнением с помощью курируемых постов и видео.

Цель выпускной квалификационной работы направлена на детальный анализ деструктивного информационно-психологического воздействия, его воздействия на общество в Российской Федерации, а также на изучение соответствующей законодательной базы как на отечественном, так и на общедоступном уровне.

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

Оглавление

Введение

Современное общество сегодня переживает глубокую трансформацию, вызванную стремительным технологическим прогрессом. Эти изменения ввели новые механизмы распространения информации и психологического воздействия, которые нарушают традиционные каналы коммуникации и изменяют коллективное сознание.

Инновационные технологии и экспериментальные подходы переопределяют способ создания и потребления информации. Как новые стратегии, так и усовершенствованные традиционные методы находятся в активной разработке. Цифровые платформы, включая социальные сети и приложения для обмена мгновенными сообщениями, позволяют людям создавать и делиться контентом в любое время и из любого места. Хотя эта эволюция улучшает коммуникацию, она также создает возможности для целенаправленной манипуляции общественным мнением с помощью курируемых постов и видео.

Критической проблемой в этом меняющемся ландшафте является отсутствие надежной правовой базы для управления деструктивной информацией и психологическим влиянием. Действующее законодательство часто неадекватно, что позволило экстремистским, преступным и антиобщественным группам процветать в сети. Присущая цифровому пространству анонимность еще больше усложняет ситуацию, поскольку оно часто используется для распространения призывов и сообщений, которые ставят под угрозу общественную стабильность. Эта проблема усугубляется законами, которые не поспевают за быстрым технологическим прогрессом.

Рост искусственного интеллекта добавляет еще один уровень сложности в дискуссию. Уже достигнув значительных успехов в области ИТ, ИИ вскоре может быть использован в качестве инструмента для вредоносного влияния или даже приобретать юридическую личность в определенных контекстах.

Дискуссия о замене человеческих ролей роботизированными системами набирает обороты, особенно по мере того, как автоматизированные технологии все чаще используются в медицине, безопасности и промышленных операциях. Заглядывая вперед, можно сказать, что существует вероятность того, что роботы могут превратиться в независимые субъекты с далеко идущим социальным воздействием, и все это при отсутствии всеобъемлющей правовой структуры для управления такими разработками.

Объектом ВКР является правовая защита российского общества от деструктивного информационно-психологического воздействия в системе национальной безопасности Российской Федерации.

Предметом ВКР является нормативно-правовые механизмы, стратегии и инструменты обеспечения информационно-психологической безопасности в Российской Федерации, направленные на защиту общества от деструктивного окружающего мира в условиях современного информационного угрозы.

Цель ВКР направлена на детальный анализ деструктивного информационно-психологического воздействия, его воздействия на общество в Российской Федерации, а также на изучение соответствующей законодательной базы как на отечественном, так и на общедоступном уровне.

Для поставленной цели необходимо решить ряд совместных задач:

- проанализировать сущность и выявить ключевые признаки деструктивного информационно-психологического воздействия как социального и правового явления;
- классифицировать методы и средства осуществления деструктивного информационно-психологического воздействия, определить их особенности и механизмы воздействия на массовое и индивидуальное сознание;
- изучить международно-правовые подходы и стандарты, направленные на защиту от негативного информационно-психологического влияния,

а также проанализировать возможность их адаптации в российском правовом поле;

- определить правовые основы обеспечения информационно-психологической безопасности в Российской Федерации, выявить принципы, лежащие в их основе;
- рассмотреть деструктивное информационно-психологическое воздействие как общенациональную угрозу, проанализировать его масштабы и последствия в российском обществе;
- исследовать действующие правовые механизмы защиты граждан от деструктивного информационно-психологического воздействия и выявить пробелы в их правовом регулировании;
- оценить последствия деструктивного информационно-психологического воздействия на население;
- изучить состояние и проблемы развития институциональных систем, обеспечивающих информационно-психологическую безопасность, а также предложить направления их совершенствования;
- разработать стратегические приоритеты совершенствования законодательства РФ, направленного на противодействие деструктивному информационно-психологическому воздействию.

Настоящая научная работа опирается на интегративный подход, предусматривающий объединение положений и методологических основ таких дисциплин, как правоведение, психология, политология, теория коммуникации и журналистика. Для комплексного осмысления исследуемых процессов задействован широкий арсенал методов: от универсальных научных процедур (включая логический анализ, метод аналогии, индуктивные и дедуктивные построения, абстрагирование, структурное сопоставление) до специализированных инструментов, среди которых формально-юридический анализ, методы эмпирико-социологического и статистического характера, а также элементы структурно-функционального подхода.

Нормативно-правовая основа проводимого исследования сформирована на базе ключевых нормативных правовых источников, образующих структуру современной правовой системы Российской Федерации. Прежде всего, это положения Конституции Российской Федерации, обладающие высшей юридической силой и определяющие основы правового регулирования в стране. Существенную роль играют федеральные законы, международные договоры, ратифицированные Российской Федерацией, а также подзаконные акты, включая указы Президента РФ, постановления Правительства РФ, нормативные правовые акты министерств и ведомств, принятые в пределах их компетенции.

Теоретико-методологическую платформу исследования составляют обоснованные научные подходы, отражённые в работах признанных специалистов в области юриспруденции, правоведения и смежных дисциплин. Среди них особо следует отметить вклад таких авторов, как В.А. Баришполец, Г.В. Грачев, И.К. Мельник, В.В. Латынов, С.И. Макаренко, А.Ю. Касюк, Е.Н. Пашенцев, И.В. Смирнов, Е.П. Безносюк. Их научные разработки внесли весомый вклад в становление понятийного аппарата и концептуальных подходов, используемых в ходе настоящего анализа.

Научная и практическая значимость рассматриваемого труда во многом обусловлена тем, что он сочетает юридическую интерпретацию с результатами прикладных социологических исследований и наблюдений, что позволяет не только оценить применимость действующих правовых норм, но и выявить реальные особенности их реализации в условиях стремительного развития цифровых технологий и глобальной трансформации общественно-правовых отношений.

Структура исследования включает введение, три содержательные главы, заключительную часть и перечень нормативных и научных источников. Данный формат способствует последовательному изложению проблематики и обеспечивает системное восприятие раскрываемых положений.

Глава 1 Основные аспекты деструктивного информационно-психологического воздействия

1.1 Сущность и особенности деструктивного информационно-психологического воздействия

Обзор научной литературы и законодательных документов Российской Федерации выявляет присущую ему неоднозначность в определении понятия деструктивного информационно-психологического воздействия. В то время как во многих исследованиях рассматривается более широкий спектр информационно-психологического воздействия, включающий как позитивные, так и негативные эффекты, деструктивный вариант рассматривается лишь как одна из граней более обширного явления. Таким образом, комплексное понимание начинается с рассмотрения общего понятия и двух его основных компонентов: объекта и субъекта воздействия.

В.А. Баришполец дает основополагающее определение информационно-психологического воздействия как «информационного, психотропного или психофизического воздействия на психику человека, влияющего на восприятие действительности, поведенческие функции, а в некоторых случаях и на функционирование органов и систем организма» [1]. Эта точка зрения отражена в работе С.И. Макаренко «Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах XXI века» [31]. Обе точки зрения подчеркивают, что основным объектом такого воздействия является личность, чье психологическое и физическое состояние подвержено различным формам манипуляции. «Убеждение представляет собой метод воздействия, основанный на систематическом использовании как логических, так и эмоциональных аргументов. Она включает в себя создание аргументированного информационного поля, способного не только донести до конкретных определённых фактов, но и вызвать устойчивый эмоциональный отклик,

который приводит к установлению установленных условий и поведению» [69]. С.И. Макаренко выполняет эту картину, отмечая: «Комплексное использование аргументации и эмоциональной экспрессии формируется для уверенности в источнике воздействия. При этом важнейшую роль играет не только содержательная, но и форма подачи информации, которая способна активировать подсознательные механизмы восприятия» [31]. Эти отрывки подчёркивают, что эффективность убеждения зависит от синергии между рациональным доводом и эмоциональным воздействием.

В работе В. А. Баришполеца приводит фундаментальное определение информационно-психологического воздействия, которое обосновывает совокупность информационных, психотропных и психофизических элементов, влияющих на восприятие поведения и личности. Как он пишет:«Информационно-психологическое воздействие представляет собой сложный комплекс, в который включены не только чистота сигналов, но и эмоционально-окрашенные стимулы, способные модифицировать нейрофизиологические состояния и, в соответствии с рекомендациями, изменять поведенческие установки человека. Данный процесс относится к прямым коммуникационным каналам, а также к более сложным механизмам подсознательного общества, что делает его многоуровневым и динамичным» [1].

В академических дискуссиях индивид рассматривается в двух различных ролях. Как личность человек обладает уникальными чертами и сознанием, которыми можно манипулировать. Напротив, как гражданин индивид встроен в более широкий социально-политический контекст, участвуя в общественной жизни и пользуясь конституционными правами. Например, статья 30 Конституции Российской Федерации гарантирует право создавать общественные объединения, а статья 32 обеспечивает право участвовать в управлении — как напрямую, так и косвенно — через голосование и выборы [21].

Помимо индивидуума, объектом влияния могут быть коллективные сущности. Это коллективное сознание можно разделить на три уровня:

- групповое сознание: сплоченное сообщество с общими ценностями и нормами.
- массовое сознание: слабо организованное, временное объединение людей, связанных общими эмоциональными переживаниями.
- общественное сознание: всеобъемлющий набор идей и ценностей, характерных для определенной эпохи.

А. Ю. Касюк отмечает, что «информационно-психологическое воздействие затрагивает как индивидуальное, так и общественное сознание» [23]. При этом государственные институты признаются ключевыми объектами в силу их важнейшей роли в поддержании общественного порядка и обеспечении функционирования государства. Также в его работе отмечено «Информационно-психологическое воздействие, будучи направленным на воздействия не только мнений, но и эмоционального фона общества, соответствует двум основным уровням – индивидуальному и массовому. При этом воздействие на личность обнаруживается через непосредственную манипуляцию восприятия, а на коллективном уровне – через общекультурные и социальные установки, что обеспечивает устойчивые модели поведения в социуме» [23]. Цитата приводит к тому, что для глубокого анализа необходимо учитывать социальные динамики и групповые взаимодействия.

В отличие от объекта, субъект информационно-психологического влияния определяется как источник, который владеет определенными знаниями, использует обозначенные методы и использует определенные средства для воздействия на объект. Этот субъект — «часто возникающий внутри или вне установленных систем — часто упоминается как «актор» в научном дискурсе «[33]. При рассмотрении влияния посредством суггестивных методов терминология далее различает «суггестор» (влияющий субъект) и «суггестенд»

(влияемый объект), термины, которые последовательно поддерживаются на протяжении всего этого обсуждения.

Этот анализ не только подчеркивает концептуальную неопределенность, окружающую разрушительное информационно-психологическое воздействие, но и подчеркивает практическую потребность в более четких определениях. Отсутствие точной терминологии усложняет разработку эффективных нормативных рамок и стратегий смягчения. Разлагая общее явление на его основные элементы — объект (как индивидуальный, так и коллективный) и субъект — работа закладывает фундаментальную основу для будущих исследований и формулирования политики. Она привлекает внимание к важности интеграции идей как из академических исследований, так и из законодательной практики для защиты индивидуальных прав и поддержания общественной стабильности в эпоху, отмеченную быстрой цифровой трансформацией.

В целом, исследование выступает за более тонкий подход к пониманию и регулированию информационно-психологических влияний. Такой подход необходим не только для теоретической ясности, но и для практической разработки правовых механизмов, которые могут адекватно решать проблемы, связанные как с полезными, так и с деструктивными формами влияния.

Относительно сущности информационно-психологического воздействия В.А. Баришполец определяет его как «совокупность информационного, психотропного и психофизического воздействия. Тем не менее, некоторые исследователи предостерегают от подведения под это понятие всех психофизических явлений, утверждая, что это может неоправданно расширить рамки информационно-психологической безопасности» [1]. Например, Г.В. Грачев утверждает, что «концепция информационно-психологического воздействия (ИПВ) позволяет исследователям выделить из более широкого круга психофизических воздействий отдельное подмножество, тем самым упорядочивая фокус своих исследований» [11].

В практическом применении не все психофизиологические факторы попадают в сферу информационного и психологического влияния. Влияющий субъект может в первую очередь влиять на слуховые и зрительные каналы — жизненно важные каналы получения информации — при этом не оказывая практически никакого влияния на вкусовое или тактильное восприятие. Исследователи часто применяют сенсорный критерий для определения того, какие каналы активируются. Кроме того, объективные меры влияния учитывают, что помимо физических эффектов субъект может напрямую влиять на психику другого человека посредством акустических, электромагнитных или оптических сигналов — например, определенные звуковые частоты могут вызывать раздражение или агрессию.

Процесс воздействия также охватывает распространение информации. Пункт 1 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» (Закон № 149-ФЗ, с изменениями от 14.07.2022) определяет информацию в широком смысле как «данные (сведения, сообщения) независимо от формы их представления» [35]. Это определение подчеркивает, что информация может передаваться не только с помощью технических средств, таких как телевизионное вещание, но и с помощью печатных материалов или даже путем прямого устного общения. Когда субъект, используя такие методы, как убеждение или внушение, стремится сформировать восприятие другого человека, взаимодействие между информационными и психологическими тактиками становится очевидным. Примечательно, что систематические исследования психологического воздействия имеют историю, восходящую к 1940-м годам [29], хотя эти методы использовались задолго до начала формальных исследований, первоначально через печатные СМИ, а теперь преимущественно через цифровые каналы.

В современном обществе лица, формирующие общественное мнение, часто обращаются к таким платформам, как YouTube, ВКонтакте и другим социальным сетям, чтобы генерировать и распространять контент — от видео и

фотографий до постов — который, хотя и кажется безобидным, часто направлен на нарушение общественного порядка. Эти создатели контента иногда намеренно распространяют фейковые новости или эмоционально заряженную дезинформацию, чтобы спровоцировать определенную реакцию и направить общественное восприятие.

Помимо массового распространения контента, межличностное общение остается важнейшим аспектом психологического влияния. Как личное, так и технологически опосредованное взаимодействие, усиленное ростом социальных сетей и мгновенных сообщений, расширило сферу влияния. Сегодня анонимные субъекты могут участвовать в спорных обменах с незнакомцами в сети, усиливая конфликты внутри виртуальных сообществ.

Данная работа подчеркивает сложность информационно-психологического влияния, выделяя его двойные измерения: сенсорное (психофизическое) и коммуникативное (информационное). Анализируя эти компоненты, исследование закладывает основу для более точного понимания того, как влияние оказывается по различным каналам. Анализ также подчеркивает, что хотя психофизические эффекты реальны, их роль ограничена конкретными сенсорными ограничениями. Напротив, расширенное определение передачи информации, подкрепленное правовыми рамками, такими как Федеральный закон [35], иллюстрирует разнообразные методы, посредством которых информация передается.

Значимость этого исследования заключается в его интегративном подходе, опирающемся как на академическую литературу, так и на законодательные документы. Оно не только проясняет границы информационно-психологического влияния, но и выявляет критические области, где необходимы дальнейшие исследования. Будущие исследования должны быть направлены на уточнение этих определений и изучение взаимодействия между динамикой цифровых медиа и правовыми нормами. Такие усилия будут иметь жизненно важное значение для разработки надежных стратегий по снижению рисков,

создаваемых манипулятивными влияниями во все более взаимосвязанном и оцифрованном мире.

Современный онлайн-ландшафт превратился в благодатную почву для вредоносного поведения, включая травлю, троллинг и флейминг. Негативные сообщества множатся в Интернете, часто занимаясь такими видами деятельности, как вербовка членов террористов, пропаганда членовредительства или самоубийства и разжигание ненависти среди или внутри социальных групп.

В свете этих вызовов российское законодательство ввело меры ответственности для противодействия такой практике. Например, статья 282 Уголовного кодекса Российской Федерации рассматривает такие преступления, как «возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» [70]. Эти правовые положения призваны пресекать распространение деструктивных сетевых влияний и защищать достоинство личности.

Помимо человеческих субъектов, искусственный интеллект все чаще признается потенциальным источником информации и психологического воздействия. Согласно подпункту «б» пункта 5 главы I Указа Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» от 10.10.2019 № 490, ИИ охватывает набор технологических решений, которые имитируют когнитивные функции человека, включая самообучение и решение проблем без фиксированных алгоритмов [49]. Поскольку многие компании теперь интегрируют голосовых помощников и чат-ботов в свои продукты, пользователи могут получать доступ к информации быстрее, чем когда-либо прежде. Однако ускоренные темпы развития ИИ опередили создание всеобъемлющих правовых рамок и защитных мер, что делает его привлекательным инструментом для злоумышленников, террористических группировок и других вредоносных субъектов.

Исследования Пашенцева подчеркивают «опасность злонамеренного использования искусственного интеллекта для подрыва индивидуальной

репутации, манипулирования рынками криптовалют и угрозы кибератак на критическую инфраструктуру» [56]. Помимо этих рисков, ИИ может усилить межэтнические, расовые и социальные конфликты. В настоящее время он используется как инструмент в информационной и гибридной войне, напрямую формируя общественное сознание. Растет обеспокоенность тем, что по мере дальнейшего развития технологий искусственный интеллект может в конечном итоге превратиться в самостоятельный субъект информационно-психологического воздействия.

Принимая во внимание все эти факторы, информационно-психологическое воздействие можно концептуализировать как комбинированное информационное и психофизическое воздействие на психику отдельного человека или группы, которое имеет силу изменять восприятие, отношение и поведение. Хотя такое воздействие может иметь позитивные применения, его способность причинять вред столь же значительна, когда оно используется деструктивно. В этом контексте деструктивное информационно-психологическое воздействие понимается как негативная сила, которая изменяет мировоззрение и отношение объекта, в конечном итоге приводя к поведению, которое ставит под угрозу человеческую жизнь, провоцирует социальные конфликты и дестабилизирует как национальные, так и мировые порядки.

Тщательное изучение нормативных правовых актов и документов стратегического планирования позволяет дать многогранное определение деструктивного информационно-психологического воздействия, которое охватывает несколько ключевых аспектов:

- прямая угроза национальной безопасности;
- злоупотребление правом на информацию;
- преступление против личности: правонарушения;
- соучастие в уголовных преступлениях;
- признание сделок недействительными;
- обоснование государственного вмешательства.

Правовой анализ этих проблем выявляет междисциплинарный характер деструктивного информационно-психологического воздействия: оно охватывает различные отрасли российского права и затрагивает многочисленные институциональные сферы.

Эта работа предлагает комплексный анализ деструктивных онлайн-практик, объединяя идеи из законодательных документов, технологических разработок и междисциплинарных исследований. Она подчеркивает срочность обновления правовых рамок, чтобы идти в ногу с быстро развивающимися технологиями, такими как искусственный интеллект. Исследование также подчеркивает двойственный характер информационно-психологического влияния: хотя оно может способствовать позитивной коммуникации и распространению информации, его потенциал для злоупотребления — особенно когда он используется в качестве оружия — представляет серьезные риски для общественной безопасности и национальной стабильности.

Анализируя явление на правовые, технологические и социальные компоненты, он обеспечивает более четкое понимание того, как деструктивные практики проявляются в сети. Эта всеобъемлющая перспектива имеет решающее значение для разработки эффективных контрмер и обеспечения того, чтобы вмешательство государства было как оправданным, так и соразмерным. Результаты служат призывом к действию для политиков, исследователей и практиков, чтобы они сотрудничали в разработке стратегий, которые смягчают неблагоприятные последствия деструктивных информационных и психологических воздействий в нашем все более цифровом мире.

Комплексный анализ нормативных документов и материалов стратегического планирования показывает, что правовая природа деструктивного информационно-психологического воздействия многогранна. В этом воздействии можно выделить несколько основных элементов:

- угроза безопасности: это явление напрямую подрывает национальную безопасность, дестабилизируя общественный порядок и ставя под угрозу целостность государства.
- злоупотребление информационными правами: оно тесно связано с неправомерным использованием права на информацию и свободы СМИ, когда распространение вредоносного контента может исказить общественное восприятие.
- преступление против личности: Деструктивное воздействие признается преступным деянием, если оно ставит под угрозу жизнь или посягает на честь и достоинство личности.
- соучастие в преступной деятельности: может выступать в качестве формы соучастия в уголовных преступлениях — посредством организации, подстрекательства или предоставления интеллектуальной поддержки, — что способствует более масштабной противоправной деятельности.
- признание сделок недействительными: когда решения или соглашения принимаются под влиянием существенной ошибки, вызванной таким воздействием, они могут быть признаны юридически недействительными.
- обоснование государственного вмешательства: Наличие этих влияний оправдывает применение государственных принудительных мер, таких как блокирование информационных ресурсов, для защиты общественных и национальных интересов.
- междисциплинарные последствия и значимость исследования.

Этот анализ наглядно иллюстрирует междисциплинарный характер проблемы, поскольку она охватывает несколько отраслей российского права, включая уголовное, административное и информационное регулирование. В работе подчеркивается, что для решения проблемы деструктивного информационно-психологического воздействия необходима комплексная

правовая база. Такая база должна сбалансировать императив защиты национальной безопасности с сохранением прав личности и свобод СМИ.

Кроме того, это исследование способствует более глубокому пониманию того, как правовые механизмы могут быть адаптированы для противодействия новым угрозам в цифровую эпоху. Синтезируя идеи из нормативных документов и материалов стратегического планирования, работа обеспечивает критически важную основу для будущей разработки политики и совершенствования законодательства. Она призывает законодателей, экспертов по безопасности и ученых-юристов к сотрудничеству в разработке надежных мер, которые смягчают пагубные последствия деструктивных информационно-психологических практик, одновременно защищая основополагающие принципы свободы слова и демократического управления.

1.2 Методы и средства деструктивного информационно-психологического воздействия

Наши исследования природы деструктивного информационно-психологического воздействия показывают, что оно представляет собой специфическое проявление в более широком спектре информационно-психологических воздействий. Хотя его методы во многом совпадают с общими подходами, акцент здесь делается на результатах, которые преимущественно негативны. Это исследование вносит вклад в текущую дискуссию, проясняя используемые методы и подчеркивая их потенциальные последствия.

Современная литература предлагает различные перечни методов информационно-психологического воздействия. Так, С.И. Макаренко описывает современные подходы как «сложные «психотехнологии», направленные на воздействие на психику человека» [31, с. 408]. В схожем ключе И. Смирнов, Е. Безносюк и А. Журавлев «рассматривают эти психотехнологии как технологии, оказывающие прямое воздействие на нервную систему» [62]. В то время как

многие работы лишь поверхностно освещают эту тему, Н.Д. Узлов дает углубленное определение, «характеризуя психотехнологии как организованный и эффективный комплекс практик, применяемых в различных социальных сферах для решения психологических проблем и достижения целевых социальных эффектов по определенному алгоритму» [69]. В нашей работе мы определяем психотехнологии как методы информационно-психологического воздействия, изменяющие психику человека и способные в конечном итоге привести к изменению поведения. В ходе проведения, посвящённом информационному противоборству, С. И. Макаренко подробно анализирует феномен деструктивного воздействия через призму современных психотехнологий. Он обратил внимание: «Современные психотехнологии, используемые в информационной войне, представляют собой не просто набор инструментов для передачи данных, целостную систему, способную изменять когнитивные и эмоциональные состояния людей. Такие технологии, действующие как на рациональные, так и на иррациональные аспекты психики, создают особый тип информационного давления, которые трудно нейтрализовать стандартными методами» [31]. Данный отрывок подчёркивает уровень междисциплинарного подхода для понимания и противодействия новым формам общества.

Убеждение — первый метод. Он включает в себя воздействие как на эмоциональные, так и на рациональные аспекты оппонента путем представления четких, убедительных аргументов. Цель состоит в том, чтобы убедить аудиторию в точке зрения актера. Однако одних логических аргументов недостаточно; жизненно важно, чтобы сообщение было не только услышано, но и понято. Такие факторы, как осведомленность получателя о проблеме, уровень образования, отношение к актеру и языковая совместимость, играют важную роль. Исследования показывают, что убеждение более эффективно, когда получатель относится к источнику благосклонно или разделяет схожие характеристики, такие как политические убеждения или культурное

происхождение. Кроме того, при подаче следует избегать сухого изложения фактов и вместо этого интегрировать эмоциональный компонент. Убеждение обычно использует три типа аргументов:

- фактические аргументы: основаны исключительно на проверяемых событиях.
- аргументы в пользу позитивных ожиданий: сочетающие факты с обещаниями лучшего будущего.
- аргументы с негативным ожиданием: призваны вызвать гнев или ненависть к объекту воздействия.

В убеждении также существуют различные стили общения. Двустороннее общение подразумевает обмен аргументами, что позволяет действующему лицу противостоять доводам оппонента — этот подход часто наблюдается в дискуссиях среди хорошо образованных людей, склонных сравнивать различные точки зрения. Напротив, одностороннее общение эффективно, когда получатель не питает враждебности к источнику и предрасположен принять переданную точку зрения, хотя аргументы все равно должны быть ясными и убедительными.

Второй метод, внушение, действует либо сознательно, либо бессознательно, заставляя людей принимать убеждения или установки действующего лица без критической оценки. Ученые различают различные аспекты внушения. Одной из важных точек зрения является субъективное влияние, оказываемое внушающим на получателя. Например, В. М. Бехтерев утверждал, что «внушающий оказывает влияние посредством определенных эмоций и чувств» [2]. «Внушение – это процесс, в ходе которого человек принимает определенные установки или идеи, зачастую не прибегая к их критическому анализу, из-за влияния эмоциональных и сенсорных стимулов. Особенно эффективно этот метод воздействует в условиях, когда когнитивные способности человека ослаблены под воздействием стресса или эмоционального напряжения» [2]. Этот метод широко применяется в различных понятиях, от рекламы до информационной войны, что подчёркивает его актуальность для

понимания современных методов манипуляции. Убеждение, так и внушение являются центральными методами информационно-психологического воздействия, причем первое делает акцент на логической и эмоциональной аргументации, а второе действует посредством менее критично оцененного принятия идей.

Второй аспект внушения касается характеристик самого процесса восприятия. Здесь ключевым фактором является отсутствие знаний и критического мышления, что означает, что человек должен быть высоко внушаемым. Исследователи выявили особые группы, которые особенно уязвимы — часто это подростки и пожилые люди. Подростки, движимые энтузиазмом, склонны оказывать большое доверие авторитетным лицам, в то время как люди старшего возраста могут принимать информацию за чистую монету из-за своего возраста. Однако возраст — не единственный определяющий фактор; неспособность человека оценить ситуацию — особенно во время кризисов, таких как стихийные бедствия или экономическая нестабильность (например, высокая инфляция или дефолт) — также повышает внушаемость.

Можно сказать, что внушение может происходить как напрямую, так и косвенно. В отличие от убеждения, которое опирается на четкие доказательства и логическую аргументацию, внушение в первую очередь нацелено на эмоции. Оно наиболее эффективно, когда получатель предрасположен принять сообщение на веру, особенно в условиях, когда его критические способности скомпрометированы.

Третий метод, который следует рассмотреть, — это манипуляция сознанием. Чтобы понять его полный смысл, необходимо распознать несколько ключевых характеристик: это форма психологического воздействия; манипулятор рассматривает цель лишь как средство достижения личной выгоды; он нацелен на односторонние выгоды; и он действует скрытно, как в своем применении, так и в своем предполагаемом результате. Манипуляция, как

правило, заключается в эксплуатации личных слабостей посредством психологического давления, используя тактику, которая является одновременно искусной и незаметной. По сути, этот метод заключается в скрытом воздействии на кого-либо для обеспечения односторонних выгод, заставляя цель принять точку зрения манипулятора. Наиболее точное определение манипуляции дал Доценко Е. Л., который описал ее как «вид психологического воздействия, искусное выполнение которого приводит к скрытому возбуждению намерений у другого человека, не совпадающих с его существующими в данный момент желаниями» [15]. «Манипуляция сознанием – это вид воздействия, при котором субъект, с помощью сложных психологических приемов, добивается изменений в волевых структурах другого человека, зачастую обходит его выдающиеся способности и сознательное сопротивление. Основным принципом данного метода является его скрытый характер, когда истинные цели воздействия остаются незаметными для объекта» [15]. Подобный подход позволяет, поскольку современные технические средства манипуляции могут быть интегрированы в широкий спектр информационно-психологических воздействий, создавая серьезные вызовы для защиты психического здоровья.

Манипуляцию можно разделить на два типа: неосознанную и осознанную. При рассмотрении деструктивного информационно-психологического воздействия исследователи, как правило, фокусируются на осознанной манипуляции. Г. В. Грачев и И. К. Мельник выделили несколько групп факторов, которые влияют как на «эффективность, так и на потенциальную опасность таких манипулятивных приемов» «Предложение «актора» в информационно-психологическом воздействии должно трактоваться не только как носитель определенных знаний и методов, но и как динамичный участник процесса, чья роль может обсуждаться в зависимости от контекста и характера воздействия. Именно эта гибкость позволяет субъекту воздействия адаптироваться к изменяющимся условиям и эффективно реализовывать свои цели» [12]. В этом утверждении делается акцент на необходимость расширения понятий

«суггестор» и «суггестенд», что является необходимым условием для выработки методов противодействия. [12]. Первая группа относится к содержанию и структуре самих манипулятивных приемов. Вторая группа включает внешние факторы информационно-коммуникационной среды, такие как качество звука и изображения, мастерство манипулятора, которые влияют на общее воздействие. Третья группа состоит из индивидуальных факторов, определяющих восприимчивость человека к манипуляции. Хотя часто упоминается низкий уровень образования, другие характеристики, такие как робость, неуверенность в себе, отсутствие достаточных знаний по предмету, также играют решающую роль. Исследователи далее делят эту третью группу на ситуативные и неситуативные факторы.

Ситуационные факторы относятся к психическому состоянию человека в экстремальных условиях, например, в толпе или во время интенсивных переговоров, когда эмоции, как правило, накаляются. Напротив, «неситуационные факторы связаны с врожденными чертами личности, такими как критическое мышление, скептицизм или неуверенность в себе, которые могут влиять на то, насколько человек подвержен манипуляциям» [12].

С развитием Интернета манипулятивные методы значительно развились, расширив сферу разрушительного информационно-психологического воздействия. Одним из примечательных методов является представление бессознательной акустической информации. Хотя психофизическое воздействие имеет свои пределы в рамках разрушительной информационно-психологической тактики, звук остается мощным инструментом.

В 1993 году Фрэнсис Раушер и Гордон Шоу провели эксперимент, позже названный «эффектом Моцарта», в котором «добровольцы слушали сонату композитора, прежде чем пройти тест на пространственное мышление. Результаты показали, что участники решали задачи быстрее после музыкального воздействия, хотя эффект был временным» [5]. Этот эксперимент иллюстрирует потенциал музыки влиять на когнитивные процессы, принцип, лежащий в

основе ее использования в кинематографии для формирования эмоциональной атмосферы фильма. Аналогичным образом национальные гимны, благодаря своим отличительным мелодиям, могут вызывать сильные ассоциации и внушать чувство патриотизма.

Другим ключевым методом является представление неосознанной визуальной информации. Исследования показывают, что примерно 80% информации, которую мы получаем, является визуальной. Поскольку социальные сети сейчас доминируют в потреблении медиа, люди все больше отдают предпочтение видео и изображениям, а не простому тексту. Создатели контента регулярно включают фотографии или видео в свои посты, чтобы привлечь и удержать внимание аудитории. Такие факторы, как положение объекта, форма, движение, цвет и яркость изображений, могут оказывать глубокое влияние на зрителей. Психологи обнаружили, что уровень яркости может влиять на настроение — хорошо освещенная среда, как правило, заряжает нас энергией, в то время как тусклая обстановка может способствовать апатии или грусти. В сфере деструктивного информационно-психологического влияния актеры могут намеренно разрабатывать визуальный контент, чтобы манипулировать эмоциональными реакциями своей аудитории.

Последний метод включает комбинированный подход, когда несколько методов используются одновременно для усиления общего воздействия. Например, влиятельный человек может опубликовать убедительный пост в социальных сетях, сопровождаемый видео, которое использует бессознательные визуальные подсказки. В качестве альтернативы видеообращение на YouTube может использовать сознательную манипуляцию для построения взаимопонимания со зрителями, вставляя компрометирующие изображения, все это под тщательно подобранное музыкальное сопровождение. Эффективность этих методов во многом зависит от используемого средства; сегодня Интернет и телевидение доминируют как основные платформы для распространения такого влияния, в то время как радио постепенно теряет свою значимость.

По данным Всероссийского центра изучения общественного мнения, основанным на тенденциях на 6 октября 2022 года, «медиапотребление в настоящее время, как правило, следует гибридной модели, сочетающей телевидение и онлайн-источники. Исследование ВЦИОМ, в котором анализировались ответы по полу, возрасту, уровню образования и месту проживания, показало, что 53% россиян активно пользуются как телевидением, так и интернетом, причем эта тенденция несколько сильнее выражена среди граждан в возрасте 45–59 лет по сравнению с более молодыми поколениями. Анализ моделей потребления медиа выявляет четкое разделение предпочтений между поколениями. Среди молодых людей в возрасте 18-24 лет 66% являются активными пользователями Интернета, в то время как в возрастной группе 25-34 лет этот процент немного снижается до 52%. Напротив, телевидение остается доминирующим выбором для более старших демографических групп — 43% граждан в возрасте 60 лет и старше, а также 43% неработающих пенсионеров в первую очередь полагаются на телевидение для получения информации. Между тем, только 1% молодой аудитории активно смотрят телевидение. Сельские жители также больше склоняются к телевидению, 25% из них идентифицируют себя как активных телезрителей» [68].

Эти цифры показывают, что хотя телевидение остается актуальным, оно уступило место Интернету как ведущей платформе для потребления информации. Данные также свидетельствуют о том, что по мере взросления молодого поколения, которое в основном пользуется Интернетом, Всемирная паутина еще больше укрепит свой статус основного источника информации. Упадок традиционных СМИ, особенно печатных, еще больше поддерживает эту тенденцию. С цифровым сдвигом большинство крупных газет и журналов переместили свой контент в онлайн, используя социальные сети и платформы мгновенного обмена сообщениями для охвата аудитории.

Хотя люди старшего возраста по-прежнему предпочитают печатные СМИ, их значительно меньше, чем тех, кто потребляет информацию через цифровые

платформы. Рассматривая методы деструктивной информации и психологического воздействия, а также каналы, по которым они распространяются, становится ясно, насколько велик контроль субъектов над общественным восприятием, особенно через Интернет, который в настоящее время служит одним из самых мощных инструментов формирования общественного и политического дискурса.

1.3 Международно-правовые стандарты защиты от негативного информационно-психологического воздействия

В сегодняшнюю цифровую эпоху обеспечение информационной и психологической безопасности является многогранной задачей, требующей как национальных инициатив, так и международного сотрудничества. Ученые выступают за скорейшее создание всеобъемлющего международного договора для установления универсальных стандартов в этой области, который мог бы сыграть решающую роль в предотвращении кибертерроризма и укреплении глобальной стабильности. В то же время различные существующие международные правовые инструменты уже закладывают основу для регулирования этих вопросов.

«Каждый человек имеет право на свободу выражения мнений и на получение информации. При этом данное право должно осуществляться с соблюдением баланса между свободой слова и необходимостью защиты от информации, способной причинить вред психическому здоровью и общественному порядку» [6]. Международный пакт о коррупции и финансовые права регулируют эти принципы, подчёркивая обязанность принимать меры государств по защите уязвимых групп, в частности детей, от негативного воздействия информационного контента [30]. Важнейшим столпом, поддерживающим информационную и психологическую безопасность, является право в области прав человека, которое уравновешивает индивидуальные

свободы с соответствующими обязанностями в информационной сфере. Россия остается участником основных международных документов, включая:

- Всеобщая декларация прав человека (10 декабря 1948 г.) [6]
- Международный пакт о гражданских и политических правах (16 декабря 1966 г.) [30]

Международное право уделяет особое внимание защите детей от пагубного информационного и психологического воздействия. Конвенция о правах ребенка (20 ноября 1989 г.) включает в себя несколько ключевых положений:

- статья 17(a) призывает медиаорганизации распространять контент, который поддерживает социальное и культурное развитие детей [24];
- статья 17(e) призывает государства принять меры, которые защищают несовершеннолетних от вредной информации [24];
- статья 19 обязывает государства принимать активные меры по защите детей от психологического насилия, унижений и жестокого обращения [24].

Хотя Конвенция защищает свободу слова и выражения мнений, она одновременно подчеркивает острую необходимость защиты несовершеннолетних от потенциально разрушительного воздействия медиасреды.

Помимо универсальных договоров, региональные соглашения также затрагивают эти вопросы. Например, Конвенция СНГ о правах человека и основных свободах (26 мая 1995 г.) закрепляет право на неприкосновенность частной жизни, включая конфиденциальность переписки, за исключением случаев, когда ограничения оправданы императивами национальной и общественной безопасности или общественного порядка [25]. Более того, статьи 10 и 11 этой Конвенции поддерживают свободу мнений, слова и религии в соответствии с глобальными стандартами прав человека.

Наше исследование рассматривает эти международные и региональные правовые рамки, чтобы обеспечить целостный взгляд на информационную и психологическую безопасность в цифровую эпоху. Синтезируя принципы, закрепленные в документах по правам человека и региональных соглашениях, мы подчеркиваем необходимость скоординированного правового ответа, который связывает мировые стандарты с национальной реализацией. Наше исследование вносит вклад в эту область следующим образом:

- демонстрация того, как существующие правовые инструменты устанавливают права и обязанности в цифровой сфере.
- подчеркнуть важность защиты уязвимых групп, особенно детей, от вредоносного влияния в Интернете.
- Утверждая, что, хотя существующие правовые рамки обеспечивают прочную основу, быстро меняющийся цифровой ландшафт требует дальнейшего международного сотрудничества и правовых инноваций.
- Предполагается, что всеобъемлющий международный договор может стать важнейшим инструментом предотвращения кибертерроризма и поддержания международной стабильности.

Можно сказать, что правовая сфера, которая регулирует информационную и психологическую безопасность, поддерживается надежными международными и региональными рамками, такими как Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах и Конвенция о правах ребенка [6, 30, 24]. Кроме того, региональные инструменты, такие как Конвенция СНГ, вносят дополнительный вклад в эту нормативную среду [25]. Наша работа подчеркивает, что, хотя эти инструменты обеспечивают существенную защиту, постоянное международное сотрудничество и правовое совершенствование являются обязательными для решения возникающих проблем в цифровую эпоху и обеспечения безопасной информационной среды для всех.

Таким образом, хотя международные правовые рамки уже регулируют аспекты информационно-психологической безопасности, растущие риски, создаваемые цифровыми технологиями и киберугрозами, подчеркивают настоятельную необходимость более всеобъемлющего и реализуемого глобального соглашения в этой сфере.

Устав ООН играет ключевую роль в защите государственного суверенитета от внешнего информационного вмешательства. В частности, пункт 7 статьи 2 разъясняет, что положения Устава не уполномочивают ООН вмешиваться во внутренние дела государств-членов или заставлять их разглашать подробности своих внутренних процессов [71]. Это положение гарантирует, что государства остаются защищенными от необоснованного внешнего давления, за исключением ситуаций, когда существует «угроза миру, нарушение мира или акты агрессии», что затем позволяет применять принудительные меры, изложенные в Главе VII Устава [71].

В современную эпоху Интернет стал основной платформой для распространения информации. Поскольку средства массовой информации все чаще переходят на цифровые каналы, люди теперь в значительной степени полагаются на новостные сайты и социальные сети для получения обновлений в режиме реального времени. Однако эта цифровая эволюция опередила развитие универсальной международной правовой базы. В настоящее время нормы и процедуры управления киберпространством в значительной степени определяются необязательными международными рекомендациями, а не обязательными к исполнению договорами.

Одной из заметных внутренних инициатив является Указ Президента Российской Федерации № 203 (9 мая 2017 г.), в котором изложена Стратегия развития информационного общества в России на 2017–2030 годы. В Главе II этой стратегии содержатся ссылки на ключевые международные соглашения, в том числе:

- Окинавская хартия глобального информационного общества (22 июля 2000 г.);
- Декларация принципов: «Построение информационного общества – глобальная задача в новом тысячелетии» (12 декабря 2003 г.);
- План действий по реализации Тунисского обязательства (15 ноября 2005 г.) [50].

Эти соглашения представляют собой первые шаги к регулированию информационно-коммуникационных технологий (ИКТ), признавая их в качестве движущих сил производительности, экономического роста и улучшения качества жизни. В частности, Тунисское обязательство подчеркивает необходимость борьбы с киберпреступностью и поощряет «позитивное использование Интернета» [67].

Несмотря на эти усилия, всеобщий договор, который всесторонне регулировал бы киберпространство, остается неуловимым. Этот пробел препятствует эффективной борьбе с киберпреступностью и мониторингу сетевых угроз. Конвенция о киберпреступности рассматривается многими как многообещающий кандидат на роль первого глобального правового инструмента, регулирующего международное кибервзаимодействие, одновременно обеспечивая государственную безопасность от информационных и психологических угроз.

Вместо обязательного международного договора государства в настоящее время полагаются на несколько специализированных резолюций ООН для защиты своих цифровых информационных пространств. Среди них следует отметить резолюции Генеральной Ассамблеи ООН A/55/63 [59] и A/RES/56/63 под названием «Борьба с преступным использованием информационных технологий» [60], которые призывают к расширению межправительственного сотрудничества в борьбе с киберпреступностью. Более того, Глобальная контртеррористическая стратегия ООН, принятая резолюцией Генеральной Ассамблеи A/RES/60/288 8 сентября 2006 года, играет решающую роль в этой

сфере. Она обязывает государства «принимать правовые меры против подстрекательства к терроризму и ограничивать распространение экстремистского контента, уделяя особое внимание онлайн-угрозам и выступая за скоординированные усилия на региональном и международном уровнях» [10].

Исследование объединяет вышеуказанные международные и внутренние правовые рамки, чтобы предложить всесторонний анализ мер, действующих для противодействия негативной информации и психологическому влиянию. Оценивая сильные и слабые стороны текущих международных соглашений, резолюций ООН и внутренних стратегий, наша работа подчеркивает настоятельную необходимость в обязательном глобальном договоре о киберпространстве. Этот договор мог бы стандартизировать нормы и процедуры, тем самым повышая коллективную способность противодействовать киберпреступности и защищать общественную безопасность. Наши выводы вносят вклад в более широкий дискурс по информационной безопасности, соединяя анализ политики с практическими последствиями и предлагая действенные шаги к более безопасной цифровой среде.

Взаимодействие между национальным суверенитетом, международными правовыми принципами и быстрым развитием цифровой коммуникации подчеркивает сложные проблемы в обеспечении информационной и психологической безопасности. Хотя существующие документы, такие как Устав ООН и различные резолюции ООН, предоставляют основные руководящие принципы, отсутствие всеобъемлющего международного договора остается критическим пробелом. Наша работа подчеркивает этот пробел и выступает за более тесное международное правовое сотрудничество для лучшего регулирования киберпространства и защиты обществ во всем мире.

Заметным инструментом на региональной арене является Конвенция Шанхайской организации сотрудничества (ШОС) о борьбе с экстремизмом. В этом документе подчеркивается важность бдительного мониторинга как

традиционных СМИ, так и Интернета для быстрого выявления и нейтрализации экстремистских идеологий (пункт 6, статья 7) [27]. Он также подчеркивает необходимость укрепления морального и духовного образования (пункт 8, статья 7) в качестве упреждающей меры по снижению восприимчивости граждан к негативному психологическому воздействию, исходящему от террористических организаций.

Задолго до цифровой эпохи международные руководящие принципы сыграли значительную роль в формировании ответственности традиционных СМИ. Например, Декларация ЮНЕСКО от 28 ноября 1978 года излагает основные принципы вклада СМИ в дело мира, прав человека и борьбы с расизмом, апартеидом и подстрекательством к войне [14]. Этот документ выступает за диверсификацию источников информации, гарантируя, что общественность может получить объективное понимание событий, и подчеркивает важность свободного общения для журналистов. Он также подчеркивает важную роль СМИ в привитии ценностей мира, справедливости и взаимного уважения среди молодежи. Аналогичным образом, Декларация принципов «Построение информационного общества — глобальный вызов нового тысячелетия» от 12 декабря 2003 года подтверждает приверженность свободе выражения мнений и прессы. Эта декларация призывает специалистов СМИ ответственно обращаться с информацией и поддерживать высокие этические и профессиональные стандарты [17].

В сфере обеспечения международной информационной безопасности важнейшее значение имеют такие документы, как Соглашение между правительствами государств-членов ШОС. В статье 2 этого соглашения основными угрозами международной информационной безопасности определены:

- Информационная преступность;
- Информационный терроризм;

- Распространение контента, дестабилизирующего общественно-политические системы и наносящего ущерб духовной, нравственной и культурной среде [66].

В этом соглашении эти вызовы не только классифицируются как центральные в проблеме негативного информационного и психологического воздействия, но и излагаются стратегии совместных мер противодействия, разработки совместных инициатив и обмена передовым опытом между государствами-членами.

Несмотря на существование различных международных и региональных документов, направленных на защиту информации и психологической безопасности, отсутствие обязательного универсального договора представляет собой значительную проблему. Поскольку террористические организации и другие злонамеренные субъекты постоянно изобретают новые методы, чтобы повлиять на общественное мнение и нарушить государственные функции, этот пробел в регулировании позволяет некоторым государствам обходить существующие нормы. Трудность в разработке всеобъемлющего международного договора о психологической безопасности еще больше усугубляется различными политическими системами, религиозными убеждениями, уровнями развития ИКТ и различными структурами Всемирной паутины в разных государствах.

Исследование критически рассматривает эти региональные и международные инструменты, интегрируя их идеи для устранения недостатков регулирования в текущей глобальной структуре. Анализируя меры, изложенные в таких документах, как Конвенция ШОС [27], Декларация ЮНЕСКО [14] и Декларация принципов информационного общества [17], а также Соглашение ШОС о международной информационной безопасности [66], мы подчеркиваем необходимость в целостном и реализуемом глобальном правовом инструменте.

Выводы по Главе 1.

В первой главе дипломной работы проведён всесторонний теоретико-правовой анализ феномена деструктивных молодёжных субкультур, раскрыты их социальные, психологические и правовые характеристики. Автор обозначает, что в условиях цифровизации и трансформации коммуникационной среды молодёжь становится особенно уязвимой перед влиянием девиантных сообществ, формирующих деструктивные установки поведения, подрывающие общественные и правовые устои.

Проанализированы базовые понятия и признаки, позволяющие отграничить деструктивные объединения от традиционных форм молодёжной самореализации. Особое внимание уделено таким группам, как «АУЕ», «Колумбайн» и «МКУ», которые характеризуются наличием антисоциальной идеологии, пропагандой насилия, отказом от социальных норм, а порой и прямыми призывами к совершению преступлений.

Важным аспектом главы является рассмотрение правовых основ противодействия указанным явлениям. Автор делает акцент на положениях Конституции Российской Федерации, федеральных законов, таких как ФЗ «О противодействии экстремистской деятельности», ФЗ «Об информации, информационных технологиях и о защите информации», а также международно-правовых обязательствах России в сфере защиты прав ребёнка. Подчёркивается, что эффективное реагирование на угрозы со стороны деструктивных субкультур требует комплексного подхода — правового, социального, педагогического и информационного.

Таким образом, в первой главе заложен теоретический и нормативный фундамент для дальнейшего практического анализа, что позволяет сделать вывод о необходимости системного регулирования и межведомственного взаимодействия в целях минимизации влияния деструктивных субкультур на молодёжь.

Глава 2 Информационно-психологическая безопасность и защищенность граждан РФ от деструктивного информационно-психологического воздействия

2.1 Правовые основы информационно-психологической безопасности и ее принципы

Для всесторонней защиты граждан Российской Федерации от вредоносной информации и неблагоприятных психологических воздействий необходимо детально проанализировать правовую базу, регламентирующую как информационную, так и психологическую безопасность. При всей значимости данной проблемы до настоящего времени не выработано единое законодательное определение.

В этой связи А.А. Смирнов и другие исследователи отмечают, что информационно-психологическая безопасность представляет собой «состояние защищенности личности, социальных групп и общества от деструктивных информационных и психологических воздействий» [63]. Еще в начале 2000-х предпринимались попытки разработать проект Федерального закона «Об информационно-психологической безопасности», призванного четко разграничить объекты и субъекты информационно-психологического влияния. В данном проекте указывались и некоторые ключевые угрозы, среди которых: «пагубное воздействие на здоровье человека; скрытное подавление свободы слова личности и искусственное создание синдромов зависимости; размывание политической, культурной и нравственной самоидентификации; манипулятивные действия, направленные на воздействие на общественное сознание; фрагментация единого информационного и духовного пространства Российской Федерации, что приводит к ослаблению традиционных социальных структур и общественной морали, а также ущемлению других жизненно важных интересов личности, общества и государства» [44].

На сегодняшний день комплексное законодательное определение информационно-психологической безопасности по-прежнему отсутствует. В качестве национального интереса данное явление упоминается лишь кратко в главе III Указа Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [46].

Необходимо четко различать информационную безопасность и информационно-психологическую безопасность. Под первой понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, обеспечение конституционных прав и свобод человека и гражданина, достойного качества жизни, суверенитета, территориальной целостности и устойчивого социально-экономического развития Российской Федерации, а также обороноспособности и безопасности государства» [51]. Информационно-психологическая безопасность, напротив, охватывает более широкий спектр мер защиты, в том числе и ограждающих психику человека от негативных психологических воздействий.

Важным аспектом этого дискурса является защита детей, которые особенно подвержены вредному влиянию. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (от 29.12.2010 № 436-ФЗ) решает эту уязвимость, регулируя распространение вредной информации в различных медиапродуктах [38]. Хотя это законодательство напрямую не определяет более широкие понятия информационной и психологической безопасности, оно предоставляет обширный перечень запрещенного контента и устанавливает стандарты оборота и классификации информационной продукции. Кроме того, оно определяет обязанности федеральных надзорных органов. Примечательно, что, хотя это и стало первым законодательным шагом в регулировании этих вопросов, закон не охватывает положения об ответственности за негативное информационное и психологическое воздействие во всемирной паутине — основной арене современного распространения информации.

Критический анализ этих законодательных усилий выявляет существенные пробелы, требующие дальнейшего исследования и уточнения. Отсутствие четкого, единого определения не только усложняет правоприменение, но и оставляет место для интерпретационных двусмысленностей, которые могут подорвать эффективную защиту. В эпоху, когда цифровая коммуникация стремительно развивается, создание надежных правовых определений и механизмов имеет важное значение. Работа таких ученых, как А. А. Смирнов, обеспечивает фундаментальную основу, на которой могут строиться будущие законодательные инициативы. Двигаясь вперед, крайне важно, чтобы правовые реформы учитывали как традиционные, так и возникающие угрозы, интегрируя идеи психологических исследований и адаптируясь к динамике цифровых медиа. Этот комплексный подход повысит эффективность правовой защиты и обеспечит защиту граждан в сложной информационной среде.

Для устранения пробелов в регулировании Интернета краеугольным камнем служит Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», вступивший в силу 27 июля 2006 года. Этот закон устанавливает четкие обязанности для тех, кто распространяет информацию в сети Интернет, вводя понятие «организатор распространения информации» (статья 10.1) [35]. Он также устанавливает требования к управлению контентом в социальных сетях, определяет обязанности операторов сайтов, интернет-сообществ и информационных систем (статья 10.6) [35].

Средства массовой информации, являющиеся основным каналом как информационного, так и психологического воздействия, подпадают под действие специальной правовой базы. Закон № 2124-1 «О средствах массовой информации» (27 декабря 1991 г.) играет решающую роль в этом контексте. Ключевое положение статьи 4 этого закона касается злоупотребления свободой СМИ путем запрета скрытых практик, таких как скрытые вставки — приемов,

которые могут подсознательно влиять на аудиторию или отрицательно сказываться на ее здоровье [45]. Этот закон примечателен тем, что является одним из немногих, которые явно учитывают психологическую безопасность граждан в своих положениях.

Реклама является еще одной важной сферой регулирования для обеспечения информационной и психологической безопасности. Федеральный закон «О рекламе» (13 марта 2006 г. № 38-ФЗ) определяет рекламу в статье 3, части 1 как любую форму информации, направленную на привлечение внимания, поддержание интереса и продвижение объекта рынка [36]. Статья 5 также запрещает недобросовестную рекламу, которая может порочить честь, достоинство или репутацию гражданина или содержать нецензурную лексику, оскорбительные образы или дискриминационные сравнения по признаку пола, расы или религии. Это законодательство также регулирует практику интернет-рекламы и включает меры по защите детей от вредоносной рекламы, которая может подорвать самооценку, побудить к само разрушительному поведению или подорвать доверие к родительским фигурам [36].

Помимо этих конкретных актов, более широкая правовая архитектура обеспечения информационной и психологической безопасности строится на конституционном, административном, уголовном и гражданском праве. Конституция закрепляет основные права и свободы граждан; в частности, часть 2 статьи 29, пункт 2 запрещает пропаганду или агитацию, возбуждающую социальную рознь или возвышающую одну группу над другой [21]. Административное право далее определяет роли государственных органов, ответственных за защиту граждан от вредной информации. Например, статья 13.14 Кодекса об административных правонарушениях ограничивает раскрытие конфиденциальной информации, такой как информация, касающаяся несовершеннолетних или конфиденциальных медицинских данных [22], в то время как статья 5.61.1 того же кодекса предусматривает санкции за клевету,

которая может нанести ущерб общественному восприятию и моральному благополучию личности [22].

Уголовное право также устанавливает наказания за нарушения, связанные с информационной и психологической безопасностью. Статьи 150–151 Уголовного кодекса предусматривают наказания за действия с участием несовершеннолетних, способствующие преступному или антиобщественному поведению [70]. Например, психологическое давление на несовершеннолетнего с целью подстрекательства к беспорядкам может повлечь за собой санкции, варьирующиеся от обязательных работ или ограничения свободы до лишения свободы. Кроме того, гражданское право предусматривает средство правовой защиты за моральный вред через статью 151 Гражданского кодекса, которая уполномочивает суды присуждать денежную компенсацию за любой физический или психологический вред, причиненный гражданину [13].

Эта интегрированная правовая база — это не просто набор запретов и штрафов, она отражает продуманную стратегию по созданию безопасной и ответственной цифровой среды. Решая многогранные проблемы как традиционных, так и цифровых медиа, эти законы иллюстрируют сбалансированный подход: хотя свобода выражения мнений остается основной ценностью, она гармонизируется с надежными гарантиями защиты отдельных лиц, особенно уязвимых групп, таких как дети, от пагубного влияния. Законодательные усилия по переплетению положений в различных областях — от регулирования Интернета и средств массовой информации до рекламы и конституционных прав — демонстрируют приверженность защите общественности как от явных, так и от скрытых форм психологической манипуляции.

По сути, работа, воплощенная в этих правовых мерах, заключается в создании устойчивой защитной сети. Она гарантирует, что быстрое развитие цифровых технологий и каналов связи не будет происходить за счет психологического здоровья или социальной гармонии общественности. Такой

подход имеет решающее значение в современном взаимосвязанном обществе, где границы между информацией, влиянием и психологическим благополучием все больше размываются.

Хотя существуют различные меры регулирования, целостная законодательная база, которая четко определяет концепцию, принципы, цели и сферу информационной и психологической безопасности, по-прежнему отсутствует. Действующие правовые инструменты разбросаны по множеству документов, каждый из которых рассматривает отдельные правонарушения, а не устанавливает комплексную доктрину. Этот разрозненный подход подчеркивает необходимость всеобъемлющей правовой основы для руководства будущими разработками в этой области.

Наряду с конституционными принципами Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (вступил в силу 27 июля 2006 г.) устанавливает основные правила обеспечения информационно-психологической безопасности. В этом законе выделены:

- «необходимость обеспечения целостности информационных систем на всей территории Российской Федерации.
- необходимость надежности и своевременности распространения информации.
- защита личной неприкосновенности путем запрета несанкционированного сбора, хранения, использования или распространения личных данных» [35].

В целях дальнейшего укрепления этих положений Федеральный закон «О безопасности» (№ 390-ФЗ от 28 декабря 2010 г.) предусматривает принятие превентивных мер, систематическое применение протоколов безопасности и координацию действий федеральных и международных органов [41].

Проекты предложений в этой области подчеркивают идею государственной монополии на разработку и производство специальных средств информационно-психологического воздействия (ИПВ). Эти «специальные

средства» — охватывающие технические устройства и программные инструменты — предназначены для оказания негативного психологического воздействия на отдельных лиц или группы. Учитывая стремительный технологический прогресс, такие инструменты могут быть использованы не по назначению в качестве инструментов принуждения, что делает обязательным для государства принятие строгих правовых мер для противодействия потенциальным злоупотреблениям [44].

При разработке единой доктрины также важно соответствовать международным правовым нормам. Например, Устав ООН закрепляет такие принципы, как государственный суверенитет, невмешательство во внутренние дела и мирное разрешение споров [71]. Аналогичным образом, Решение Совета глав правительств СНГ (25 октября 2019 г.) «О Стратегии обеспечения информационной безопасности государств — участников Содружества Независимых Государств» закрепляет принцип правового равенства участников информационного обмена [40].

Наш анализ выявил несколько ключевых принципов, которые должны лечь в основу эволюции информационной и психологической безопасности:

- Защита прав и свобод: соблюдать права человека и гражданина и обеспечивать уважение индивидуальных свобод.
- Верховенство закона: строго придерживаться правовых норм как основы всех мер.
- Защита граждан: усиление мер защиты граждан от вредоносной информации и психологического манипулирования.
- Свобода СМИ: гарантировать свободу прессы, не допуская ее злоупотреблений.
- Конфиденциальность: обеспечьте надежную защиту персональных данных, запретив их несанкционированный сбор, хранение, использование или распространение.

- Контролируемый доступ: строго ограничивайте доступ к конфиденциальной информации федеральным законодательством.
- Условные ограничения: разрешают ограничивать права личности исключительно в целях защиты конституционного строя, общественной морали, здоровья и государственной безопасности.
- Комплексные меры: Реализация системных правовых, организационных и информационных стратегий для обеспечения безопасности.
- Профилактический акцент: отдавайте приоритет профилактическим мерам, а не реактивным решениям.
- Сотрудничество и международное сотрудничество: развивать государственно-частное партнерство и соответствовать международным стандартам для создания устойчивой структуры безопасности.

Этот анализ показывает, что отсутствие единой правовой базы для информационной и психологической безопасности не только оставляет критические пробелы в регулировании, но и препятствует разработке эффективных, всеобъемлющих стратегий защиты граждан от меняющихся вызовов цифровой эпохи. Интегрируя конституционные гарантии, федеральные законы и международные стандарты, эта работа направлена на установление четкого стратегического направления. Она призывает к созданию надежной правовой доктрины, которая не только устраняет текущие уязвимости, но и предвидит будущие риски, тем самым обеспечивая более безопасную информационную среду для всех граждан. Такая структура будет служить как защитным щитом, так и руководством для постоянного совершенствования в условиях быстрых технологических и общественных изменений.

2.2 Деструктивное информационно-психологическое воздействие как общенациональная проблема в Российской Федерации

В нашем предыдущем обсуждении мы затронули вопросы, возникающие из-за информационного и психологического влияния. Здесь мы углубляемся в эти проблемы и изучаем стратегии для их эффективного решения.

В настоящее время значительная часть повседневной жизни граждан Российской Федерации протекает в сети. В отчете ВЦИОМ прогнозируется, что к 2024 году 73% населения будут ежедневно выходить в Интернет, проводя в среднем шесть часов в цифровой среде [57]. Этот всплеск онлайн-активности обусловлен цифровыми платформами, которые облегчают бизнес, общение, образование и досуг. Следовательно, люди постоянно погружаются в огромное море информации.

Однако этот непрерывный приток данных вызывает опасения относительно его влияния на поведение человека. Одной из основных проблем является подавляющее количество онлайн-контента, большая часть которого квалифицируется как «информационный мусор», включающий тривиальные, ненужные или ненадежные данные. С. А. Дружилов описывает это явление как «поток дисгармоничной, хаотичной, деструктивной информации, которая воздействует на человека в первую очередь через зрительные и слуховые каналы» [16]. Такое загрязнение не только снижает качество информации, но и негативно влияет на психику человека.

Ярким примером последствий недостоверной информации является распространение ошибочных сообщений о датах международных поездок, что встревожило многих россиян. Хотя Евгений Москвичев позже пояснил, что эти даты актуальны только для коммерческих перевозок, инцидент подчеркивает, как надежность источника может существенно влиять на общественные настроения. В сегодняшней глобальной цифровой сети как вредные, так и безвредные информационные отходы в значительной степени генерируются

самими пользователями. Эта реальность представляет собой две ключевые проблемы: неконтролируемое потребление информации и настоятельная необходимость разработки надежных контрмер против вводящего в заблуждение контента и психологического манипулирования.

Если глубже изучить индивидуальное воздействие, то особенно показательна концепция «модели человеческого мира» С.А. Дружилова [16]. Согласно этой концепции, каждый человек формирует ментальное представление реальности, которое включает:

- концептуальные компоненты: логическое рассуждение, причинно-следственный анализ, процессы изучения, анализа и синтеза.
- образные компоненты: эмоциональное восприятие и образная интерпретация.

Сбалансированное взаимодействие между этими компонентами имеет решающее значение для осмысленной обработки информации. Когда эмоциональный аспект затмевает логический анализ, риск стать жертвой манипулятивных тактик возрастает.

Современной проблемой, возникающей из этого дисбаланса, является феномен «клипового мышления» (происходит от термина «клип», означающего фрагмент). Эта форма познания подразумевает обработку информации короткими, яркими всплесками — привычка, выработанная неустанным потоком цифрового контента. Хотя быстрая доступность информации полезна, чрезмерная зависимость от фрагментированных данных может снизить способность к глубокому анализу и синтезу. Следовательно, общественность склонна отдавать предпочтение образам и эмоциональным сигналам, создавая уязвимости, которыми могут воспользоваться те, у кого есть скрытые мотивы.

В правовой сфере в Российской Федерации установлены меры противодействия вредоносному информационному и психологическому воздействию. Например, статья 152 Гражданского кодекса предоставляет гражданам право требовать возмещения ущерба, если их честь и репутация были

запятнаны недостоверной информацией. Это положение позволяет гражданам требовать в суде опровержения порочащих сведений, если распространитель не докажет их достоверность [13]. На практике такие дела рассматриваются с участием обеих сторон, с соблюдением принципов состязательности и равенства перед законом.

Этот анализ не только подчеркивает многогранные проблемы, вызванные информационной перегрузкой и психологическим манипулированием, но и подчеркивает необходимость скоординированных стратегий для смягчения этих рисков. Рассматривая, как цифровое поведение, такое как распространенная привычка «клипового мышления», подрывает критическое мышление, работа подчеркивает важность содействия медиаграмотности и устойчивости. Кроме того, она демонстрирует жизненно важную роль средств правовой защиты в защите индивидуального достоинства и общественного доверия в цифровую эпоху. Эти идеи прокладывают путь для будущих инициатив, направленных на баланс между быстрым доступом к информации и мерами по защите психологического благополучия.

Можно сказать, что для решения проблем информационного и психологического влияния требуется комплексный подход, который объединяет цифровую осведомленность, образовательные инициативы и надежные правовые рамки. Эта многогранная стратегия имеет важное значение для сохранения целостности общественного дискурса и обеспечения того, чтобы преимущества цифровой связи не приносили ущерба индивидуальному и общественному благополучию.

Статья 207.1 Уголовного кодекса предусматривает наказание — от штрафа до лишения свободы — за распространение заведомо ложной информации, создающей угрозу жизни и безопасности граждан [70]. Параллельно с этим Федеральный закон № 149-ФЗ, вступивший в силу 27 июля 2006 года, возлагает на владельцев сайтов ответственность за публикацию контента, способствующего преступной деятельности, разглашающего охраняемую

законом тайну, а также подстрекающего к терроризму или оправдывающего его [35].

Недавние изменения в уголовном и административном законодательстве также затронули кибербуллинг. Например, согласно статье 5.61 Кодекса об административных правонарушениях, лица, оскорбляющие людей в социальных сетях, могут быть оштрафованы на сумму от 5000 до 10 000 рублей [22]. Более того, статья 110.1 Уголовного кодекса направлена на кибербуллинг, включающий доведение до самоубийства или содействие в совершении таких действий, и предусматривает наказание в виде лишения свободы на срок от 8 до 15 лет — особенно суровое наказание, если жертвой является несовершеннолетний или правонарушение совершено в сети [70].

Хотя эти правовые инструменты жизненно важны для поддержания общественного порядка и борьбы с вредоносной информацией и психологическими манипуляциями, нормативно-правовая среда продолжает развиваться. По мере развития технологий возникают новые проблемы. Одной из таких проблем является растущая проблема «глубоких фейков» — контента, создаваемого с использованием нейронных сетей искусственного интеллекта для создания или изменения изображений, видео и аудио с высокой степенью реализма [64]. Аналогичным образом, «мусорные стримы» (или «мусорные стримы») — прямые трансляции на таких платформах, как Twitch или YouTube, демонстрирующие неэтичные действия с целью получения денежной выгоды, — еще больше усложняют цифровую среду. Примечательный инцидент произошел в 2021 году, когда сфабрикованная реклама, ложно обещающая денежное вознаграждение основателю Тинькофф Банка, подчеркнула потенциальную возможность глубинных фейков вводить общественность в заблуждение. Эти примеры иллюстрируют настоятельную необходимость в правовых механизмах, которые могут адаптироваться к таким сложным формам цифровой манипуляции и противодействовать им.

Стремительная эволюция искусственного интеллекта представляет собой дополнительный уровень сложности для правовых систем во всем мире. Законы изо всех сил пытаются идти в ногу с появлением новых технологий ИИ. Например, 28 марта 2023 года Илон Маск и другие эксперты подписали открытое письмо, призывающее приостановить разработку нейронных сетей из-за опасений по поводу их потенциального воздействия на общество. Это следует за такими вехами, как инцидент 2014 года, когда бот Юджин Густман прошел тест Тьюринга, убедив значительную часть оценщиков в его способностях, подобных человеческим. Несмотря на существенное государственное финансирование исследований ИИ во всем мире, правовая защита от потенциальных неблагоприятных информационных и психологических последствий технологий ИИ остается недостаточной. Поскольку технический прогресс продолжает повышать качество нашей жизни, крайне важно, чтобы правовые рамки развивались одновременно, чтобы смягчить непредвиденные риски.

В Российской Федерации Указ Президента от 10 октября 2019 года «О развитии искусственного интеллекта в Российской Федерации» определяет стратегические направления создания комплексной системы регулирования ИИ. Одной из ее ключевых задач является разработка этических стандартов взаимодействия человека с ИИ [49]. В ответ на вызовы, которые бросает ИИ, Альянс в области искусственного интеллекта в 2021 году представил «Кодекс этики в области искусственного интеллекта», в котором изложены ответственные практики разработки и применения ИИ [28]. Подчеркивается, что хотя текущие правовые меры обеспечивают основу для борьбы с вредоносной информацией и психологическими манипуляциями, они должны постоянно развиваться для решения новых и возникающих угроз. Интеграция надежных правовых санкций с инновационными подходами к регулированию имеет важное значение. По мере развития цифровых технологий правовые рамки должны быть динамичными и проактивными, гарантируя, что общественная безопасность и

социальное благополучие защищены как от традиционных кибернеправомерных действий, так и от новых форм цифровой эксплуатации.

Различные правовые положения в Российской Федерации направлены на противодействие распространению опасной дезинформации и поддержание общественной безопасности. Например, статья 207.1 Уголовного кодекса устанавливает санкции — от денежных штрафов до лишения свободы — для тех, кто распространяет заведомо ложную информацию, которая ставит под угрозу жизнь и безопасность граждан [70]. В том же ключе Федеральный закон № 149-ФЗ, принятый 27 июля 2006 года «Об информации, информационных технологиях и о защите информации», возлагает на операторов веб-сайтов ответственность за размещение контента, способствующего совершению преступных деяний, разглашающего государственную или иную секретную информацию, пропагандирующего или оправдывающего терроризм [35].

Недавние изменения в уголовном и административном законодательстве также затронули кибербуллинг. Согласно статье 5.61 Кодекса об административных правонарушениях, лица, которые оскорбляют других людей в социальных сетях, подвергаются штрафам в размере от 5000 до 10 000 рублей [22]. Более того, статья 110.1 Уголовного кодекса касается кибербуллинга, который включает в себя подстрекательство к самоубийству или содействие ему, особенно когда эти действия направлены на несовершеннолетних или происходят на цифровых платформах, и предусматривает для правонарушителей тюремное заключение сроком от 8 до 15 лет, при этом правовая ответственность наступает с 16 лет [70].

В то время как действующие законы имеют основополагающее значение для поддержания общественного порядка и смягчения вредоносной информации и психологического манипулирования, быстрое развитие цифровых технологий требует дальнейших правовых инноваций. К новым проблемам относятся «deepfake»-контент, созданный с использованием нейронных сетей ИИ для создания или изменения реалистичных мультимедийных представлений [64], и

«trash streams», которые относятся к прямым трансляциям на таких платформах, как Twitch или YouTube, где люди совершают неэтичные действия ради финансовой выгоды. Например, в 2021 году сфабрикованная реклама, ложно обещающая денежные вознаграждения основателю Тинькофф Банка, подчеркнула потенциал deepfakes для введения общественности в заблуждение. Растущая настороженность общественности по отношению к сомнительному цифровому контенту подчеркивает как достигнутый прогресс, так и необходимость усовершенствованных правовых механизмов.

Стремительное развитие искусственного интеллекта — это всемирное явление, которое бросает вызов правовым системам за пределами России. Например, 28 марта 2023 года Илон Маск и другие эксперты подписали открытое письмо, призывающее приостановить разработку нейронных сетей из-за опасений по поводу их потенциального воздействия на общество. Такие вехи, как достижение бота Юджина Густмана в 2014 году, который прошел тест Тьюринга, убедив 33% судей в своей человечности, демонстрируют быстрый прогресс ИИ. Несмотря на продолжающиеся государственные инвестиции в исследования ИИ, нынешняя правовая защита от информационного и психологического воздействия этих технологий остается недостаточной. Поскольку ИИ продолжает проникать в повседневную жизнь — создавая портреты, отвечая на вопросы и даже сочиняя статьи, — крайне важно, чтобы правовые рамки развивались для устранения этих непредвиденных рисков.

В ответ на это Российская Федерация предприняла шаги по регулированию развития ИИ. Указ Президента от 10 октября 2019 года «О развитии искусственного интеллекта в Российской Федерации» определяет основные направления по созданию комплексной нормативной базы ИИ, включая разработку этических стандартов взаимодействия человека и ИИ [49]. В дополнение к этому Альянс в области искусственного интеллекта в 2021 году представил «Кодекс этики в области искусственного интеллекта», в котором изложены ответственные практики использования и развития ИИ [28].

В этой работе подчеркивается, что хотя существующие правовые меры обеспечивают важнейшую основу для борьбы с вредоносным цифровым контентом и психологическими манипуляциями, быстрое появление новых технологий требует постоянных законодательных инноваций. Интеграция надежных правовых санкций с адаптивными стратегиями регулирования имеет важное значение для обеспечения того, чтобы общественная безопасность не была поставлена под угрозу по мере развития цифровых платформ. Постоянно обновляя правовые рамки для решения как традиционных киберпреступлений, так и новых угроз, таких как deepfakes и неэтичные прямые трансляции, политики могут лучше защитить общество от сложных проблем, создаваемых современной цифровой коммуникацией.

2.3 Правовые механизмы защиты от деструктивного информационно-психологического воздействия

В сегодняшнюю цифровую эпоху были разработаны различные правовые инструменты для защиты людей от неблагоприятных последствий вредоносной информации и психологической манипуляции. Чтобы понять эти защитные меры, необходимо изучить методы регулирования, используемые правовыми системами.

Теория права определяет методы регулирования как «совокупность приемов и способов воздействия на субъекты общественных отношений» [3]. Эти методы обычно подразделяются на две категории:

– Императивные методы: они основаны на иерархическом подходе, где участники подвергаются строгому контролю без дискреционных полномочий. Императивные методы подразделяются на: Запретительные меры: прямые запреты на определенные виды поведения. Обязательные меры: требования, которые обязывают к определенным действиям. Этот метод характеризуется отсутствием

гибкости, гарантируя, что предписанные правила будут соблюдаться без отклонений [3].

– Факультативные методы. В отличие от императивного подхода, факультативные методы основаны на принципе равенства сторон. Они предоставляют индивидуумам определенную степень выбора в своих действиях. Например, часть 2 статьи 14 Закона «О защите детей от информации, причиняющей вред их здоровью и развитию» предоставляет несетевым интернет-ресурсам право самостоятельно устанавливать возрастные ограничения на информационную продукцию [38].

Действующие правовые нормы используют ряд запретов, направленных на ограничение вредоносной информации и смягчение психологического влияния. Известные примеры включают:

- Злоупотребление свободой СМИ: Статья 4 Закона о средствах массовой информации запрещает злоупотребление свободой СМИ, предотвращая действия, которые могут нанести вред общественному дискурсу [45].
- Распространение незаконной информации: Часть 6 статьи 10 Закона об информации запрещает распространение контента, который является противоправным [35].
- Ограничения в отношении иностранных СМИ: Часть 7 статьи 10 Закона об информации ограничивает распространение сообщений и материалов иностранными средствами массовой информации, действующими в качестве иностранных агентов, или созданными ими российскими организациями, если их происхождение явно не раскрыто [35].
- Ложная и недобросовестная реклама: Часть 1 статьи 5 Закона о рекламе запрещает недобросовестную рекламу, которая может ввести в заблуждение или нанести вред потребителям [36].

В дополнение к этим запретам, на различных цифровых субъектов налагаются определенные правовые обязательства для обеспечения соблюдения и защиты общественных интересов. К ним относятся:

- «Организаторы распространения информации в сети Интернет (ОРИ): регулируются статьей 10.1;
- Операторы поисковых систем: в соответствии со статьей 10.3;
- Агрегаторы новостей: регулируются статьей 10.4;
- Владельцы аудиовизуальных услуг: регулируются статьей 10.5;
- Операторы социальных сетей: подпадают под действие статьи 10.6» [35].

Третья стратегия регулирования предполагает выдачу разрешений для уточнения правового статуса лиц и организаций в сфере информационного права. Например, статья 15.1-2 Закона об информации позволяет гражданам обращаться в прокуратуру субъекта Российской Федерации с требованием принять меры по удалению или блокированию клеветнической и ложной информации, в частности, контента, ложно обвиняющего их в совершении преступления, размещенного в сети Интернет [35].

Работа предлагает существенные сведения о том, как эти разнообразные правовые стратегии взаимодействуют для создания сбалансированной цифровой среды. Она подчеркивает необходимость постоянной адаптации правовых механизмов для решения возникающих проблем в цифровом пространстве. По мере развития технологий должны развиваться и наши нормативные рамки, чтобы гарантировать, что защитные меры остаются надежными и эффективными. Эта всеобъемлющая оценка подчеркивает важность поддержания динамической правовой системы, способной противостоять как традиционным, так и новым формам цифровой эксплуатации.

Механизмы правовой защиты вытекают из методов правового регулирования — по сути, комплекса правовых инструментов, призванных

управлять и упорядочивать общественные отношения. Можно выделить несколько основных правовых механизмов:

- введение правовых запретов и ограничений: например, статья 4 Закона о средствах массовой информации запрещает «злоупотребление свободой массовой информации» [45].
- регулирование оборота отдельных видов информационной продукции: Примером может служить статья 13 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». В данной статье установлено, что информационная продукция, содержащая указанный контент, не должна транслироваться на телевидении и радио в период с 4 до 23 часов по местному времени, за исключением случаев, когда доступ осуществляется через платные сервисы, проверяющие возраст зрителя путем ввода кодов или совершения иных подтверждающих действий [38].
- закрепление ответственности за субъектами информационных отношений: еще один механизм предполагает разграничение обязанностей различных субъектов, участвующих в распространении информации. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет ответственность различных субъектов цифровой сферы, в том числе:

1) Организатор распространения информации в сети Интернет (статья 10.1);
2) Операторы поисковых систем (статья 10.3);
3) Агрегаторы новостей (статья 10.4);
4) Владельцы аудиовизуальных услуг (статья 10.5); а также
5) Владельцы социальных сетей (статья 10.6) [35].

– возрастная классификация и маркировка информационной продукции: Еще одним механизмом является возрастная классификация и маркировка контента. Статья 12 Федерального закона от 29 декабря 2010 г. № 436-ФЗ предписывает маркировать информационную продукцию в соответствии с возрастом, например, для детей до шести лет (0+), для лиц в возрасте шести лет (6+), двенадцати лет (12+), шестнадцати лет (16+) и полностью запрещенную для несовершеннолетних (18+) [38]. Эта диспозитивная мера гарантирует, что пользователи получают четкое уведомление о возрастном соответствии при доступе к веб-сайтам или определенному контенту.
– судебная экспертиза информационной продукции Федеральный закон от 31 мая 2021 г. № 73-ФЗ «О государственной судебно-экспертной деятельности» [54] является основной правовой базой, регулирующей экспертную деятельность в России. Правоохранительные органы могут запрашивать проведение этих экспертиз вне формальных процессуальных действий.
– идентификация цифровых пользователей Важнейшей мерой борьбы с вредоносной информацией является надлежащая идентификация лиц, пользующихся цифровыми сервисами. Статья 2 Федерального закона от 29 декабря 2022 г. № 572-ФЗ определяет идентификацию как комплекс мер, направленных на установление и проверку персональной информации путем сопоставления ее с уникальным идентификатором [37].
– ограничение доступа к противоправному контенту Удаление или ограничение доступа к противоправному контенту является еще одним основополагающим правовым инструментом. Федеральный закон «Об информации, информационных технологиях и о защите информации» (от 27 июля 2006 г. № 149-ФЗ) описывает эти механизмы. Например, в 2012 г. статья 15.1 ввела реестр доменных

имен, в который были включены все интернет-ресурсы, нарушающие российское законодательство [35].

– установление юридической ответственности
  Для предотвращения и наказания вредоносного поведения устанавливается юридическая ответственность за правонарушения, посягающие на информационно-психологическую безопасность (ИПБ). Как подробно описано ранее, правовая база применяет уголовную, административную и гражданско-правовую ответственность для решения различных правонарушений, связанных с деструктивным информационно-психологическим воздействием.
– регулирование мер контрпропаганды
  Меры контрпропаганды подразумевают принятие мер, которые напрямую противостоят вредоносной пропаганде определенных субъектов. Хотя российское законодательство не предлагает всеобъемлющего регулирования в этой области, в Федеральном законе «О противодействии терроризму» [55] и других административных законах существуют разрозненные правовые положения, которые помогают смягчить распространение деструктивных сообщений.
– продвижение цифровой грамотности и культуры информационной безопасности
  Наконец, законодательные инициативы также направлены на развитие цифровой грамотности и формирование культуры информационной безопасности. Привитие привычки осознанного, ответственного потребления информации с раннего возраста рассматривается как необходимое условие. В соответствии с этим 28 апреля 2023 года Правительством Российской Федерации была утверждена Концепция информационной безопасности детей. В данной концепции определены такие задачи, «как организация мероприятий по повышению грамотности детей в области информационной

безопасности, формирование навыков законопослушного и ответственного поведения в цифровой среде, воспитание способности к самостоятельному и ответственному потреблению информационных продуктов» [26].

В совокупности обсуждаемые механизмы образуют комплексную правовую основу, направленную на смягчение воздействия вредоносной информации и психологического манипулирования, тем самым защищая общественные интересы в современную цифровую эпоху.

Описанные здесь защитные меры имеют решающее значение для формирования перспективных стратегий, особенно тех, которые направлены на защиту молодого поколения от вредоносного контента и ненадлежащего психологического влияния. Тем не менее, стремление к ответственному потреблению информации должно охватывать все возрастные группы, гарантируя, что взрослые будут в равной степени подготовлены к навигации в сложном цифровом ландшафте.

Хотя в Российской Федерации в настоящее время отсутствует единый, всеобъемлющий нормативный акт, посвященный исключительно информационной и психологической безопасности, существующие правовые инструменты продемонстрировали значительную эффективность. Тем не менее, в свете быстрого развития нашего информационного общества и технологических достижений, крайне важно постоянно разрабатывать и внедрять новые методы. Как подчеркивалось ранее, российское правительство активно усиливает свои правовые гарантии для решения этих новых проблем.

В этой работе подчеркивается важность динамичной и адаптивной правовой системы, которая не только реагирует на текущие угрозы, но и предвидит будущие риски во все более взаимосвязанном цифровом мире.

Таким образом, во второй главе была проведена комплексная оценка правовых основ обеспечения информационно-психологической безопасности и рассмотрены принципы, лежащие в её основе. Выявлено, что масштабы и

многообразие деструктивного информационно-психологического воздействия превращают эту проблему в общенациональную и требуют системного подхода со стороны государства. Анализ правовых механизмов, используемых для противодействия подобным угрозам, показал, что несмотря на наличие отдельных норм и инструментов, существующее законодательство нуждается в дальнейшем совершенствовании и четкой регламентации сферы информационно-психологической безопасности. Всё это указывает на необходимость формирования комплексных мер защиты, направленных не только на пресечение негативного воздействия, но и на повышение правовой и информационной грамотности граждан, а также на развитие межведомственного взаимодействия в данной сфере.

Выводы по Главе 2.

Вторая глава посвящена практическому анализу текущей ситуации, связанной с активностью деструктивных молодёжных объединений на территории Российской Федерации. В ней автор обобщает статистические данные, информацию правоохранительных органов и результаты деятельности организаций, занимающихся мониторингом интернет-пространства, таких как Лига безопасного интернета. Представленные цифры свидетельствуют о масштабности проблемы — охват деструктивных сообществ достигает миллионов пользователей, в том числе несовершеннолетних.

Показано, что основным инструментом вовлечения молодёжи в разрушительные субкультуры становятся социальные сети, мессенджеры и анонимные площадки, где пропагандируется насилие, суицид, нацизм, сатанизм и иные формы деструктивной идеологии.

Таким образом, глава 2 выявляет не только высокую степень угрозы, которую представляют деструктивные субкультуры, но и уязвимость действующей системы профилактики. Сделанный вывод — необходима модернизация мер реагирования, усиление информационной безопасности и выработка чётких алгоритмов межведомственного взаимодействия.

Глава 3 Современные проблемы и перспективы совершенствования правового обеспечения информационной безопасности от деструктивного психологического воздействия в РФ

3.1 Исследование последствий деструктивного информационно-психологического воздействия на граждан РФ

Ранее статистика ВЦИОМ показывала, что российское общество в основном следует гибридной модели потребления медиа, при этом основным источником информации становится Всемирная паутина. Фактически, опрос, проведенный в мае 2023 года, показал, что 73% респондентов заходят в Интернет практически ежедневно [57]. Поскольку традиционные бумажные СМИ постепенно теряют свое влияние, все больше СМИ переходят на онлайн-платформы. К сожалению, этот сдвиг также предоставляет агрессивным акторам новые каналы для оказания деструктивного информационного и психологического воздействия на граждан.

Фейковые новости остаются актуальной проблемой. В предыдущих главах затрагивалась их значимость, и их общественное влияние продолжает оставаться глубоким. Например, организация по проверке фактов Lapsha Media выделила три ключевые области, уязвимые для фальсификаций: «здравоохранение, специальные военные операции, а также политика и национальная безопасность» [65]. Кроме того, опрос Rambler&Co, проведенный с 1 по 4 марта 2023 года с участием 458 525 человек, был направлен на то, чтобы «определить, могут ли граждане России различать правду и ложь» [19]. Результаты показали, что «62% респондентов считают, что могут распознать фейковые новости. Они выделили беспристрастность (59%), наличие ссылок на источники информации (18%), лаконичный и профессиональный язык (10%), профессиональный стиль (7%) и отсутствие эмоционального тона (6%) как показатели достоверной информации» [19]. Однако важно отметить, что этот опрос охватил лишь часть

от общей численности населения России, составляющей около 146 миллионов человек.

Борьба с фейковыми новостями не оставляется на волю случая. Сеть компаний по проверке фактов, таких как Lapsha Media, созданная АНО «Диалог регионов» в 2022 году, активно отслеживает и проверяет информацию, предупреждая общественность о неточностях. Кроме того, различные интернет-платформы теперь занимаются проверкой веб-сайтов и контента, публикуемого отдельными лицами. Несмотря на эти усилия, многие граждане остаются неосведомленными об этих ресурсах, а некоторые менее способны контролировать психологическое воздействие вводящей в заблуждение информации.

Примером может служить полемика вокруг новых правил поездок, объявленных в январе 2023 года. Lenta.ru опубликовала пост в ВК, в котором подробно описывалось введение обязательного бронирования дат и времени поездок для «всех транспортных средств без исключения» [18]. Хотя многие пользователи отреагировали с энтузиазмом, меньшая группа выразила скептицизм. Более того, ситуация усугубилась «интернет-троллями» — лицами, которые намеренно провоцируют и разжигают конфликты. Эти тролли, сродни субъектам, стремящимся дестабилизировать общественный порядок, в конечном итоге лишились своих аккаунтов в социальных сетях, вероятно, из-за жалоб пользователей или администраторов групп.

Можно сказать, что хотя граждане России в основном потребляют информацию через Интернет и, таким образом, в значительной степени подвергаются воздействию как достоверного, так и вредоносного контента, совместные усилия проверяющих факты, медиаплатформ и информированных пользователей помогают смягчить неблагоприятные последствия фейковых новостей и агрессивного поведения в Интернете.

В 2022–2023 годах один широко распространенный фейк утверждал о начале второй мобилизации [61]. Наши исследования показывают, что такие лжи

редко бывают случайными; они, как правило, распространяются с четкой целью. В большинстве случаев преступник использует тревожные события — как глобальные, так и внутренние — для создания паники. Например, в феврале 2023 года новости о второй мобилизации вызвали неоднозначную реакцию. Некоторые люди отвергли это заявление с помощью логичных контраргументов, в то время как другие впали в состояние паники, поскольку информация быстро распространилась по социальным сетям. В конечном итоге, когда государственные органы опровергли эту историю, общественное беспокойство несколько утихло.

Эти инциденты показывают, что фейковые новости распространяются не только традиционными медиаканалами. Участники, включая «интернет-троллей», также используют разделы комментариев для дальнейшего распространения ложной информации — аналогично тактике, наблюдаемой в недавнем посте о новых требованиях к поездкам за границу.

Помимо общенациональных нормативных актов, важную роль играют и локальные соглашения. К ним относятся условия предоставления услуг, принимаемые при регистрации, и особые правила, устанавливаемые отдельными интернет-сообществами. Например, в 2020 году в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» была введена статья 10.6. Эта статья обязывает владельцев веб-сайтов не допускать использования своих платформ для распространения нецензурной лексики или подстрекательского контента, который может спровоцировать конфликты, а нарушения могут повлечь за собой дисциплинарную, уголовную, гражданскую или административную ответственность [35]. Аналогичным образом социальные сети, такие как ВКонтакте, применяют собственные правила, нарушения которых могут привести к блокировке аккаунта.

Важно также отметить, что негативное информационно-психологическое воздействие не ограничивается интернетом. Например, однажды радио- и

телеканалы транслировали фейковые предупреждения о ракетных ударах по таким городам, как Белгород, Воронеж, Уфа и Казань [73]. Влияние этой дезинформации было разным: жители Уфы заподозрили технический сбой, так как оповещение пришло только с одной местной станции (Comedy Radio), тогда как жители приграничных регионов испытали повышенное чувство страха. Однако граждане, живущие дальше от границы с Украиной, реагировали спокойнее и оценивали ситуацию более рационально. Благодаря оперативному вмешательству МЧС истинный характер угрозы был быстро прояснен.

Обеспечение безопасности государственных СМИ регулируется Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» (26 июля 2017 г. № 187-ФЗ). Статья 4 этого закона устанавливает руководящие принципы — законность, непрерывность, комплексность, приоритетность предотвращения компьютерных атак, а также определяет «критическую информационную инфраструктуру» как информационные системы, сети электросвязи и автоматизированные системы управления жизнеобеспечением [42]. Данный закон не только разъясняет права и обязанности субъектов критической инфраструктуры, но и устанавливает конкретные стандарты безопасности, которые более подробно изложены в Приказе ФСТЭК от 25 декабря 2017 г. № 239, в котором прописаны требования к защите значимых объектов этой инфраструктуры [48].

Параллельно Уголовный кодекс усиливает эти защитные меры. Статья 274.1 предусматривает уголовную ответственность за любое несанкционированное вмешательство в критически важную информационную инфраструктуру или за нарушения протоколов, регулирующих хранение, обработку и передачу защищенных данных [70]. Эти положения гарантируют, что даже в случае попытки взлома государственные информационные системы будут защищены под строгим правовым надзором. Кроме того, любое

несоблюдение этих требований безопасности государственными служащими влечет за собой правовые последствия.

Напротив, коммерческие радио- и телесети зачастую демонстрируют менее строгую безопасность, что является следствием недостаточной подготовки сотрудников и возможного отсутствия специализированных антихакерских процедур. Более того, вторжение в системы вещания карается статьей 13.18 Кодекса об административных правонарушениях, которая предусматривает штрафы «в размере от 500 до 1000 рублей для физических лиц, от 1000 до 2000 рублей для должностных лиц и примерно от 10 000 до 20 000 рублей для юридических лиц» [22].

Инцидент с ложной тревогой еще раз иллюстрирует устойчивость системы. Несмотря на разную реакцию в разных регионах, многие граждане быстро распознали обман — ответ, которому способствовали хорошо зарекомендовавшие себя протоколы гражданской обороны, использующие четкие сигналы, такие как «воздушная тревога» и «воздушная тревога отбой» [20]. В реальных чрезвычайных ситуациях эти оповещения транслировались бы по всем доступным каналам, тем самым повышая общественную готовность и сопротивляемость обманным приемам.

Этот анализ выявляет существенное несоответствие между системами безопасности государственных и коммерческих медиаканалов. Надежная правовая защита и технические меры, применяемые к государственным информационным системам, подчеркивают важность всестороннего обучения и систематических протоколов — элементов, которые менее распространены в коммерческом секторе. Такие уязвимости требуют целенаправленных улучшений в стратегиях кибербезопасности частных вещателей для обеспечения единообразной защиты во всех медиаканалах.

Представленная здесь работа освещает не только текущие правовые механизмы, защищающие критически важную информационную инфраструктуру, но и текущие проблемы, создаваемые развивающимися

киберугрозами. Она подчеркивает необходимость постоянного совершенствования правовых и технических мер по защите публичной информации и поддержанию психологической безопасности в цифровую эпоху. Дальнейшее развитие политики должно быть сосредоточено на устранении этих пробелов путем принятия расширенных программ обучения, обновления протоколов безопасности и совершенствования правовых рамок для соответствия быстро меняющимся технологическим ландшафтам.

Ранее мы рассмотрели, как такие методы, как убеждение и внушение, используются для оказания деструктивного информационного и психологического воздействия — тактика, используемая в разных странах, включая Российскую Федерацию. Эти методы проявляются в создании фейковых статей, вводящих в заблуждение постов, обманчивой рекламы и даже в том, как актер произносит речь. Пропагандисты часто призывают к определенным действиям, унижают своих оппонентов или взывают к жалости, чтобы повлиять на общественное мнение. Как обсуждалось ранее, эффективность этих методов во многом зависит от уровня образования и осведомленности целевой аудитории.

В сфере информационной войны — как на международном, так и на внутреннем уровне — преобладающими стратегиями являются распространение ложной информации и проведение хакерских атак. Тематическая реклама также стала значимым инструментом. Например, с начала Специальной военной операции появилось множество фрагментов целевой рекламы. Один из ярких случаев связан с видеороликом, призывающим российских солдат сдаться, обещающим им безопасность на Украине [72]. Хотя многие россияне выразили скептицизм, особенно в первые дни операции, вызванное беспокойство было значительным. После многочисленных жалоб Роскомнадзор заблокировал многие из этих веб-сайтов, а последующие усилия по разоблачению еще больше подорвали доверие к такому контенту, что привело к в значительной степени негативному восприятию среди общественности.

Из этих наблюдений следует несколько выводов. Во-первых, способность российских граждан противостоять фейковым новостям зависит от их личных обстоятельств, психологического склада, уровня образования и осведомленности. Во-вторых, общественный надзор играет решающую роль в противодействии дезинформации. Наконец, Интернет выделяется как наиболее широко используемая платформа для доступа к информации, фактически создавая цифровое пространство, где права граждан защищены лишь частично.

3.2 Развитие институциональных систем обеспечения информационно-психологической безопасности

Эксперты подразделяют общую систему безопасности на две основные подсистемы: государственную и негосударственную. Федеральный закон «О безопасности» (28 декабря 2010 г. № 390-ФЗ) дает основу для такого анализа, определяя аппарат безопасности как включающий Президента, палаты Федерального Собрания, Правительство и различные федеральные органы исполнительной власти [41]. Хотя все эти органы помогают защищать общественные отношения, определенная подгруппа несет основную ответственность. К ним относятся федеральные учреждения, такие как Министерство связи, связи и массовых коммуникаций, Роскомнадзор, Министерство внутренних дел, ФСБ, Министерство обороны и Министерство иностранных дел.

Центральную роль в формировании государственной политики и регулировании правовых вопросов в сфере информационных технологий, массовых коммуникаций и СМИ играет Министерство развития, связи и массовых коммуникаций [52]. В настоящее время это министерство возглавляет инициативы по защите детей от потенциально опасной информации. Среди его ключевых проектов — разработка комплексной концепции цифровой защиты. Эта стратегия призвана оградить несовершеннолетних от информационных

угроз, поощрять безопасные действия в сети и вооружить их навыками выявления мошеннических схем [32]. Такие меры жизненно важны для укрепления устойчивости молодого поколения к деструктивным информационным воздействиям.

Кроме того, министерство отвечает за установление требований безопасности к сетям связи для предотвращения несанкционированного доступа. В этом качестве оно тесно сотрудничает с надзорным органом, а именно Роскомнадзором [52]. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, более известная как Роскомнадзор, напрямую контролирует потоки информации как в электронных, так и в традиционных средствах массовой информации [53]. Его полномочия, изложенные в постановлении Правительства РФ от 16 марта 2009 года «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций», включают в себя контроль за соблюдением законодательства о защите детей от вредоносного контента, обеспечение соблюдения ограничений на распространение информации в телекоммуникационных сетях (включая сеть Интернет) и регулирование теле- и радиовещания [53].

Этот анализ подчеркивает комплексную правовую стратегию, в которой государственные и негосударственные механизмы работают в тандеме для противодействия негативной информации и психологическому влиянию в цифровую эпоху. Исследование подчеркивает, как целевые обязанности среди ключевых федеральных органов не только усиливают текущие защитные меры, но и указывают на области для будущего улучшения. Например, сотрудничество между Министерством развития, связи и массовых коммуникаций и Роскомнадзором иллюстрирует скоординированные усилия по совершенствованию протоколов цифровой безопасности.

Работа раскрывает критическую роль этих регулирующих институтов в построении надежной среды безопасности, особенно по мере того, как цифровые

угрозы становятся все более изощренными. Она также подчеркивает важность непрерывного развития и адаптации правовых механизмов для решения возникающих проблем. В конечном счете, укрепление этого комплексного подхода имеет жизненно важное значение для защиты общественных отношений и обеспечения психологической безопасности населения в условиях все более сложного цифрового ландшафта.

Роскомнадзор играет важнейшую роль в мониторинге цифрового ландшафта, отслеживая доменные имена, указатели сайтов и сетевые адреса, которые распространяют информацию, запрещенную в Российской Федерации, и активно ограничивает доступ к таким ресурсам [53]. Одной из основных мер является блокировка веб-сайтов, которые распространяют ложную информацию или подстрекают к незаконной деятельности и массовым преследованиям.

В сфере киберпреступности Министерство внутренних дел возглавляет борьбу с правонарушениями в сфере информационной безопасности. Департамент осуществляет проверку сетей связи на предмет выявления запрещенного контента, способного нанести ущерб информационной и психологической безопасности граждан, а также занимается административными правонарушениями и противодействием терроризму и экстремизму [47].

Напротив, Федеральная служба безопасности (ФСБ) посвящает свои операции защите информационных систем и связанных с ними инфраструктур. С помощью обширных разведывательных и контрразведывательных операций ФСБ стремится защитить государство и общество от вредоносной информации и психологического воздействия. Ее контрразведывательная деятельность специально нацелена на усилия иностранных спецслужб и организаций, которые стремятся подорвать безопасность Российской Федерации [43].

Министерство обороны также решает задачи психологического воздействия. Как указано в части 7 пункта 40 Указа Президента от 16 августа 2004 г. (№ 1082), на Министерство возложены функции по совершенствованию

системы вооруженных сил, в том числе по реализации мер по защите личного состава от психологических воздействий противника [7]. Кроме того, на Министерство возложены функции сохранения и развития патриотических традиций, противодействуя тем самым деструктивному психологическому воздействию как из внешних, так и из внутренних источников.

На международной арене Министерство иностранных дел призвано обеспечивать внешнюю политику России путем управления информационными потоками и противодействия утечкам негативных данных о стране и международных организациях. Его основная функция в сфере информационно-психологической безопасности — отстаивание национальных интересов России на международном уровне и содействие международному сотрудничеству в борьбе с информационными угрозами [8].

Анализ нормативной базы показывает, что каждое из этих агентств вносит свой уникальный вклад в поддержание информационной и психологической безопасности. Хотя среди экспертов существует консенсус относительно того, что специализированное агентство, занимающееся исключительно противодействием вредоносной информации и психологическому влиянию, не является необходимым, учитывая многогранный характер проблемы, крайне важно повышать экспертизу в существующих структурах. Мы поддерживаем эту точку зрения, но подчеркиваем необходимость специализированных программ обучения. В частности, создание специализированного подразделения в Министерстве внутренних дел, укомплектованного экспертами в области информационных технологий, психологии и профилирования, могло бы значительно улучшить время реагирования на агрессивные действия и способствовать разработке целевых стратегий.

В этой работе подчеркивается, как межведомственный подход обеспечивает комплексную защиту от сложных угроз, создаваемых вредоносной информацией и психологическими манипуляциями. Она подчеркивает важность непрерывной эволюции правовых и операционных рамок для соответствия

темпам технологических достижений и киберугроз. Интеграция специализированных навыков в существующие структуры — это не просто операционное улучшение, а стратегическая необходимость, гарантирующая, что государство останется устойчивым в эпоху, когда информационная война становится все более распространенной.

Помимо государственной поддержки, Россия также получает выгоду от надежной неправительственной сети, которая вносит значительный вклад в обеспечение информационной и психологической безопасности. Эта сеть включает в себя СМИ, общественные объединения, образовательные учреждения, ИТ-компании и активных граждан. Как подчеркивалось ранее, общественный надзор подтверждает, что неправительственные организации играют жизненно важную роль в этой сфере. Не только компании, но и отдельные граждане могут применять агрессивную тактику — например, использовать инструменты социальных сетей для подачи дополнительных жалоб — для противодействия вредоносному поведению в Интернете.

Ярким примером в этой сети является так называемый «киберштаб», сообщество добровольцев, занимающихся мониторингом онлайн-контента на предмет нарушений. Эта группа уполномочивает региональные транзитные агентства действовать против нарушений в сфере информации. В их обязанности входит проверка интернета на наличие скрытого или запрещенного контента, например, сообщений, рекламирующих запрещенные вещества, подстрекающих к насилию, провоцирующих самоубийство или распространяющих откровенные материалы 18+ и детской порнографии, а также оперативное уведомление администраторов социальных сетей о блокировке контента или прокуратуры, когда это необходимо.

Повышение роли киберштабов в рамках общественной безопасности может значительно улучшить обнаружение и реагирование на цифровые нарушения. Для достижения этого необходимо разработать структурированную систему, которая четко определяет методы, функции и операционные

требования для кибершабов. Хотя участие в таких инициативах остается добровольным и доступным независимо от формального образования, эффективное вмешательство в сферу информационной и психологической безопасности требует привлечения специалистов, обладающих опытом в области ИТ и психологии. Более того, кибершаб должен отдавать приоритет образовательным мероприятиям, включая лиц, которые профессионально обучены определять признаки вредоносной информации и ее психологические эффекты.

Параллельно с этим решающее значение имеет повышение качества психологической помощи, поскольку психологическая устойчивость граждан является ключевой защитой от пагубных информационных влияний. Образовательным учреждениям следует уделять особое внимание, учитывая, что дети часто неохотно обращаются за психологической помощью из-за чувства незащищенности или страха. Исследования показывают, что подростки особенно уязвимы к негативному влиянию цифровой среды. Следовательно, сталкиваясь с семейными проблемами, давлением со стороны сверстников или влиянием деструктивных сообществ, подростки должны иметь доступные механизмы поддержки. В нашу современную эпоху проактивная государственная «здоровая пропаганда» — или надежная психологическая поддержка — имеет важное значение. Также существует острая необходимость в законодательстве о психологической помощи для защиты граждан от мошенников, выдающих себя за профессиональных психологов. Кроме того, были разработаны образовательные программы для поощрения осознанного потребления информации среди молодежи. Одной из существенных проблем, выявленных для нового поколения, является «клиповое мышление», при котором способность проводить глубокий анализ ставится под угрозу, что приводит к чрезмерной зависимости от эмоциональных сигналов и делает людей более восприимчивыми к манипуляциям. Эта проблема еще больше усугубляется тем, что дети все больше времени проводят в Интернете [32].

Эта работа подчеркивает критическое взаимодействие между государственными инициативами и неправительственными усилиями. Она подчеркивает необходимость специализированного обучения, скоординированной волонтерской деятельности и расширенных систем психологической поддержки для решения меняющихся проблем, возникающих в цифровую эпоху.

В итоге, развивая государственную и негосударственную систему обеспечения информационно-психологической безопасности мы сможем защитить российское общество от деструктивно-информационно-психологического воздействия.

3.3 Стратегические приоритеты совершенствования российского законодательства об информационно-психологической безопасности

Наше исследование деструктивного информационно-психологического воздействия выявило несколько ключевых направлений, в которых может быть усилена правовая защита граждан России. Во-первых, существует острая необходимость в разработке комплексного Федерального закона об информационно-психологической безопасности. Такое законодательство проясняло бы характер информационно-психологической деятельности, устанавливало бы руководящие принципы для органов безопасности и четко определяло бы угрозы, с которыми сталкиваются граждане России. Тем самым оно обеспечило бы структурированную основу, детализирующую роли и обязанности как государственных, так и негосударственных органов, а также определило бы конкретные сферы влияния, требующие защиты.

В дополнение к этому, необходимо создать «Информационный код». Анализ воздействия деструктивного информационно-психологического воздействия, подкрепленный исследованиями ВЦИОМ, показывает, что россияне проводят значительное количество времени во Всемирной паутине.

Это цифровое пространство, часто плохо регулируемое, эксплуатируется злоумышленниками, которые нацеливаются на пользователей с помощью обманных комментариев, глубоких фейков и ложных ссылок. Распространенные тактики включают взлом личных аккаунтов для выдачи себя за других лиц, отправку сомнительных ссылок родственникам и распространение нелестных фотографий или видео, все это может привести к финансовым потерям или репутационному ущербу. Несмотря на растущую осведомленность среди пользователей, такие кибератаки продолжают происходить.

Еще одной важной мерой является создание Федерального закона «О психологической помощи». Хотя попытки регламентировать психологическую помощь впервые были выдвинуты еще в 1993 году, более ранние законопроекты были отклонены в пользу решения проблемы психиатрической помощи. В 2022 году эксперты МГУ и МЧС предложили две версии этого законопроекта.

Кроме того, жизненно важным остается продвижение «здоровой пропаганды» психологической помощи. Хотя отношение общества к психологии улучшилось за последние два десятилетия, многие люди все еще не решаются обратиться за помощью, предпочитая игнорировать свои проблемы. Наконец, существует значительная потребность в просвещении общественности по вопросам осознанного потребления Интернета. Это включает в себя обучение молодого поколения сбалансированной обработке информации — не перегружая свой разум — и продуктивному использованию Всемирной паутины. Такое просвещение имеет решающее значение для предотвращения возникновения «клипового мышления» — явления, при котором люди теряют способность определять суть информации, критически анализировать ситуации и становятся уязвимыми для манипуляций. Эта проблема касается не только детей; многие взрослые, которые проводят много времени в социальных сетях, таких как TikTok и Vkontakte, также демонстрируют фрагментарное мышление. Хотя просмотр коротких видеороликов по своей сути не вреден, чрезмерное потребление может привести к клиповому мышлению и пустой трате времени.

Вместо ограничения доступа к этим платформам — меры, которая часто имеет обратный эффект, делая запретное более привлекательным, — мы предлагаем использовать мягкую силу. Это может включать интерактивные мероприятия в общеобразовательных учреждениях, направленные на снижение зависимости от гаджетов во время перемен, и одновременное развитие у детей способности выражать свое мнение и участвовать в содержательных дискуссиях [32].

Проведённый анализ свидетельствует о том, что деструктивные молодёжные субкультуры представляют собой реальную угрозу нравственному и психоэмоциональному становлению несовершеннолетних. Указанные неформальные объединения, действующие под названиями «АУЕ», «Колумбайн», «МКУ», а также так называемые «группы смерти», направлены на подрыв устоявшихся моральных норм и традиционных ценностных ориентиров в молодёжной среде.

Согласно статистическим данным, обнародованным Лигой безопасного интернета по итогам 2022 года, к информационному влиянию подобных сообществ были причастны порядка 10,5 миллионов несовершеннолетних пользователей. Представители указанной организации подчёркивают, что современные цифровые платформы нередко становятся каналами распространения девиантных установок, включая апологию насилия, социопатического поведения, пропаганду оккультных практик, наркомании, экстремизма, а также идеологий, основанных на расовой и национальной нетерпимости.

Особую опасность представляет популяризация образов серийных и массовых убийц, романтизация суицидального поведения, а также искажение понятий ценности человеческой жизни через призму агрессии и ритуального насилия. Эти тенденции формируют у подростков искажённое восприятие социальной реальности, способствуя распространению асоциальных форм поведения и психологической дестабилизации [4].

Не менее острой является необходимость усовершенствования нормативной базы, регулирующей искусственный интеллект. На протяжении всего нашего исследования неоднократно высказывались опасения относительно того, что нейронные сети могут стать инструментами информационной и психологической манипуляции и даже обрести статус независимых субъектов. Яркий пример произошел на Sony World Photography Awards 2023, когда немецкий фотограф Борис Эльдагсен представил фотографию, созданную нейронной сетью, чтобы проверить, могут ли судьи различать реальные и искусственные изображения. В конечном итоге работа, созданная ИИ, победила в конкурсе, что побудило Эльдагсена отказаться от награды. Этот инцидент подчеркивает не только быстрый прогресс искусственного интеллекта, но и настоятельную необходимость повышения статуса Кодекса этики в этой области до федерального нормативного правового акта, тем самым обеспечивая надежные этические стандарты и снижая потенциальные риски.

Возможности искусственного интеллекта вызывают и серьезные опасности. В руках злоумышленников ИИ научился оказывать мощное деструктивное информационно-психологическое воздействие. Технологии уже позволяют создавать дипфейки, неотличимые от других изображений. Учитывая стремительное развитие ИИ, вполне возможно, что в ближайшем будущем он будет оставаться в статусе субъекта правовых отношений в сфере информационно-психологического воздействия. В этой связи современный усовершенствованный Кодекс искусственного интеллекта наделив его силовую силу для регулирования взаимодействия между ИИ и человеком.

Таким образом, остаются основные направления развития в области информационно-психологической безопасности.

Выводы по главе 3.

Третья глава содержит предложения автора по оптимизации механизмов противодействия распространению деструктивных субкультур в молодёжной среде. Подчёркивается важность правовой определённости в вопросах

квалификации противоправной деятельности участников таких групп, в том числе необходимости введения в законодательство новых категорий, отражающих цифровую природу современного девиантного поведения.

В качестве приоритетного направления обозначено развитие профилактических мер: внедрение систем мониторинга контента, повышение правовой грамотности подростков, использование потенциала школьных и вузовских учреждений для формирования устойчивых нравственных и гражданских ориентиров. Также предложено совершенствовать систему психологической помощи и раннего выявления подростков, оказавшихся в зоне риска.

Особое внимание уделено необходимости усиления государственного контроля за информационной средой, включая разработку и применение алгоритмов выявления опасного контента, расширение полномочий Роскомнадзора и активизацию сотрудничества с IT-компаниями. В числе инициатив также названы меры по стимулированию позитивного интернет-контента, в том числе через государственную поддержку медиаобразования.

Таким образом, глава 3 отражает стремление автора к формированию целостной, сбалансированной модели противодействия деструктивным влияниям, основанной на правовых, организационных и воспитательных подходах, что должно способствовать укреплению морально-нравственной устойчивости молодёжи в условиях цифровой эпохи.

Заключение

Хотя феномен деструктивной информации и ее психологическое воздействие еще не были всесторонне определены или фундаментально изучены, обзор исследований ведущих ученых выявляет несколько общих характеристик. Это явление в первую очередь включает распространение негативной информации и оказание психофизического воздействия, которое может изменить восприятие мира, изменить отношение к окружающей среде и в конечном итоге повлиять на поведение человека. Субъект, ответственный за такое влияние, часто называемый «актором», намеренно стремится подорвать общественную стабильность, спровоцировать сбои и дестабилизировать как национальные, так и международные порядки.

Основные методы, используемые в этом процессе, включают убеждение, внушение и манипуляцию сознанием. В дополнение к этим прямым подходам, используются вторичные инструменты, такие как бессознательные акустические и визуальные стимулы, часто в сочетании, для достижения более мощного эффекта. Информация широко распространяется по различным каналам, включая Интернет, средства массовой информации, телевидение и радиопередачи, причем предполагаемые цели варьируются от предпринимательской деятельности до общества в целом и даже государственных учреждений.

Чтобы смягчить эти вредные влияния, необходимо обеспечить информационное и психологическое благополучие граждан как на национальном, так и на международном уровне. Эта цель может быть достигнута посредством двойного подхода, который сочетает в себе надежное внутреннее законодательство с активным международным сотрудничеством. Решающее значение для этих усилий имеет четкое определение «информационной и психологической безопасности» — термина, который исследования определили как состояние защищенности личности, общества и государства от внутренних и

внешних угроз, охватывающее не только информационное содержание, но и его психофизические последствия.

Анализ нормативно-правовых актов Российской Федерации показывает, что, несмотря на наличие различных мер, единого документа или комплексной системы, посвященной этой проблеме, не существует. Хотя были предприняты первые шаги по противодействию вредоносной информации и психологическому манипулированию, остаются неясности. Одной из особенно нерешенных проблем является трактовка информационно-психологической безопасности в контексте новых технологий, таких как блокчейн. Эта неопределенность подчеркивает необходимость дальнейшего совершенствования и разработки новых правовых рамок для решения этих развивающихся проблем.

В третьей главе исследования уделено внимание состоянию граждан РФ на негативное информационно-психологическое влияние. Было установлено, что склонность к дезинформации напрямую зависит от конкретных жизненных особенностей, индивидуальных психологических характеристик, уровня образования и общей компетентности населения. Анализ также показал, что Интернет является основным каналом воздействия по сравнению с другими информационными платформами. Наиболее часто используются методы убеждения, внушения и манипуляции с сознанием, а их комбинированное применение позволяет добиться максимального эффекта, тогда как другие методы применяются значительно реже.

Анализ ситуации со стороны населения РФ на информационно-психологическое воздействие позволит выработать ряд предложений по противодействию негативным информационным гражданам. Так, во второй части главы задумана концепция формирования как государственной, так и негосударственной системы, направленная на обеспечение информационно-психологической безопасности. Центральным элементом этой системы является подготовка специалистов в области информационно-психологического

воздействия, с особым упором на воспитание резкого настроенного отношения к интернет-контенту среди молодёжи.

В рамках исследования большое внимание уделялось психологическим проблемам, поскольку сохранение психического здоровья граждан является основным аспектом деструктивного информационного общества. Помимо этого, были ограничены прогрессивные направления с появлением защиты в сфере информационной и психологической безопасности. В частности, развитие нормативно-правовой базы: от появления информационного законодательства до создания специальной психологической помощи. Не менее важной считается проблема искусственного интеллекта, которая, интегрируясь в повседневную жизнь, в будущем потребует отдельного правового регулирования как на волнах, так и на поверхности Земли. В этом третьем ключевом предложении является разработка федерального законодательства, направленного на обеспечение информационной и психологической безопасности.

Если рассматривать систему защиты от информационно-психологического воздействия, то она состоит из трех уровней:

- международный уровень – включает меры по обеспечению глобальной безопасности и противодействию транснациональным угрозам;
- национальный уровень – защищать правовые и организационные основы, формируемую основу для защиты общественных интересов;
- индивидуальный уровень – представляет собой личную безопасность граждан, которую необходимо развивать с раннего возраста через воспитание и образование.

Эти три уровня составляют единые государства, где национальная и личная напряженность напрямую связана с положениями, существующими в Российской Федерации. При устойчивом дальнейшем развитии отечественного закона и его адаптации к новым вызовам возможно создать систему системы защиты общества от разрушительного информационно-психологического воздействия.

Список используемой литературы и используемых источников

1. Баришполец В. А. Информационно-психологическая безопасность: основные положения // Журнал радиоэлектроника. Наносистемы. Информационные технологии. 2013. № 2. С. 62 – 104.-Режим досутпа:URL: https://cyberleninka.ru/article/n/informatsionnopsihologicheskaya-bezopasnost-osnovnyepolozheniya/viewer (дата обращения: 13.02.2025).
2. Бехтерев В.М. Внушение и его роль общественной жизни. [Электронный ресурс]/ Бехтерев В.М. – Режим доступа: URL: https://www.litmir.me/br/?b=92750&p=58 (дата обращения: 13.02.2025)
3. Башно С.В. Способы и методы правового регулирования. [Электронный ресурс]/ Башно С.В. – Режим доступа: URL: https://cyberleninka.ru/article/n/sposoby-i-metody-pravovogoregulirovaniya/viewer (дата обращения: 18.04.2023)
4. Более 10 млн детей России подписаны на деструктивные группы и сообщества в интернете. [Электронный ресурс]/ ТАСС – Режим доступа: URL: https://tass.ru/obschestvo/15758099 (дата обращения: 20.05.2023)
5. Выполнение музыкальных и пространственных задач/Фрэнсис Х. Раушер, Гордон Л. Шоу, Екатерина Н.Кай// Nature. – Vol.8. - 1993. – P. 611
6. Всеобщая декларация прав человека от 10 декабря 1948 г. (принята Генеральной Ассамблеей ООН 10.12.1948). [Электронный ресурс]. – КонсультантПлюс. – Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_120805/(дата обращение: 16.02.2023)
7. «Вопросы Министерства обороны Российской Федерации» [Электронный ресурс]: Указ Президента РФ от 16.08.2004 N 1082 (ред. от 04.05.2022).URL:https://www.consultant.ru/document/cons_doc_LAW_48879/ (дата обращения: 7.05.2023)

8. «Вопросы Министерства иностранных дел Российской Федерации» [Электронныйресурс]: Указ Президента РФ от 11.07.2004 N 865(ред.от22.05.2023).URL:https://www.consultant.ru/document/cons_doc_LAW_19071/35859dcb2bc3d81362f30ad4cf86229c07c05ecd/(дата обращения: 7.05.2023)

9. ВЦИОМ: Новости. В поисках психологической помощи. [Электронный ресурс]: URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/vpoiskakh-psikhologicheskoi-pomoshchi (дата обращения: 21.04.2023)

10. Глобальная контртеррористическая стратегия Организации Объединенных Наций от 8 сентября 2006 года. [Электронный ресурс]: URL: https://documents-dds-ny.un.org/doc/ UNDOC/GEN/N05/504 /90/PDF/ N0550490.pdf? OpenElement (дата обращения: 13.02.2025)

11. Грачев Г.В. Личность и общество: информационно-психологическая безопасность и психологическая защита. [Электронный ресурс]/ Грачев Г.В. – Режим доступа: URL: http://licman.narod.ru/books/psychology/01/gratchov.htm (дата обращения: 13.02.2025)

12. Грачев Г.В., Мельник И.К. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия [Электронный ресурс]/ Грачев Г.В., Мельник И.К. – Режим доступа: URL: http://evartist.narod.ru/text3/76.htm (дата обращения: 13.02.2025)

13. Гражданский кодекс Российской Федерации (ГК РФ) от 30 ноября 1994 года N 51-ФЗ [Электронный ресурс]: URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 29.12.2023)

14. Декларация от 28 ноября 1978 г. об основных принципах, касающихся вклада средств массовой информации в укрепление мира и международного взаимопонимания, в развитие прав человека и в борьбу против расизма и апартеида и подстрекательства к войне Принята Генеральной Конференцией ЮНЕСКО на ее двадцатой сессии 28 ноября 1978 года.[Электронный ресурс].–КонсультантПлюс.–Режим доступа:

URLhttps://www.un.org/ru/documents/decl_conv/declarations/st_hr1_141.shtml (дата обращения: 20.02.2023)

15. Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. [Электронный ресурс]/ Доценко Е.Л. – Режим доступа:URL: https://stavroskrest.ru/sites/default/files/files/books/psihologia_ manipulacii.pdf (дата обращения: 13.02.2025)

16. Дружилов С.А. «Загрязнённость» информационной среды и проблемы психологического здоровья личности [Электронный ресурс]/ Дружилов С.А. – Режим доступа: URL: https://top-technologies.ru/ru/article/view?id=31614 (дата обращения: 19.04.2023)

17. Декларация принципов «Построение информационного общества - глобальная задача в новом тысячелетии» от 12 декабря 2003 год. [Электронный ресурс]: URL: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf(дата обращения: 13.02.2025)

18. Для пересечения границы России предложили бронировать дату и время [Электронный ресурс]/ Лента.РУ. – Режим доступа: URL: https://vk.com/wall-67991642_6362977 (дата обращения: 17.04.2023)

19. Исследование: более 60% россиян уверены, что умеют отличать фейки от правдивых новостей [Электронный ресурс]/ ТАСС– Режим доступа: URL: https://tass.ru/obschestvo/14005711 (дата обращения: 25.04.2023)

20. Инструктаж по гражданской обороне и защите от чрезвычайных ситуаций [Электронный ресурс]: URL: https://msr.mosreg.ru/sobytiya/meropriyatiya/zaschita-naseleniya-otchrezvychaynyh-situaci/instruktazh-po-grazhdanskoy-oborone-i-zashchite-otchrezvychaynyh-situaciy (дата обращения: 25.04.2023)

21. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийским голосованием 01.07.2020). [Электронный ресурс]. – КонсультантПлюс. – Режим

доступа:URL: https://www.consultant.ru/ document/cons_doc_LAW_28399/ (дата обращения: 13.02.2025)

22. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 28.05.2022) [Электронный ресурс] Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

23. Касюк. А.Ю. информационно-психологическое воздействие в информационном противоборстве// Вестник Московского государственного лингвистического университета. Общественные науки. 2021. № 1. С. 22-33.- Режим доступа:URL: https://cyberleninka.ru/article/n/informatsionno-psihologicheskoe-vozdeystviev-informatsionnom-protivoborstve/viewer (дата обращения: 13.02.2025).

24. Конвенция о правах ребенка от 20 ноября 1989 г. (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990) [Электронный ресурс]. – КонсультантПлюс.–Режим доступа:URL: https://www.consultant.ru/document/cons_doc_LAW_9959/ (дата обращения: 17.02.2023)

25. Конвенция Содружества Независимых Государств о правах и основных свободах человека" (заключена в Минске 26.05.1995) (вместе с "Положением о Комиссии по правам человека Содружества Независимых Государств", утв. 28.09.1993) [Электронный ресурс]. – КонсультантПлюс.–Режимдоступа:URL: https://www.consultant.ru/ document/cons_doc_LAW_6966/ (дата обращения: 13.02.2025)

26. «Концепция информационной безопасности детей» [Электронный ресурс]: утверждена распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р URL: https://static.consultant.ru/obj/file/doc/pr_050523-1105.pdf (дата обращения: 13.02.2025)

27. Конвенция Шанхайской организации сотрудничества по противодействию экстремизму от 9 июня 2017 года. [Электронный ресурс]: URL: https://docs.cntd.ru/document/542655220 (дата обращения: 13.02.2025)

28. Кодекс этики в сфере искусственного интеллекта [Электронный ресурс]: URL: https://ethics.a-ai.ru/ (дата обращения: 13.02.2025)

29. Латынов В.В. Психологическое воздействие: принципы, механизмы, теории [Электронный ресурс]/ Латынов.В.-Режим доступа: URL: https://lib.ipran.ru/upload/ papers/paper_21662912.pdf (дата обращения: 13.02.2025)

30. Международный пакт о гражданских и политических правах (принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН). [Электронный ресурс]. – КонсультантПлюс. – Режим доступа:URL: https://www.consultant.ru/document/cons_doc_LAW_5531/ (дата обращения: 16.02.2023)

31. Макаренко С.И. Информационное противоборство радиоэлектронная борьба в сетецентрических войнах XXI века: монография. XXI века. Монография. СПб.: Наукоемкие технологии, 2017. 546 с.

32. Минцифры разработало Концепцию цифровой защиты детей [Электронный ресурс] / Министерство цифрового развития, связи и массовой коммуникации Российской Федерации URL: https://digital.gov.ru/ru/events/44157/?utm_referrer=https%3a%2f%2fyandex.r u%2f (дата обращения: 13.02.2025)

33. Охапкин В.П., Охапкина Е.П., Исхакова А.О., Исхаков А.Ю. Деструктивное информационно-психологическое воздействие в социальных сетях//Научный журнал моделирование, оптимизация и информационные технологии. 2020. № 1. С.114.Режим доступа:URL: https://moitvivt.ru/ru/journal/pdf?i d=733 (дата обращения: 13.02.2025)

34. «Об основных гарантиях прав ребёнка в Российской Федерации» Федеральный закон от 24.07.1998 года № 124 – ФЗ. [Электронный ресурс]:

https://www.consultant.ru/document/cons_doc_LAW_19558/ (дата обращения:8.10.2022)

35. «Об информации, информационных технологиях и о защите информации» Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 14.07.2022) Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

36. «О рекламе» Федеральный закон от 13 марта 2006 г. № 38-ФЗ Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

37. «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации»: Федеральный закон от 29.12.2022 N 572-ФЗ Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

38. «О защите детей от информации, причиняющий вред их здоровью и развитию»: Федеральный закон от 29.12.2010 года № 436-ФЗ Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

39. «О защите населения и территорий от чрезвычайных ситуация природного и техногенного характера» Федеральный закон от 21.04.1994 года №68-ФЗ Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

40. «О стратегии обеспечения информационной безопасности государств – участников содружества Независимых Государств». [Электронный ресурс]: Решение Совета глав правительств СНГ от 25 октября 2019 года. – Режим доступа. URL: https://eecolog.ru/docs/mUnTBGPCVSS8fg2QpeBeO (14.03.2023)

41. «О безопасности» [Электронный ресурс]: Федеральный закон от 28.12.2010 N 390-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_108546/(дата обращения: 18.01. 2025)

42. «О безопасности критической информационной инфраструктуры Российской Федерации» Федеральный закон от 26.07.2017 N 187-ФЗ (последняя редакция). Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

43. «О федеральной службе безопасности»: Федеральный закон от 03.04.1995 N 40-ФЗ (последняя редакция). Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

44. «Об информационно-психологической безопасности»: Проект Федерального закона. Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

45. «О средствах массовой информации»: Закон Российской Федерации от 27 декабря 1991 г. № 2124-1(ред. От 05.12.2022). Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

46. «О Стратегии национальной безопасности Российской Федерации»: Указ Президента от 02.07.2021 года № 400. Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

47. «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации»: Указ Президента РФ от 21.12.2016 N 699 (ред. от 11.02.2023). Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

48. «Об утверждении Требований по обеспечению безопасности значимых объектов критической инфраструктуры Российской Федерации»: Приказ ФСТЭК России от 25.12.2017 № 239 (ред. От 20.02.2020): http://publication.pravo.gov.ru/Document/View/0001201803270041 (дата обращения: 17.01.2025)

49. «О развитии искусственного интеллекта в Российской Федерации» (вместе с "Национальной стратегией развития искусственного интеллекта на

период до 2030 года"): Указ Президента РФ от 10.10.2019 N 490. URL: Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

50. «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»:Указ Президента РФ от 09.05.2017 N 203 Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

51. «Об утверждении Доктрины информационной безопасности» [Электронный ресурс]: Указ Президента от 5.12.2016 года № 646 URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 10.01.2025)

52. «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» [Электронный ресурс]: Постановление Правительства РФ от 02.06.2008 N 418 (ред. от 09.03.2023) Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

53. «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций») [Электронный ресурс]: Постановление Правительства РФ от 16.03.2009 N 228 (ред. от 30.03.2023) Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

54. «О государственной судебно-экспертной деятельности» [Электронный ресурс]: Федеральный закон от 31 мая 2021 г. № 73-ФЗ Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

55. «О противодействии терроризму» Федеральный закон от 06.03.2006 N 35ФЗ [Электронный ресурс]: (последняя редакция) Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

56. Пашенцев Е.Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационнопсихологической безопасности и пути их нейтрализации//Государственное управление. Электронный вестник.2019. № 76. С. 279-300. - Режим доступа: URL:file:///C:/Users/User/Downloads/zlonamerennoe-ispolzovanie iskusstv ennogo-

intellekta-novye-ugrozy-dlya-mezhdunarodnoy-informatsionnopsihologicheskoy-bezopasnosti-i-puti-ih-neytralizatsii.pdf (дата обращения 19.12.2024)

57. Пользование Интернетом [Электронный ресурс]/ ВЦИОМ – Режим доступа: URL: https://wciom.ru/ratings/polzovanie-internetom (дата обращения: 7.01.2025)

58. Проект Федерального закона о психологической помощи [Электронный ресурс]: URL: https://oppl.ru/up/files/files/2022/zakonoproekt.pdf (дата обращения: 20.01.2025)

59. Резолюция Генеральной ассамблеи ООН A/55/63 от 4 декабря 2000 г. «Борьба с преступным использованием информационных технологий» // Организация Объединенных Наций. [Электронный ресурс]: URL: http://www.un.org/ru/documents/ods.asp?m=A/RES/55/63 (дата обращения: 23.10.2022)

60. Резолюция Генеральной ассамблеи ООН A/56/121 от 19 декабря 2001 г. «Борьба с преступным использованием информационных технологий» // Организация Объединенных Наций. [Электронный ресурс]: URL: http://www.un.org/ru/documents/ods.asp?m=A/RES/56/121 (дата обращения: 23.12.2024)

61. Сообщение о начале «второй волны» мобилизации в России оказалось недостоверным. [Электронный ресурс]/ Лента.РУ. – Режим доступа: URL: https://lenta.ru/news/2022/10/12/volni_net/ (дата обращения: 17.01.2025)

62. Смирнов И., Безносюк Е., Журавлёв А. Психотехнологии: Компьютерный психосемантический анализ и психокоррекция на неосознаваемом уровне [Электронный ресурс]/ Смирнов И., Безносюк Е., Журавлёв А. – Режим доступа:URL: https://gigabaza.ru/doc/87209-pall.html (дата обращения: 28.01. 2025)

63. Смирнов А.А. Проблемы формирования системы правового обеспечения информационно-психологической безопасности [Электронный ресурс]/ Смирнов А.А.– Режим доступа: URL:

https://cyberleninka.ru/article/n/problemy-formirovaniya
sistemypravovogoobespecheniya-informatsionno-psihologicheskoy-bezopasnosti/
viewer (дата обращения: 11.02.2025)

64. Смирнов А.А. «Глубокие фейки». Сущность и оценка потенциального влияния на национальную безопасность [Электронный ресурс]/ Смирнов А.А.– Режим доступа: URL: https://cyberleninka.ru/article/n/glubokie-feykisuschnost-i-otsenkapotentsialn ogo -vliyaniya-na-natsionalnuyu-bezopasnost (дата обращения: 7.01.2025)

65. Самые популярные фейки января 2023[Электронный ресурс]/ Лапша Медиа. - Режим доступа: URL: https://dzen.ru/a/Y90ULjJrUCGWSOeA (дата обращения: 10.01.2025)

66. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года [Электронный ресурс]: URL: https://docs.cntd.ru/document/902289626 (20.12.2025)

67. Тунисское обязательства от 15 ноября 2005 год. [Электронный ресурс]: URL: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения: 25.12.2022)

68. Тренды медиапотребления [Электронный ресурс]/ ВЦИОМ – Режим доступа: URL: https://wciom.ru/analytical-reviews/analiticheskiiobzor/trendy-mediapotreblenija-2022 (дата обращения: 25.12.2025)

69. Узлов Н.Д. Психотехнология: к проблеме определения понятия// Вестник Пермского университета. Философия. Психология. Социология. 2011. №5. С.32-42.–Режим доступа: URL: file:///C:/Users/ User/Downloads/psihotehnologiya-k-probleme-opredeleniya ponyatiya%20 (1).pdf (дата обращения: 28.10.2025)

70. Уголовный Кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (последняя версия). [Электронный ресурс]: Режим доступа URL: http://www.consultant.ru/ (дата обращения: 01.01.2025)

71. Устав организации объединённых наций от 26 июня 1945 года (с поправками от 17 декабря 1963 года, 20 декабря 1965 года, 20 декабря 1971 года). [Электронный ресурс]: URL: https://www.consultant.ru/document/cons_doc_LAW_121087/ (дата обращения:30.01.2025)

72. Украинская военная реклама на российских сайтах. [Электронный ресурс]: URL: https://sladkowa.livejournal.com/513184.html (дата обращения:30.01.2025)

73. Угроза ракетного удара [Электронный ресурс]/ Лента.РУ. – Режим доступа:URL: https://lenta.ru/news/2023/02/22/hackers_radio/ (дата обращения: 30.01.2025)