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 Российской Федерации

Обучающийся Д.В. Богданова
(Инициалы Фамилия) (личная подпись)

Научный руководитель к.ю.н. В.В. Романова
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Аннотация

Проблема правой защиты граждан Российской Федерации от деструктивно-информационно-психологического воздействия как никогда актуальна в наши дни. Мы живём в век технологий, разработки которых с каждым годом набирают обороты. Стремительно развивается искусственный интеллект, и то, что было фантастикой становится реальностью. Вместе с тем и совершенствуются методы информационно-психологического воздействия.

По правде говоря, информационно-психологическое воздействие применялось ещё несколько столетий назад, однако, широкой огласке не придавалась. Сейчас многие российские учёные, как и мы, обеспокоены уровнем информационно-психологического воздействия на население Российской Федерации. Поэтому перед нами была поставлена цель изучить деструктивно-информационно-психологического воздействия, проследить его влияние на российское общества, а также проанализировать перспективы развития правовой защиты российского общества от деструктивно-информационно-психологического влияния. Для этого мы поставили перед собой задачи изучить научную литературу указанному вопросу, нормативно-правую базу Российской Федерации, нормативно-правовые документы на международном уровне, а также провести анализ деструктивно-информационно-психологического воздействия на российское общество и выявить пути развития информационно-психологической безопасности.

Структура работы: введение, три главы, заключение, список используемой литературы и используемых источников.

Оглавление

Введение

Мир не стоит на месте. Разрабатываются всё новые методы воздействия и усовершенствуются старые. Проводятся эксперименты, появляются новые технологии способные влиять на людей.

В условиях нашего времени, изучение природы и содержания, а также влияния на людей деструктивного информационно-психологического воздействия как никогда важно. С появлением социальных сетей, мессенджеров люди могут общаться в любое время суток, не важно, где они находятся. В то же время у некоторых субъектов появилось больше возможностей взаимодействовать с людьми, влиять на их мнение через «посты» и видео в социальных сетях.

Отсюда вытекает и следующая проблема. Из-за того, что на законодательном уровне вопрос деструктивно-информационно-психологического воздействия не урегулирован, на просторах Всемирной сети «Интернет» распространилось достаточно много сообществ, пропагандирующих экстремистские, криминальные и антисоциальные идеи. Анонимность позволяет субъектам провоцировать конфликты, призывать к чему-либо в социальных сетях, что может впоследствии расстроить порядок в обществе. Кроме того, законодательство не поспевает за быстро развивающимися технологиями. Многие учённые обеспокоены тем, что в скором времени искусственный интеллект, создание которого стало буквально прорывом в области информационных технологий, может послужить средством для деструктивно-информационно-психологического воздействия. А в дальнейшем стать и субъектом влияния. Уже сейчас поднимаются вопрос о замене человека роботом в тех или иных профессиях. В медицину, в сферу безопасности, промышленное производство уже постепенно внедряются роботы, способные сами выполнять какие-либо операции. Есть вероятность, что в будущем они смогут стать если и неполноправными субъектами, то своего рода средствами воздействия на общество. Несмотря на это на

законодательном уровне всё ещё нет нормативно-правовых актов, способных регулировать деструктивно-информационно-психологическое воздействие. А также нет нормативно правовых актов, закрепляющих методы защиты общества от негативного воздействия.

Вышеуказанные проблемы затронули весь мир, включая Российскую Федерацию. Поэтому они является актуальными на данный момент, так как именно мы, проживая XXI век, находимся в гуще событий, когда технологии развиваются с невероятной скоростью, проводятся новые исследования над подсознанием, а человек сам по себе остаётся всё ещё слабо защищённым от деструктивного информационно-психологического воздействия. Люди являются лёгкой мишенью для субъектов, способных влиять на нашу психику по средствам определенных методов.

Целью работы является анализ деструктивно-информационно-психологического воздействия. Изучение его влияния на российское общество, а также исследование законодательной базы на уровне Российской Федерации и на международном уровне. Кроме того, провести оценку проблемы и перспектив развития правовой защиты российского общества от деструктивно-информационно-психологического влияния.

Задачи исследования для достижения поставленной цели:

- Изучить научную литературу касаемо деструктивно-информационно-психологического воздействия;
- Дать определение деструктивно-информационно-психологическому воздействию и выявить его методы влияния;
- Проанализировать международно-правовые акты о защите от деструктивно-информационно-психологического воздействия;
- Исследовать законодательную базу Российской Федерации по защите от деструктивно-информационно-психологического воздействия;
- Провести анализ и оценку проблем касающихся защиты российского общества от деструктивного-информационно-психологического воздействия.

- Предложить пути решения проблем связанные с правовой защитой деструктивно-информационно-психологического воздействия.

Методологическую основу работы составляет междисциплинарный подход к исследованию проблемы, который использует положение психологии, юриспруденции, теории коммуникации, политологии, журналистики. Также в процессе написания работы использовались общенаучные и частные методы.

Методы исследования: абстрагирование, анализ, синтез, аналогия, индукция, а также сравнение. Кроме того использовались такие частные методы научного познания, как социологические и статистические методы, формально юридический метод, структурно функциональный метод, сравнительно-правовой метод.

Нормативную базу составляет Конституция Российской Федерации, международные договоры и иные международно-правовые акты, федеральные законы, документы стратегического планирования в сфере обеспечения национальной безопасности РФ, подзаконными нормативными правовыми актами федерального уровня (указами Президента РФ, постановления Правительства РФ, приказы федеральных органов исполнительной власти).

Теоретическую основу исследовательской работы составляют работы следующих учёных юристов: 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. Безносюк, А. Журавлёв, Н.Д. Узлов, Е.Л. Даценко, В.П. Охапкин, Е.П. Охапкина, А.О. Исхакова , А.Ю. Исхаков, В.М. Бехтерев, Фрэнсис Х. Раушер, Гордон Л. Шоу, Екатерина Н. Кай., С.В. Башно, С.А. Дружилов, А.А. Смирнов,

Структура работы определена введением, тремя главами, заключением и списком литературы и используемых источников.

Глава 1 Основные положения деструктивно-информационно-психологического воздействия

1.1 Содержание и характеристика деструктивно-информационно-психологического воздействия

При исследовании научной литературы и законодательных актов Российской Федерации не было найдено точного определения деструктивно-информационно-психологического воздействия. Чаще всего в работах видных учёных встречается именно информационно-психологическое воздействие, которое, как отмечается, включает в себя негативное и позитивное влияние. Из чего можно сделать предположение, что деструктивно-информационно-психологическое воздействие является лишь одним из видов информационно-психологического влияния. Поэтому для того, чтобы понять природу исследуемого явления следует сначала изучить информационно-психологическое воздействие как таковое, а также его объект и субъект.

В.А. Баришполец определял информационно-психологическое воздействие как «информационное, психотропное или психофизическое воздействие на психику человека, оказывающее влияние на восприятие им реальной действительности, в том числе на его поведенческие функции, а также в некоторых случаях на функционирование органов и систем человеческого организма» [1]. С.И. Макаренко в своей работе «Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах XXI века» придерживался того же мнения[31]. Исходя из указанного определения, следует вывод о том, что объектом информационно-психологического воздействия является человек, его психологическое и физическое состояние. В научных статьях человек как основной объект воздействия чаще всего рассматривается в качестве гражданина и индивида. В качестве индивида человек - это объект информационно-психологического воздействия, у которого есть свои личные особенности, обладающий сознанием,

подверженный разного рода манипуляциям. Как гражданин человек играет роль субъекта, имеющего свои духовные ценности, установки, а также участвующего в политической жизни своего государства. Например, в Российской Федерации в соответствии со ст. 30 Конституции РФ гражданин РФ имеет право на создание общественных объединений[21]. Кроме того гражданин РФ имеет право, согласно ст. 32 Конституции РФ, учувствовать в управлении делами государства, как непосредственно, так и через своих представителей, имеет право избирать и быть избранным [21].

Человек как объект воздействия является основным. Однако в качестве объекта стоит выделить и общество в целом, так как часто целью могут являться непосредственно воздействие на групповое, массовое и общественное сознание. А.Ю. Касюк. в своей работе писал, «информационно-психологического воздействие — это влияние на индивидуальное и общественное сознание…» [23]. Таким образом, под групповым сознанием понимается вид общественного сознания, при котором небольшое по своим размерам объединение людей, схоже между собой по взглядам, интересам и ценностям. Массовое сознание подразумевает определённый вид общественного сознания, свойственный неструктурированной массе людей. В отличие от группы, масса – это временно возникающие общности, в которых люди могут быть не схожи по интересам и взглядам, но они объединены значимостью психических переживаний. Примером может служить митинг. В свою очередь общественное сознание определяется как совокупность коллективных представлений, идей, взглядов присущих определённой эпохе.

Также часто объектом воздействия является непосредственно государственные структуры, так как они являются важным звеном в системе государства. Благодаря органам государственной власти существует общественный порядок и если что-то выходит из строя, то соответственно меняется и настроение в обществе. По сути, государство – это взаимосвязь государственной власти с населением страны. Успех государства зависит от успешного взаимодействия общества и государственной власти. Поэтому

субъект с целью информационно-психологического воздействия может влиять как на государственные органы страны, так и на общество, и на человека.

Что касается самого субъекта информационно-психологического воздействия, то он может быть как внутренним, так и внешним. Под субъектом воздействия подразумевается источник информации, владеющий теми или иными знаниями и методами информационно-психологического воздействия, а также использующий определённые средства воздействия. Целью субъекта является воздействие на объект. В научных работах есть устоявшиеся термин определения субъекта воздействия – «актор»[33]. Кроме того, говоря о таком методе воздействия, как внушение, по отношению к субъекту применяется термин суггестор, а по отношению к объекту суггеренд. Впоследствии в работе будут использовать данные термины.

В большинстве случаев к субъектам воздействия, согласно многим научным работам, относят: государственные и правительственные учреждения (в том числе иностранные); правовые и силовые (военные) организации; общественные организации; учреждения здравоохранения; финансово-экономические, коммерческие и торговые организации (в том числе зарубежные); криминальные структуры (в том числе международные); микрогруппы; отдельные субъекты.

Если говорить о сущности информационно-психологического воздействия, то согласно определению В.А. Баришпольца данное явление подразумевает информационное, психотропное и психофизическое влияния. В свою очередь есть мнения о том, что не стоит все виды оружия психофизического воздействия относить к информационно-психологическому влиянию, так как это может неоправданно расширить предмет информационно-психологической безопасности. Г. В. Грачев в своей работе обозначил, что понятие ИПВ позволяет выделить из всего спектра разновидностей психофизического воздействия определенную совокупность и тем самым сузить предмет исследования [11]. В действительности не все психофизиологические факторы могут влиять на человека с точки зрения

информационно-психологического воздействия. Например, субъект в пределах информационно-психологического воздействия не может влиять на вкусовые и тактильные рецепторы оппонента, но может оказывать влияние на слуховые и зрительные, так как человек при получении информации использует непосредственно сенсорные каналы восприятия. При исследовании данного фактора многие используют сенсорный критерий (тип использования сенсорного канала восприятия). Кроме этого, в научных работах обращается внимание на критерий объективного воздействия (объект информационного воздействия), подразумевающий то, что помимо соматических элементов, субъект может влиять на другого субъекта, воздействуя непосредственно на его психику, а именно с помощью акустических, электромагнитных и оптических сигналов. В пример можно привести звуки, способные на определённой частоте вызвать у субъекта раздражение и агрессию. Таким образом, исходя из всего вышесказанного и изучив подробно психофизическое воздействие, можно сделать вывод, что оно имеет место быть, но в контексте информационно-психического воздействия присутствует в определённых границах.

Кроме вышеописанного фактора, стоит изучить информационно-психологическое воздействие и со стоны информационного влияния. Согласно п. 1. ст. 2. Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации» «информация – это сведения (данные, сообщения) независимо от формы их представления» [35]. То есть информация может передаваться не только по средствам технических носителей (телевизионное вещание), но и по средствам печатных сообщений (газета, листовки), а также в устной форме при непосредственном контакте с субъектом. Следовательно, в информационно-психологическое воздействие включает в себя две формы, распространение информации и коммуникация. Само по себе информационное влияние очень часто переплетается с психологическим. Желая повлиять на субъект, актор (субъект, совершающий действие в отношении других) использует различные рода манипуляции, а также методы убеждения и внушения. На тему

психологического воздействия учённые проводили достаточно много исследований. Чаще всего, говоря об этапах прогресса в изучении данного воздействия, отправной точкой ставят 1940-е годы[29]. Однако, люди применяли методы психологического воздействия задолго до начала исследований. В те времена чаще использовались листовки, печатные средства массовой информации, сейчас же главной информационной площадкой является всемирная сеть «Интернет». В основном акторы, желая донести до населения свои убеждения, используют непосредственно её, понимая, что так будет проще воздействовать на старшее и младшее поколение, так как сейчас каждый человек проводит большинство своего времени в социальных сетях, работая или желая просто проводя досуг.

Таким образом, акторы обычно используют информационные платформы, подобные YouTube, Вконтакте и другие социальные сети, создавая так называемый, контент (сведения, которые субъект хочет донести другим). Он создаётся по средствам видео, фотографий, «постов» в социальных сетях. Порой, они носят безобидный характер, а иногда целью является дестабилизация порядка внутри общества и страны в целом. Для того, чтобы повлиять на общество, субъектом очень часто создаются так называемые фейки (не соответствующее действительности информация), которые носят деструктивный характер, и распространение которых, достаточно сложно контролировать. В подобном контенте акторы чаще всего используют шокирующие сведения, дабы вызвать определённую эмоцию и внушить субъекту воздействия желаемое.

Помимо распространения негативной информации в научных работах также выделяется коммуникация – общение между индивидами или группой лиц, возникающее как в реальном мире, так и с помощью технических средств. Данная форма проявления информационно-психологического воздействия была и раньше, но в XXI веке, с появлением социальных сетей и мессенджеров, получила больше возможностей для распространения. Общение между малознакомыми людьми стало доступным вместе с созданием новых

технологий. Акторы могут, скрывая свою личность, влиять на других людей, разжигать споры в интернет-сообществах и не только. По этой причине в онлайн-среде стали развиваться такие направления негативной коммуникации как буллинг, троллинг и флейминг. Помимо этого стали активно развиваться онлайн-сообщества, которые несут в себе негативный характер. Например, такие сообщества создаются с целью вербовки в террористические организации, толкание на самоубийство или с целью разжигания ненависти между определёнными социальными группами или внутри них. Для пресечения данных направлений в законодательстве Российской Федерации предусмотрена определённая мера ответственности. Примером может служить, ст.282 Уголовного Кодекса Российской Федерации «о возбуждении ненависти либо вражды, а равно унижение человеческого достоинства» [70].

Кроме того, некоторые учёные выделяют в качестве источника информационно-психологического воздействия не только человека, но и искусственный интеллект. В соответствии с подпунктом «б», пунктом 5 главы I Указа Президента «О развитии искусственного интеллекта в Российского интеллекта» от 10.10.2019 года № 490 «искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений» [49]. С развитием технологий многие компании начали внедрять в продукт своей деятельности голосовых-помощников и чат-ботов. Пользователь, заходя в приложение, может с лёгкостью найти нужную информацию с помощью голосовых помощников. Однако, здесь присутствует и обратная сторона медали. Проблема состоит в том, что искусственный интеллект развивается

достаточно быстро, а законодательная база и меры защиты от злонамеренного использования искусственного интеллекта ещё не сформированы. Искусственный интеллект является эффективным средством для злоумышленников, террористических организаций и других субъектов в качестве воздействия на человека.

Е.Н. Пашенцев в своей научной статье отмечал «об опасности злонамеренного использования искусственного интеллекта с целью подрыва репутации отдельных личностей, манипуляции с криптовалютой, а также угрозы кибератак на элементы инфраструктуры» [56]. Также использование искусственного интеллекта способно разжечь межнациональный, расовые, социальные конфликты в обществе. Кроме всего прочего искусственный интеллект может служить, а точнее уже является оружием информационных и гибридных войн для нанесения непосредственного «удара» по общественному сознанию. В данном случае искусственный интеллект выступает в роли посредника и является лишь средством, оружием в руках акторов. Однако, в научной среде обеспокоены тем, что с развитием технологий и стремительным прогрессом в некоторых странах искусственный интеллект может стать субъектом информационно-психологического воздействия.

Таким образом подводя итог всего вышесказанного, можно сделать вывод, что информационно-психологическое воздействие – это информационное и психофизическое воздействие на психику объекта (как индивидуально, так и массово), способное изменять восприятие мира, отношение к чему бы то не было, и как следствие может менять и поведение. Исходя из изученных материалов, также стоит сделать вывод о том, что информационно-психологическое воздействие способно благоприятно влиять на людей, однако, при желании оно может и оказать негативное влияние с целью нарушения порядка в обществе. Из этого следует, что деструктивно-информационно-психологическое воздействие является видом информационно-психологического. Поэтому деструктивно-информационно-психологическое воздействие можно определить как негативное информационное и

психофизическое воздействие на психику объекта, способное изменять восприятие мира, отношение к чему бы то ни было, и как следствие, может менять и поведение человека. Целью своего рода является покушение на человеческую жизнь, разжигание конфликтов внутри общества, в целом дестабилизация порядка в стране и в мире.

Если подробней изучить правовую природу деструктивно-информационно-психологического воздействия, проанализировав нормативно-правовые акты и документы стратегического планирования, то можно сделать вывод о том, что деструктивно-информационно-психологическое воздействие стоит определить как:

- угроза безопасности;
- формы злоупотребления правом на информацию и свободой массовой информации;
- преступление против личности (жизнь, честь, достоинства человека);
- вид соучастия в совершении преступления (организации, подстрекательства, интеллектуального пособничества);
- основания для признания недействительности сделки (совершение сделки под влиянием существенного заблуждения);
- основания для применения мер государственного принуждения, включая блокировку информационного ресурса и другие.

Изучая правовою природу деструктивно-информационно-психологического воздействия, понимаешь, что данная проблема является межотраслевой и затрагивает все институты российского права.

1.2 Методы и средства деструктивного информационно-психологического воздействия

Исследование сущности деструктивно-информационно-психологического воздействия привело нас к выводу о том, что оно является одним из видов информационно-психологического воздействия. Соответственно и методы у

них будут схожи. Единственное, мы будем рассматривать методы информационно-психологического воздействия через призму негативного влияния. Среди работ учённых можно найти разный перечень методов информационно-психологического воздействия. С.И. Макаренко в своей работе писал, что методы информационно-психологического воздействия «превратились сегодня в сложные технологии воздействия на психику людей, обобщенно называемые в литературе психотехнологиями» [31, с. 408]. И. Смирнов, Е. Безносюк, А. Журавлёв в своей работе включали в состав психотехнологий средства, влияющие на нервную систему[62]. В большинстве работ психотехнологии описывались как набор методов для воздействия на человеческое сознание, что давало лишь поверхностное понимание его сущности и не отражало полную специфику. Более точно термин «психотехнологии» описал Н.Д. Узлов, отразив его как «организованная и продуктивная деятельность людей в различных сферах социальной практики, ориентированная на эффективное решение психологических задач с заранее определенным социальным эффектом и представляющая собой совокупность приемов, средств и методов психологического воздействия и влияния, объединенных определенным алгоритмом их применения» [69]. В нашем случае психотехнологиями являются методы информационно-психологического воздействия на психику человека, и, следовательно, способные изменить его поведение. В научных работах приводятся разные перечни методов информационно-психологического воздействия, но между ними прослеживается определённая схожесть. Из чего можно выделить основные методы воздействия:

Первый метод - убеждение. Характеризуется как воздействие на эмоциональную и рациональную части оппонента по средствам приведения чётких аргументов. Главной целью является убедить людей в нужных для актора доводах. Конечно, чтобы заставить людей колебаться одних логичных аргументов недостаточно. Актору нужно убедиться в том, что человек его слышит. То есть надо понимать об осведомлённости субъекта в обсуждаемом

вопросе, уровне его образования, как он относится к актору и способен ли он его понять. В некоторых работах отмечается, метод убеждения влияет тогда, когда оппонент относится благоприятно к источнику информации. Вероятность успеха повышается в том случае, если два субъекта схожи, например, по политическим убеждениям, национальному признаку или при отсутствии языкового барьера. Кроме того речь актора не должна сопровождаться сухими фактами. Чтобы достичь цели, нужно затронуть эмоциональную составляющую. Различают три вида аргументов: истинные факты; аргументы, апеллирующие к позитивным ожиданиям; аргументы, апеллирующие к негативному ожиданию. Первый вид подразумевает точность приводимых доводов, основанных на реальных событиях и никак иначе. Второй вид отличается от первого тем, что к фактам добавляются обещания на лучшую жизнь, тем самым успокаивая общество и вселяя надежду на лучшее. Третий вид, напротив, разжигает в человеке злость и ненависть к тому, на что или на кого направлена речь актора. Также субъекты часто используют «двустороннее сообщение», способ убеждения, при котором человек использует свои аргументы против контраргументов противника. В такие моменты обычно он противопоставляет свои доводы, доводам противника, желая, убедить общество в том, что его идеи лучше. Обычно такой способ используют во взаимодействии с людьми, у которых достаточно высокий уровень образования, и которые испытывают потребность в сопоставлении разных точек зрения и мнений. Есть и другой способ, называемый «односторонним сообщением». Он работает, если субъект не испытывает неприязни к источнику воздействия и готов с лёгкостью принять его точку зрения. Однако, не смотря на это речь актора всё равно должна сопровождаться чёткими и понятными аргументами. Отличие убеждения от внушения являются именно аргументация и доказательства.

Второй метод - внушение (суггестия). Оно под собой подразумевает либо неосознанное, либо осознанное психологическое воздействие на человека, при котором он готов без какой либо критики принять убеждения или установки

актора. Говоря о такой форме психологического воздействия как суггестия, учённые выделяют два его направления. Первый, предметность способа воздействия. Он изучает то, каким именно образом сеггестор (личность, которая внушает), влияет на суггерента (личность, которой внушают). Учённый В.М. Бехтерев считал, что суггестор воздействует на оппонента через определённые эмоции, чувства [2].

Вторым направлением внушения указываются особенности процесса восприятия. Главным критерием считается неосведомленность и отсутствие критического мышления. То есть, человек должен быть легко внушаемым. Учённые выделяют определённый контингент людей, которые являются наиболее ведомыми. Во многих работах в факторе риска чаще указываются подростки или люди пенсионного возраста. Первые очень увлекаемы и больше уважают того человека, кто является для них авторитетом. Вторые в силу своего возраста могут принимать слова говорящего за правду и искренность. Конечно, благоприятным фактором внушения является не только возраст. Нужно, чтобы в момент внушения человек был не в состоянии оценить ситуацию. Отмечается, что внушение может быть сильнее во время стихийного бедствия или критического состояния страны (высокая инфляция, дефолт). Также уровень внушения повышается под воздействием целенаправленной рекламы, значимости передаваемой информации.

Кроме того, стоит сказать про виды внушения. Различают непосредственное (прямое воздействие на людей, личный контакт) и опосредованное (внушение через прессу, рекламу, фильмы и тог далее). Частым приёмом опосредованного внушения является намёк, одобрение, осуждение или «обманутые ожидания».

Таким образом, можно сделать вывод о том, что внушение может быть как напрямую, так и косвенно. Помимо этого, в отличие от убеждения, особенность внушения – это влияние не посредством каких-либо доказательств и чётко поставленных аргументов, не попытка воздействовать на логику и разум человека, а в основном давление суггестора на эмоции суггерета. Также

отмечается, что внушение будет лучшим методом, когда суггерет готов на веру принимать передаваемые сведения, то есть степень его внушаемости и критичность обстановки вокруг.

Третий метод - манипуляции сознанием. Чтобы точно понимать, что такое манипуляционное воздействие стоит также обратить внимание на его признаки, а именно: психологическое воздействие; отношение манипулятора к другому как средству достижения собственных целей; стремление получить односторонний выигрыш; скрытый характер воздействия (как факта воздействия, так и его направленность); использование (психологической) силы, игра на слабостях; побуждение, мотивационное привнесение; мастерство и сноровка в осуществлении манипулятивных действий. Исходя из этого, можно сделать вывод, что манипуляция – это скрытое воздействие на человека, с целью получения односторонней выгоды. В случае манипуляции, как и с другими методами информационно-психологического воздействия результатом всегда является односторонняя выгода, так как актор влияет на субъекта с целью навязывания ему своей точки зрения. Только манипуляция сознанием является довольно сложным методом, имеющим несколько видов воздействия. Ему было посвящено множество исследований. Наиболее точное определение манипуляции дала Доценко Е.Л., определив данный метод, как «вид психологического воздействия, искусное исполнение которого ведет к скрытому возбуждению у другого человека намерений, не совпадающих с его актуально существующими желаниями»[15].

Данный метод воздействия подразделяется на два направления, неосознанное и осознанное влияние. В случае манипуляции, как метода деструктивного информационно-психологического воздействия, учённые рассматривают в основном осознанную манипуляцию. Г.В. Грачев и И.К. Мельник выделяли несколько групп факторов, влияющих на степень их действенности и опасности для человека[12]. Под первой группой подразумевалась совокупность факторов, связанных с содержанием и структурой манипулятивных технологий, используемых для воздействия на

человека. Во вторую группу входят внешние факторы информационно-коммуникативных ситуаций, которые влияют на качество результата манипуляции. К ним можно отнести качество звука и изображения, мастерство манипулятора. В третью группу входят факторы, определяющие подверженность человека манипулятивному воздействию. Люди, которые подвержены манипуляциям, чаще всего имеют низкий уровень образования. Однако, это ещё не основной признак. На внушаемость могут влиять черты характера, такие как пугливость, неуверенность, не информированность в обсуждаемой теме. Поэтому учённые подразделяют третью группу факторов на две подгруппы, ситуационные факторы и внеситуационные факторы.

Под ситуационными факторами понимается психическое состояние индивида, вызванное нахождением в толпе, в участии в переговорах или в любых экстремальных условиях, когда он начинает проявлять свои эмоции. Внеситуационные указывают на индивидуальные особенности личности, которые влияют на результат манипуляции. Например, его критичность, подозрительность, неуверенность в себе и тому подобное [12].

Сейчас манипулятивные методы вышли на новый уровень, так как границы воздействия стали шире с появлением всемирной сети «Интернет». Собственно, как и другие методы деструктивно-информационно-психологического воздействия.

Четвёртый метод - предъявление неосознаваемой акустической информации. Ранее мы писали о том, что на человека может оказываться психофизическое влияния, но в пределах деструктивно-информационно-психологического воздействия оно имеет определённые границы. В качестве примера был приведён звук. Он же является одним из методов и в тоже время средством воздействия. Звук имеет сильное влияние, как на эмоциональную, так и на рациональную составляющие человеческого сознания. Исследованиями давно доказано, человек получает через звук 10 % информации. Также он влияет на нашу нервную систему, успокаивая или раздражая её звуковыми вибрациями. В 1993 году Фрэнсис Раушер и Гордон

Шоу провели эксперимент, который позже назвали «эффектом Моцарта» [5]. Суть заключалась в том, чтобы дать добровольцам послушать сонату композитора, а после попросить пройти тест на пространственное мышление. В итоге добровольцы решили задачи быстрее, чем до прослушивания композиций. Только эффект длился не долго. Через некоторое время люди пришли в норму, то есть вернулись к своему естественному уровню. Несмотря на то, что результат был кратковременным, всё-таки он доказал, музыка может влиять на человека. Именно поэтому в кинематографе большую роль играет правильно подобранная музыка, так как именно от неё зависит настроение картины. Также можно привести в пример гимн, мелодия которого ведёт за собой ряд звуковых и зрительных ассоциаций, может вызывать чувство гордости за свою страну.

Пятый метод - предъявление неосознаваемой зрительной информации. Согласно проводимым исследованиям человек получает 80% информации через зрительное восприятие. С появлением социальных сетей, люди всё больше потребляют информацию, просматривая те или иные видео на разных информационных площадках. Читать обычные тексты становится не интересно, и для того, чтобы заинтересовать пользователя многие авторы к своим «постам» обязательно прикрепляют фото или видео.

В большинстве случаев человек обращает внимание на положение, форму и движения объекта, а также на цвет и яркость картинки. Психологи давно выяснили, что яркость влияет на настроение человека. Если в комнате много света, у индивида повышается активность и появляется бодрость. Другое дело, если в комнате тусклый свет. В таком случае может появиться апатия, грусть. Также с фото- и видеоизображениями. Мрачная картинка, в совокупности с не менее мрачным сюжетом, повышает уровень беспокойства и действует на нервную систему. В случае деструктивно-информационно-психологического воздействия акторы, создавая определённые контент (фото- или видеоматериалы) могут использовать метод неосознаваемой зрительной информации, влияя тем самым на эмоциональную составляющую личности.

Шестой метод - комбинированный. Приведённые выше методы могут применять отдельно, но чаще всего они используются в совокупности для усиления эффекта. Так актор может написать текст в социальной сети, применив методы убеждения, при этом прикрепив видео, где использует метод неосознаваемой зрительной информации. Также он может записать видео-обращение на платформе YouTube, применив метод манипуляции сознанием, убеждая общество, он «свой», а также вмонтировать в это же видео компрометирующие фото на того или иного человека. В тоже время в своих видеороликах акторы часто используются музыкальное сопровождение для создания соответствующего настроения.

Конечно, все приведённые методы деструктивно-информационно-психологического воздействия всегда будут эффективны при использовании тех или иных средств. Основными площадками для информационно-психологического воздействия является Всемирная сеть «Интернет», телевидение и СМИ. Радиовещание постепенно уходит в прошлое. В соответствии с данными Всероссийского центра изучения общественного мнения «тренды» медиапотребления от 6 октября 2022 года – это интернет и телевидение. Исследование ВЦИОМ производилось и составлялось в процентном соотношении в зависимости от пола, возраста, уровнем образования и местом проживания. В итоге, согласно статистике более половины россиян предпочитают гибридную модель медиапотребления. Ровно 53 % составляют активные пользователи телевидения и интернета. Немного больше эта модель выражена среди граждан 45-59 лет, чем среди молодого поколения. Группу активных потребителей интернета в возрастной категории 18-24 лет составляет 66%. В возрасте 25-34 года – 52%. Активных телезрителей среди молодого поколения составляет всего 1 %. В группу активных телезрителей входят в преимуществе граждане в возрасте 60 лет и старше (43%). Неработающие пенсионеры – 43% . Люди, проживающие в сельской местности – 25 % [68].

Исходя из приведённой статистики, следует вывод о том, что телевидение хоть и пользуется спросом, но находится на втором месте после всемирной сети «Интернет», так как большинство граждан в совокупности всё же пользуются социальными сетями, браузерами и другими информационными платформами. К тому же, учитывая, что молодое поколение пользуется в своём преимуществе только Интернетом, можно предположить, что через определённое время Всемирная сеть станет основной платформой потребления информации. Что касается СМИ, то печатные издания постепенно уходят в небытие. Сейчас с популярностью Интернета все крупные издания перенеслись в социальные сети, мессенджеры. По статистике его используют люди старшего поколения, которым печатные издания ближе, чем электронные, но в процентном соотношении они всё равно уступают пользователям интернета.

Таким образом, проанализировав методы деструктивно-информационно-психологического воздействия и средства их использования можно сделать вывод о том, насколько огромное влияние могут оказывать акторы на общество. В особенности через Всемирную сеть «Интернет», так как сейчас данная платформа является одним из основных источников потребления информации.

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

В нынешних реалиях требуется регулирование вопроса информационно-психологической безопасности не только внутри государства, но и на международном уровне. Многие исследователи отмечают важность создания комплексного международного договора универсального характера для обеспечения международной информационно-психологической безопасности, что способствует предотвращению кибертерроризма и стабилизации международной ситуации.

Нельзя сказать о полном отсутствии правового регулирования в сфере международной информационно-психологической безопасности. В современном мире существуют организации и международные нормативно-правовые акты, регулирующие отношения в данной области, являющиеся базой.

В первую очередь стоит обратить внимание на нормативно-правовые акты, которые затрагивают права человека. Одними из главных документов в указанной сфере, участницей которых всё ещё является Российская Федерация - Всеобщая декларация прав человека от 10 декабря 1948 года[6] и Международный пакт о гражданских и политических правах от 16 декабря 1966 года[30]. Каждый из документов содержит в себе основные права человека, такие как право на свободу слова, мнения, религии. Между тем присутствует и ограничение прав. Помимо реализации своих прав и свобод каждый человек должен с уважением относиться к правам и свободам другого, не препятствуя и не умаляя их значимости. В пример можно привести статью 19 Международного пакта, которая отмечает важность « уважения прав и репутации других лиц; для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения»[30].

Ко всему прочему в статье 4 Международного пакта закреплено право государств отступать от своих обязательств во время «чрезвычайного положения в государстве, при котором жизнь нации находится под угрозой» [30]. Однако есть условие, заключающиеся в том, что меры, принятые государством, не должны противоречить другим его обязательствами по международному праву и не влекут за собой дискриминации. Также всякая «пропаганда войны» и «всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию»[30] должны быть запрещены законом.

Большое внимание в сфере защиты от негативного информационно-психологического воздействия уделяется детям. В пункте «а» статье 17 Конвенции о правах ребёнка от 20 ноября 1989 года говорится о поощрении

СМИ «к распространению информации и материалов полезных для ребёнка в социальном и культурном отношениях» [24]. Ко всему прочему государства участники «поощряют разработку надлежащих принципов защиты ребёнка от информации и материалов, наносящих вред его благополучию»[24] (пункт «е» статья 17 Конвенция о правах ребёнка от 20.11.1989 года). В документе оговаривается не только защита детей с точки зрения информации, но и с точки зрения психологии. Согласно статье 19 Конвенции о правах ребёнка от 20.11.1989 года государства принимают все необходимые меры для защиты детей от психологического насилия, оскорбления или злоупотребления и тог далее[24]. Конечно, стоит отметить такие базовые права как свобода мнения, свобода слова и вероисповедания, которые тоже прописаны в тексте Конвенции.

Вышеуказанные документы являются основой при создании международных актов регулирующих информационно-психологическую безопасность, так как защита прав и свобод человека является важным критерием не только в информационном пространстве, но и в повседневной жизни.

Помимо универсальных международных актов схожие стандарты содержатся и в региональных международно-правовых актах о правах человека, в частности в Конвенции СНГ о правах и основных свободах человека от 26 мая 1995 г. В отношении информационной безопасности согласно ст. 9 указанной конвенции «каждый человек имеет право на тайную переписку», что говорит о защите частной жизни человека, если иное «не предусмотрено законом и необходимо в интересах государственной и общественной безопасности, общественного порядка…»[25]. Также в статьях 10 и 11 говорится о свободе мнения, слова и вероисповедания.

Говоря о защите государства и его общества от негативного информационно-психологического воздействия, можно обратиться к Уставу ООН. Согласно п.7 ст.2 Устава ООН положения, закреплённые в документе, не дают права организации вмешиваться в дела государства, и не требует от своих

членов предоставлять информацию для разрешения внутригосударственных процессов[71]. Иными словами установленный пункт защищает государство от внешнего информационного вторжения, однако, в случае «угрозы миру и нарушения мира, актов агрессии»[71] данный принцип не затрагивает принудительные меры обозначенные главой VII Устава ООН.

Если говорить о способах передачи информации, то главным из них в наше время можно назвать такую платформу, как Всемирная сеть Интернет. Как отмечалось в прошлых параграфах большинство СМИ перешли на данную площадку. Многие люди пользуются информационными сайтами и другими социальными сетями в поисках свежих новостей. Проблема состоит в том, что среди международных актов универсального характера нет документов, систематизирующих правовые нормы и регулирующих порядок в отношении всемирной сети Интернет. Единственное, что как-то регулирует отношения, касающиеся всемирной сети – рекомендательные международные акты. В главе II Указа Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» перечислены международные документы, отражающие «международные принципы создания информационного общества и подходы к его созданию», а именно Окинавская хартия глобального информационного общества от 22 июля 2000 года, Декларация принципов «Построение информационного общества - глобальная задача в новом тысячелетии» от 12 декабря 2003 год, Планом действий Тунисского обязательства от 15 ноября 2005 год [50]. Данные документы можно назвать первым шагом к урегулированию вопроса информационно-коммуникационных технологий (далее ИКТ) и всемирной сети Интернет. Они закладывают основные принципы при создании международного информационного сообщества и признают ИКТ как инструмент для повышения производительности, экономического роста и повышения качества жизни для всех. Кроме того, в Плане действий Тунисского обязательства от 15 ноября 2005 год подчёркивается важность уголовного

преследования киберпреступности и приверженность к «позитивному использованию Интернета»[67].

Однако, отсутствие универсального международного акта, который регулировал бы киберпространство, значительно усложняет отслеживание киберпреступности. Однако, конвенция по борьбе с информационными преступлениями мог бы стать первым универсальным документом, способным упорядочить международные отношения и дать гарантию безопасности государствам от информационно-психологического воздействия.

В настоящее время в сфере защиты информационного пространства государства опираются на такие документы, как специальные резолюции Генеральной ассамблеи ООН A/55/63[59] и A/RES/56/63 «Борьба с преступным использованием информационных технологий»[60], где его членами признаётся необходимость сотрудничества между государствами в борьбе против преступности с использованием информационных технологий.

Ко всему прочему стоит отметить международные нормативно-правовые акты по борьбе с терроризмом. В контексте борьбы против информационно-психологического воздействия главным документом является Глобальная контртеррористическая стратегия ООН, принятая резолюцией A/RES/60/288 Генеральной ассамблеи от 8 сентября 2006 г., которая призывает государства прилагать усилия для запрещения по закону подстрекательства к совершению террористического акта и недопущения такого поведения. Содержится в ней и отдельная норма, касающаяся Интернета: призыв к государствам изучать в сотрудничестве с ООН пути и средства координации усилий, принимаемых на международном и региональном уровнях в целях борьбы с терроризмом во всех его формах и проявлениях в сети Интернет[10].

Из региональных международных актов стоит отметить Конвенцию Шанхайской организации сотрудничества по противодействию экстремизму. Документ обращает внимание на важность мониторинга СМИ и сети Интернет с целью своевременного выявления и пресечения распространения идеологии (п.6. ст. 7 Конвенции ШОС по противодействию экстремизму)[27]. Также

создатели говорят об укреплении нравственного, духовного воспитания (п.8. ст. 7 Конвенции ШОС по противодействию экстремизму). Указанное положение является важным для защиты от негативного психологического воздействия, так как уровень нравственности и осознанности граждан снижает уровень влияния на них со стороны террористических организаций.

Что касается традиционных источников информации, СМИ, их деятельность регулируется на международном уровне такими актами, как 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, принятая Генеральной конференцией ЮНЕСКО [14]. Указанный документ отмечает важность в обеспечении доступности информации из разнообразных источников с целью получения каждым человеком возможности объективно оценивать события и факты. В связи с этим журналисты должны обладать свободой передачи сообщений и средствами доступа к информации. К тому же СМИ отводится важная роль в воспитании молодёжи в духе мира, справедливости, взаимного уважения. Кроме того, в Декларации принципов «Построение информационного общества - глобальная задача в новом тысячелетии» от 12 декабря 2003 года также упоминается приверженность к принципам свободы слова и печати в отношение СМИ, но в тоже время есть призыв к средствам массовой информации «ответственно подходить к использовании информации и обращаться с ней, в соответствии с высочайшими этическими и профессиональными стандартами»[17].

Многие учёные, исследуя международные нормативно-правовые акты в сфере защиты от негативного информационно-психологического воздействия, основываются и на правовых документах посвящённых международной информационной безопасности. Отдельно хочется выделить региональный акт, Соглашение между правительствами государств – членов Шанхайской организации сотрудничества (далее ШОС) о сотрудничестве в области

обеспечения международной информационной безопасности. В ст. 2 представленного соглашения перечислены основные угрозы международной информационной безопасности. В их число входит:

- информационная преступность;

-информационный терроризм;

-распространение информации наносящей вред общественно-политической системе, а также духовной, нравственной и культурной среде[66].

Все вышеперечисленные пункты являются составляющей негативного информационно-психологического воздействия. В качестве основных направлений определяется противодействие угрозам и совместная разработка мер по устранению проблем, а также обмен опытом. Данное соглашение в какой-то степени упорядочивает отношения внутри ШОС, позволяет государствам защитить своих граждан от информационно-психологического воздействия. Плюс ко всему в региональном международном акте обращено внимание на такие явления, как информационная преступность и на информацию, наносящая вред духовной и нравственной среде. Определены формы и механизмы сотрудничества. Таки образом, государства-участники признают существование такой проблемы, как информационно-психологическое воздействие, признают его уровень опасности, и важность разработки мер по решению вопроса.

Исследовав вопрос защиты государства и общества на международном уровне, можно сделать вывод. На данном этапе существует несколько документов, которые в той или иной мере регулируют безопасность в сфере информационно-психологического воздействия. Однако, отсутствие универсального международного нормативно-правового акта, императивного характера значительно усложняет отслеживание процессов информационно-психологических воздействия. В нашем мире террористические организации и другие субъекты находят всё новые способы воздействия на государства и их граждан. Они опережают международное законодательство, тем самым

разобщая международное сообщество. Проблема также состоит в том, что отсутствие подобного международного документа даёт некоторым государствам возможность обходить вышеуказанные нормативно-правовые акты и внедряться во внутренние дела других государства.

Конечно, создание международного нормативно-правового акта посвящённого информационно-психологической безопасности вызывает сложность, так как у каждого из государств есть свои особенности связанные с религией, политическим режимом, с уровнем развития ИКТ и всемирной сети Интернет. Однако, единый международный нормативно-правовой акт по информационно-психологической безопасности является важным шагом для устранения угроз в мировом сообществе, а также для защиты гражданина и человека. При создании такого рода документа следует определить угрозы информационно-психологического воздействия, направления деятельности при устранении угроз, определить понятия угроз и средств информационно-психологического воздействия. При всём при этом стоит учитывать особенности тех или иных государств.

Глава 2. Информационно-психологическая безопасность и защита граждан Российской Федерации от деструктивно-информационно-психологического воздействия

2.1. Характеристика правовой системы информационно-психологической безопасности и её принципы

Для того, чтобы создать правовую защиту граждан РФ от негативного информационно-психологического воздействия следует изучить правовую систему информационно-психологическую безопасности. На законодательном уровне определение данного явления никак не закреплено. А.А. Смирнов и многие учёные определяет информационно-психологическую безопасность как «состояние защищённости личности, социальных групп и общества от деструктивного информационно-психологического воздействия» [63]. В начале двухтысячных был разработан проект Федерального закона об информационно-психологической безопасности. Документ определял объекты и субъекты информационно-психологического воздействия, а также угрозы. К ним отнесли:

«- причинение вреда здоровью человека

- блокирование на неосознаваемом уровне свободы волеизъявления человека, искусственное привитие ему синдрома зависимости;

- утрата способности к политической, культурной, нравственной самоидентификации человека;

- манипуляция общественным сознанием;

- разрушение единого информационного и духовного пространства Российской Федерации, традиционных устоев общества и общественной нравственности, а также нарушении иных жизненно важных интересов личности, общества и государства». [44]

Кроме того, в данном проекте зафиксировали ответственность за осуществление негативного информационно-психологического воздействия, а

именно административная, уголовная ответственность, а также иная ответственность предусмотренная законодательством РФ. Законопроект закреплял суть информационно-психологической безопасности и её меры защиты, однако, не был одобрен Государственной думой в первом чтении.

До сих пор на законодательном уровне информационно-психологическая безопасность не была определена по существу, как собственно и информационно-психологическое воздействие. Последнее упоминается лишь раз, в главе III Указа Президента от 02.07.2021 года № 400 «О Стратегии национальной безопасности Российской Федерации» в качестве национального интереса[46].

Стоит сказать, что информационная безопасность и информационно-психологическая безопасность не являются тождественными понятиями. Информационная безопасность – это «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[51]. В свою очередь информационно-психологическая безопасность – это состояние защищённости личности, общества и государства от внутренних и внешних угроз не только информационного, но и психологического воздействия. Учитывать психологическую составляющую очень важно по причине того, что основной упор при негативном информационно-психологическом воздействии идёт непосредственно на психику человека.

В настоящий момент большое внимание в сфере защиты от информационно-психологического воздействия уделяется детям. Подрастающее поколение, как уже было сказано, наиболее уязвимый объект при негативном воздействии. Соответственно, документ, который затрагивает сферу информационно-психологической безопасности детей, Федеральный закон «О защите детей от информации, причиняющий вред их здоровью и

развитию» от 29.12.2010 года № 436-ФЗ. Предметом федерального закона являются «отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции»[38]. В документе отсутствуют понятия информационно-психологической безопасности и информационно-психологического воздействия, но есть чёткий перечень информации, способной негативно повлиять на детскую психику и соответственно запрещённой. Ко всему прочему обозначены требования для оборота информационной продукции, их классификация и разграничены полномочия федеральных государственных органов контроля. Указанный документ стал первым, принятым на законодательном уровне нормативно-правовым актом, регулирующим информационно-психологическую безопасность. Единственное, в федеральном законе нет норм, устанавливающих ответственность за информационно-психологическое воздействие во Всемирной сети интернет, которая, как уже было не однократно сказано, является главной платформой распространения информации.

Пробелы по вопросу Интернета устраняет закон Федеральный закон от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации». Он устанавливает обязанности для лиц распространяющих информацию в сети «Интернет», а также даёт определение «организатор распространяющий информацию» (ст.10.1)[35]. Особенности распространения информации в социальных сетях, а именно требования для владельцев интернет-сайтов, сообществ, информационных систем (ст.10.6)[35]. В статье содержатся положения о запрете на распространение информации, порочащей честь и достоинства личности, отдельных категорий граждан по ряду признаков. Запрещается распространение запрещённой информации, например, материалов с порнографическими изображениями малолетних, а также о способах и методах разработки наркотических средств и тог далее. Кроме того, устанавливается порядок по ограничению доступа к негативно информации и информационным ресурсам.

Говоря об правовой системе информационно-психологической безопасности нельзя ни сказать о СМИ, так как они тоже являются средством информационно-психологического воздействия. Основной нормативно-правовой акт средств массовой информации - Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Важной статьёй в сфере защиты от информационно-психологического воздействия является статья 4, о недопустимости злоупотребления свободой массовой информации. Указанное понятие содержит большой блок положений, самым примечательным из них является запрет использования СМИ «…скрытых вставок и иных технических приёмов и способов распространения информации, воздействующих на подсознание людей и(или) оказывающих вредное влияние на их здоровье…»[45]. Это один из немногих законов, который обращает внимание на психологическую безопасность своих граждан.

Кроме упомянутых источников информационно-психологического воздействия стоит также упомянуть рекламу, которой посвящён отдельный Федеральный закон «О рекламе» от 13.03.2006 года № 38 – ФЗ. В ч. 1 ст.3 реклама понимается «информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке»[36]. В ст.5 содержатся общие требования, говорящие о недобросовестной и недопустимой рекламе. Недобросовестная реклама определяется множеством аспектов, в контексте информационно-психологической безопасности можно выделить требование о недопустимости рекламы, порочащей честь, достоинство и репутацию граждан. Также в использование бранных слов, непристойных и оскорбительных образов, сравнений относительно пола, расы, религии и прочее. Также Федеральный закон «О рекламе» от 13.03.2006 года № 38 – ФЗ регламентирует разные способы распространения рекламы, в число которых входит и всемирная сеть «Интернет». Кроме того нормативно-правовой акт защищает детей от

негативной рекламы. Именно от той, что может сформировать комплекс неполноценности, побуждает причинить себе вред, подрывает доверия к родителям[36].

Помимо выше представленных нормативно-правовых актов правовую основу информационно-правовой безопасности составляет конституционно, административное, уголовное и гражданское право.

Конституционное право регулирует базовые права и свободы человека и гражданина, а также основные нормы, в соответствии с которым издаются другие нормативно-правое акты. Если рассматривать в контексте информационно-психологической безопасности, то в ч.2 ст.29 г. 2 Конституции РФ устанавливаются положения о недопущение пропаганды или агитации, возбуждающий распри в обществе. Также запрещается пропаганда превосходства одних групп над другими[21]. Тем самым законодатель препятствует деструктивному информационно-психологическому воздействию.

Что касается административного права, то оно закрепляет статус и регламентирует обязанности государственных органов исполнительной власти, непосредственно являющийся субъектом обеспечение информационно-психологической безопасности. Законодатель гарантирует запрет на разглашение информации, доступ к которой ограничен законами. К ней относится сведения о несовершеннолетних, врачебная тайна и прочее (ст. 13.14 КоАП РФ)[22]. Статья 5.61.1 КоАП РФ содержит меру воздействия за клевету, которая может повлечь незаконное очернение гражданина и тем самым повлиять на его моральное здоровье, а также негативно повлиять на восприятие его персоны окружающими[22].

Также уголовное право устанавливает юридическую ответственность за нарушение информационно-психологической безопасности ровно, как и гражданское право. Например, ст.150 – 151 УК РФ вовлечение несовершеннолетних в преступные действия или совершение антиобщественных действий[70]. Тем самым в случае использования актором психологического воздействия на несовершеннолетнего в целях совершения

беспорядка, он наказывается либо обязательными работами, либо ограничением свободы, либо лишением свободы на определенный срок. В ст.151 Гражданского кодекса РФ закрепляет положение том, что в случае причинения морального вреда (физические или нравственные страдания) гражданину, то суд может обязать нарушителя выплатить пострадавшему денежную компенсации[13].

Проанализировав нормативно-правовые акты, можно сказать, что информационно психологического воздействие всё же имеет правовое регулирование. Однако нормы закреплены в разных документах и касаются отдельных правонарушений. Сами понятие, принципы, цели, задачи информационно-психологической безопасности на законодательном уровне отсутствуют. Не смотря на то, что принципы – это нормы права, определяющие содержание и направления той или иной сферы. Их можно назвать основой, без которой дальнейшая разработка концепции информационно-психологической безопасности не представляет смысла.

При исследовании и структурировании принципов информационно-психологической безопасности изучался такой нормативно-правовой акт, как Конституция Российской Федерации. Согласно Основному закону, Российская Федерация представляет собой светское и социальное государство, гарантирующее свободу слова, мысли, запрет цензуры и доступ к информации. Кроме того, учитывается запрет пропаганды или агитации, разжигающих социальную, расовую, национальную или религиозную ненависть и вражду. А также допустимость ограничения прав и свобод человека и гражданина федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства[21].

При исследовании принципов нельзя обойти стороной Федеральный закон «Об информации, информационных технологиях и о защите

информации» от 27.07.2006 года № 149 – ФЗ. В контексте информационно-психологической безопасности примечательны принципы:

«- обеспечение безопасности РФ при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

- достоверность информации и своевременность ее предоставления;

- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.» [35]

Кроме того, общим юридическим документом для всех сфер безопасности является Федеральный закон «О безопасности» от 28.12.2010 года № 390-ФЗ. Не смотря на то, что перечень принципов не большой и в какой-то степени дублирует положения Конституции Российской Федерации, как и другие правовые документы, он также содержит нормы «о приоритете предупредительных мер в целях обеспечения безопасности» [41].А также о « системности и комплексности применения мер обеспечения информационной безопасности» и «взаимодействие федеральных органов с международными организациями в целях обеспечения безопасности»[41].

Если говорить о законопроекте информационно-психологической безопасности, то примечательным в документе является принцип государственной монополии на разработку и производство специальных средств ИПВ [44]. Под специальными средствами подразумевается «технические и программные средства, используемые для негативного информационно-психологического воздействия на человека или группу лиц»[44]. Учитывая быстроразвивающийся мир, представленный принцип не лишён смысла. Страны с высоким уровнем информационного развития могут использовать свои наработки как оружие. В таком случае Российской Федерации требуется защита. С другой стороны не исключается злоупотребление своими должностными полномочиями отдельных лиц, в руках которых будут находиться «технические и программные средства»[44]. Следовательно, при закреплении вышеуказанного принципа стоит закрепить и

меру ответственности за злоупотребление или не законное применение специальных средств.

Так как в прошлой главе мы указывали международно-правовые стандарты, то при анализе принципов информационно-психологической безопасности следует обратить внимание и на международные нормативно-правовые акты. В частности на Устав организации объединённых наций. Важными принципами для ООН являют суверенность государств, невмешательство во внутренние дела государств, решение международных споров мирным путём[71]. Кроме этого, не наименее важным для Российской Федерации считается Решение Совета глав правительств СНГ от 25 октября 2019 года «О стратегии обеспечения информационной безопасности государств – участников содружества Независимых Государств»[40], который закрепляет правовое равенство участников информационного взаимодействия.

Исходя из проведённого исследования, были выявлены принципы информационно-психологической безопасности:

- соблюдение прав и свобод человека и гражданина;
- законность;
- развитие психологической защиты граждан РФ от информационно-психологического воздействия;
- свобода средств массовой информации;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- установление ограничений доступа к информации только федеральными законами;
- допустимость ограничения прав и свобод человека и гражданина в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;

- системность и комплексность применения правовых, организационных, информационных и иных мер обеспечения ИПБ;

- приоритет предупредительных мер обеспечения ИПБ;

- частно-государственное партнерство и международное сотрудничество в обеспечении ИПБ.

Таким образом, проанализировав понятие и принципы информационно-психологической безопасности, становятся понятны направления развития данной сферы и то, как можно защитить граждан Российской Федерации от информационно-психологического воздействия.

2.2 Деструктивно-информационно-психологическое воздействие как проблема Российской Федерации

Вскользь проблемы информационно-психологического воздействия упоминались и раньше. В данном параграфе они будут подробно разобраны с целью установления чётких путей их решения.

В условиях нынешних реалий большую часть своего времени граждане РФ поводят в Интернете. Отчёт ВЦИОМ свидетельствует о том, что на 2023 год доля тех, кто каждый день пользуется Интернетом, достигла 73%, а время проведённое пользователями в информационной среде достигает почти шести часов в день[57]. Данный показатель логичен, исходя из того, что информационные площадки сейчас стали средством для развития бизнеса, общения с друзьями, обучения и просто времяпровождения. Современный гражданин практически не выпускает телефон из рук, потребляя колоссальное количество информации. Многие учёные не только в России, но и в мире начали беспокоиться о том, как информационная среда влияет на человека. Проблема состоит в большом потоке информации во всемирной сети Интернет, часть из которой образует информационный мусор, негативно сказывающейся на пользователях. Само по себе информационное загрязнение (информационный мусор) представляет собой ненужную, малозначительную и

недостоверную информацию. Дружилов С.А. определяет информационные загрязнения как «поток дисгармоничной, хаотической, разрушительной информации, воздействующий на человека, преимущественно, через его зрение и слух» [16]. Оба определения будут справедливыми, однако, стоит добавить, что информационные загрязнения также влияют и на психику человека. В пример можно привести вброс фейковой информации о бронировании даты и времени для выезда за границу. Новость весьма встревожила россиян, однако, депутат от партии «Единая Россия» Евгений Москвичев опроверг фейк, объяснив, что данные требования вводятся для коммерческих грузовиков. Вброс сам по себе достаточно безобидный, но на его примере можно увидеть, как авторитет того или иного источника информации влияет на настроение в обществе. К сожалению, информационные загрязнения так или иначе будут присутствовать в жизни человека, так как Всемирная сеть Интернет – это система глобального масштаба. По сути именно сами пользователи создают информационный мусор, опасный и безобидные. Здесь для исследователей информационно-психологической безопасности и открываются два вопроса связанные с Всемирной сетью Интернет – бесконтрольное потребление информации, а также совершенствование механизмов по противодействию негативному-информационно-психологическому влиянию.

Дружилов С.А. в одной из своих статей указал понятие «модель мира человека», под которой подразумевал ту картину мира, которую человек формирует в своей голове об окружающей его действительности. Указанная модель состоит из двух разделов – понятийной и образной [16]. К понятийной относится восприятие мира через логику, составление причинно-следственных связей, изучение, анализ и синтез. Образная больше основывается на восприятие мира через эмоции, воображение. По качеству восприятия информации эти два аспекта значительно отличаются и важно, чтобы они работали сообща. Акторы всегда делали упор на эмоции и чувства своих объектов. Проблема нашего времени состоит в том, что человеку становится труднее анализировать информацию, предоставленную ему акторами. Не так

давно в научном мире появился термин «клиповое мышление», образованный от английского слова «clip», что значит вырезка или фрагмент. Это тип мышления, при котором человек воспринимает информацию только короткими кусками и яркими образами. Формируется клиповое мышление спустя время, вследствие бесконтрольного потребления информации. Конечно, нет ничего плохого в том, что в XXI веке можно быстро найти ответы на все вопросы. Однако, человек начинает привыкать к этому и в последующем уже не может вчитываться в длинные тексты, так как понятийный отдел восприятия, отвечающий за синтез и анализ, начинает слабеть. Становится гораздо легче и интереснее получать информацию через образы и эмоции. В свою очередь, акторы используют наши эмоции для достижения целей. Соответственно они создают информационное загрязнение, которое может иметь негативный характер, а общество с клиповым мышлением являются лёгким объектом для негативного-информационно-психологического воздействия.

Говоря об ответственности за негативно-информационно-психологическое воздействие, нельзя сказать, что в Российской Федерации она отсутствует. Например, если была задета репутация и честь гражданина, то он может обратиться в суд в соответствии со статьёй 152 ГК РФ, регламентирующей право человека требовать в суде опровержения порочащих его честь, достоинство или деловую репутацию сведений[13]. В данной статье присутствует оговорка: «если распространивший такие сведения не докажет, что они соответствуют действительности» [13]. То есть при возникновении дела по статье 152 ГК РФ судом будет проведена проверка доказательств с той и с другой стороны, что подтверждает принцип состязательности и равноправия сторон при рассмотрении дел в судах. Кроме того, за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, согласно статье 207.1 УК РФ предусмотрена ответственность, начиная от штрафа заканчивая лишением свободы, в зависимости от тяжести деяния[70]. Также Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях

и о защите информации» за распространение информации «…в целях совершения уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов…»[35], предусматривает ответственность для владельцев сайтов, размещающих такого рода информацию. Кроме того, не так давно в уголовное и административное законодательства, была введена достаточно важные статьи о кибербулинге. Статьёй 5.61 КоАП РФ предусмотрена ответственность в виде штрафа в размере от 5 до 10 тыс. рублей за оскорбление в социальной сети[22]. Уголовная же ответственность за «кибербуллинг» предусмотрена, в ст. 110.1 Уголовного кодекса УК РФ за склонение к совершению самоубийства или содействие совершению самоубийства[70]. Такое деяние, если совершено в отношении несовершеннолетнего, или в информационно-телекоммуникационных сетях, включая сеть «Интернет», наказывается лишением свободы на срок от 8 до 15 лет. Уголовная ответственность за данное деяние наступает с 16 лет. Представленные статьи достаточно важны для сохранения порядка в обществе и являются важным шагом к противодействию деструктивно-информационно-психологическому влиянию, но всё же данная сфера является ещё не до конца изученной и так как формируются новые методы воздействия, и следовательно, требуются разработки новых механизмов защиты. Вопросом на повестке дня является установление юридической ответственности за так называемые «deepfake» и «треш-стримы». Deepfake (глубокий фейк) – это «технологии искусственного синтеза человеческого изображения, основанные на использовании нейросетей искусственного интеллекта, позволяющие создавать высоко реалистичные фото- и видеоизображения людей либо производить модификацию фото-, аудио- и видеоматериалов»[64]. Под «треш-стримами» подразумевается трансляция на информационной платформе в режиме реального времени, где люди

выполняют задания, чаще всего аморального характера за денежную плату. Само по себе слово «треш» произошло от английского слова «trash», что означает мусор, отброс. Данные трансляции распространяются сейчас на таких платформах как Twich, Youtube и другие. В целях негативно-информационно-психологического воздействия глубокие фейки могут быть использованы в качестве влияния на российских граждан по средствам обмана. На 2023 год собралось множество примеров, когда акторы путём использования технологий примеряли на себя лица известных личностей и рекламировали сомнительные розыгрыши. Яркий пример, фальшивый рекламный ролик 2021 года, в котором основатель банка Тинькофф обещал подарить деньги. Сейчас такого рода фейки научились распознавать, да и сами граждане относятся насторожено к сомнительным сайтам и видео. Однако, прогресс не стоит на месте и вследствие гонки изучить и создать новую технологию, появляется больше возможностей для агрессивных акторов. Это требует от российского законодательства совершенствование правовых механизмов защиты. Если говорить про треш-стримы они как раз таки имеют прямое влияние на психику человека. Чаще всего они выходят из-под контроля, и проблема состоит в том, что деятельность треш-стримеров достаточно сложно контролировать, так как нет законодательной базы по данному вопросу.

Также, проблема не только Российской Федерации, но и всего мира это быстрое развитие искусственного интеллекта. Дело в том, что законодательство не успевает за разработкой всё новых и новых программ. Учёные стали всерьёз опасаться негативного воздействия искусственного интеллекта на общество. 28 марта 2023 года Илон Маск вместе с другими деятелями науки подписал открытое письмо с требованием приостановить разработку нейросетей. На данный момент нейросеть может сгенерировать портрет, найти ответ на любой вопрос и написать статьи по заданной теме. Кроме того, ещё в 2014 году бот, Евгений Густман, прошёл тест Тьюринга, убедив 33% судей, что он настоящий человек. Тогда победа Евгения Густмана стала прорывом в разработке искусственного интеллекта. На сегодняшний день каждое государство

продолжает финансировать научные разработки, стимулируя развитие искусственного интеллекта. Тем временем само общество остаётся слабо защищённым от информационно-психологического воздействия на законодательном уровне. Нет сомнений в том, что с развитием технологий жизнь человека становится проще и лучше. При этом нельзя допускать, что бы технологии опережали нормативно-правовое регулирование, иначе это может спровоцировать новые угрозы. В Российской Федерации Указом Президента РФ от 10.10.2019 года № «О развитии искусственного интеллекта в Российской Федерации» закреплены основные направления создания комплексной системы регулирования общественных отношений в связи с развитием и внедрением искусственного интеллекта. Одним из них является «разработка этических правил взаимодействия человека с искусственным интеллектом»[49]. Как отмечалась в первой главе, в будущем искусственный интеллект может стать новым субъектом информационно-психологического воздействия и очень важно уже сейчас, параллельно с созданием новых программ, разрабатывать правовую концепцию защиты общества от возможного негативного воздействия искусственного интеллекта. На данный момент времени в Российской Федерации сформирован Альянс в сфере искусственного интеллекта, который в 2021 году представил «Кодекс этики в сфере искусственного интеллекта»[28]. Правда данный документ носит исключительно рекомендательный характер и распространяется только на гражданские разработки. Ответственность за нарушение положений указанного документа отсутствует.

Следующим немаловажным аспектом в регулировании информационно-психологического воздействия является определение информационно-психологической безопасности и закрепление её на законодательном уровне. Раннее была дана характеристика информационно-психологической безопасности, а также подчёркивалось важность установления её принципов, задач и целей, так как именно изучив указанную сферу можно сформулировать чёткие направления и пути решения негативного информационно-

психологического воздействия. Сейчас в Российской Федерации информационно-психологическая безопасность размыта по отдельным нормативно-правовым актам, что усложняет разработку новых механизмов защиты.

Проблема также состоит в том, что если сторона вопроса, касающаяся информационных технологий и информации всё-таки защищена такими документами как Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 года №149-ФЗ, то психологическое воздействие только недавно нашло своё отражение в нормативно-правовых документах. В частности можно выделить статью 20.1. КоАП РФ, которая предусматривает ответственность за «распространение в информационно-коммуникационных сетях, в том числе в сети интернет»[22] неприличной информации способной оскорбить человеческое достоинство, а также отражает явное неуважение к государству и обществу. Также следует выделить Федеральный закон от 24.07.1998 года № 124 – ФЗ «Об основных гарантиях прав ребёнка в Российской Федерации»[34], регламентирующим меры защиты ребёнка от негативной информации, которая наносит вред его нравственному, психическому и духовному развитию, а также меры по содействию в их развитии. Если говорить о детях, то они достаточно хорошо защищены российским законодательством. Однако, в нашем мире психологическому воздействию подвержены не только дети, но и люди старшего возраста. В первой главе отмечалось, наиболее подвержены информационно-психологическому влиянию граждане с повышенным уровнем тревожности. В данную категорию входят не только подростки и люди пожилого возраста, но и другие категории граждан.

Говоря о психологическом воздействии, всегда стоит учитывать не только возраст, но и уровень психологического здоровья. В Российской Федерации существует бесплатная психологическая помощь в общеобразовательных учреждениях, кроме этого, имеется «общероссийский телефон доверия» куда гражданин может позвонить с волнующим его

вопросом, но есть люди, которые до сих пор бояться обращаться за психологической помощью. Отсюда следует ещё одна проблема - страх и недоверие к психологам. Пропаганда психологической помощи, поддержка государством исследований по разработке новых методов лечения, подготовка квалифицированных специалистов могла бы снизить количество людей подверженных негативному психологическому воздействию, а также построить благоприятную среду для создания здоровой семьи. Многие учёные и психологи утверждают, что одной из причины разводов становится отсутствие психологической помощи. К этому стоит добавить, что формирование ребёнка как личности начинается в семье, соответственно развод и нездоровые отношения в доме формирует тревожного гражданина, который является благоприятным объектом для психологического негативного воздействия.

Обращаясь к данным ВЦИОМ от 22 ноября 2022 года, можно проследить, что потребность в психологической помощи выросла среди молодёжи 18-24 лет на 35 %, а среди активных потребителей интернета на 23 %[9]. Обусловлена такая статистика напряжённой международной ситуацией и ежедневно оказывающимся негативно-информационно-психологическим давлением на население Российской Федерации. Опять же личность с устойчивой здоровой психикой имеет возможность критически оценить ситуацию. Соответственно они тяжелее поддаются влиянию агрессивных акторов, нежели люди, страдающие тревожными расстройствами. Тем не менее, психологическая помощь никак не закреплена на законодательном уровне. Сейчас работа над федеральным законом « о психологической помощи в Российской Федерации»[58] ведётся и был уже представлен законопроект. Однако, документ не соответствовал этическому кодексу психологов, поэтому его отозвали. Тем временем в Федеральный закон от 21.04.1994 года №68-ФЗ «О защите населения и территорий от чрезвычайных ситуация природного и техногенного характера» были внесены поправки в 4 и 18 статьи, в которых теперь регламентируются права граждан на оказание психологической помощи

при чрезвычайных ситуациях [39]. Указанные изменения можно считать ещё одним шагом государства к поддержке психологической помощи.

Немаловажным будет и принятие нормативно-правового акта посвящённого психологической помощи, который бы давал чёткое определение о том, кто такой психолог, а также регламентировал бы деятельность специалистов, устанавливал права и обязанности психолога и требования к образованию. Проблема недоверия людей к психологам заключается в том, что нет чётких требования к специалистам. Чаще всего психологи, оказывающие бесплатную психологическую помощь, не обладают достаточными знаниями. Впоследствии состояние гражданина либо не изменяется, либо ухудшается. К платным специалистам граждане чаще всего не хотят обращаться из-за страха и завышенных цен. Чаще всего, конечно, проблемы действуют в совокупности. Сейчас с целью их устранения в Российской Федерации идёт работа над совершенствованием психологической защиты, что является важным этапом в противоборстве с негативно-информационно-психологическим воздействием.

Таким образом, анализируя деструктивно-информационно-психологическое воздействие как проблему Российской Федерации и выявив её основные аспекты, можно увидеть какие механизмы для защиты есть сейчас и что следует усовершенствовать для улучшения информационно-психологической безопасности.

2.3 Правовые средства и механизмы защиты от деструктивного-информационно-психологического воздействия

На данный момент времени существуют определённые средства и механизмы воздействия для защиты от информационно-психологического влияния. Что бы их выделить для начала стоит проанализировать методы защиты. В теории права есть общепринятое понятие методов правового регулирования, которое представляет собой «совокупность приемов и способов воздействия на субъектов общественных отношений» [3]. Основными методами

правового регулирования является императивный и диспозитивный метод. Сам по себе императивный метод – это «совокупность приемов и способов, построенных на началах субординации участников правоотношений»[3]. При императивном методе правового регулирования субъекту не предоставляется выбор, отношения основаны на подчинении. В свою очередь императивные методы делятся на запрещающие и обязывающие. Что касается диспозитивных методов, то они подразумевают под собой совокупность методов основанных на равноправие сторон и предоставляют человеку выбор при совершении им каких-либо действий. Подразделяется он на дозволение, рекомендации и поощрение. Проанализировав нормативно-правовые акты, касающиеся информационно-психологической безопасности можно сказать, что сейчас государством используются оба метода правового регулирования. Например, диспозитивный метод присутствует в ч. 2 ст. 14 Закона «О защите детей от информации, причиняющей вред их здоровью и развитию» закрепляет диспозитивную норму, согласно которой не являющийся сетевым изданием интернет-ресурс может содержать возрастную маркировку информационной продукции, которая присваивается ими самостоятельно[38]. Однако, в большей степени всё-таки преобладает императивные нормы. Если рассматривать механизм правовых запретов информационно-психологического воздействия, то к ним можно отнести:

- запрет «злоупотребления свободой массовой информации» [45] (ст. 4 Закона о СМИ);

- запрет «распространения противоправной информации» [35] (ч. 6 ст. 10 Закона об информации);

- запрет «распространения сообщений и материалов иностранного СМИ, выполняющего функции иностранного агента, и (или) учрежденного им российского юридического лица без указания на то, что эти сообщения и материалы созданы и (или) распространены такими лицами» [35] (ч. 7 ст. 10 Закона об информации);

- «запрет недобросовестной и недостоверной рекламы»[36] (ч. 1 ст. 5 Закона о рекламе);

К обязывающим методам диспозитивного регулирования можно отнести нормативно-правовые нормы установленные, в частности, для: организатора распространения информации в сети Интернет (далее – ОРИ) (ст. 10.1); оператора поисковой системы (ст. 10.3); новостного агрегатора (ст. 10.4); владельца аудиовизуального сервиса (ст. 10.5); владельца социальной сети (ст. 10.6)[35].

Третьим правовым способом регулирования обеспечения ИПБ выступает дозволение, которое преимущественно используется в информационном праве при регламентации правового статуса физических лиц. Об этом свидетельствует ст. 15.1-2 Закона об информации предоставляет гражданину право в случае обнаружения в Интернете недостоверных порочащих сведений информации, связанных с обвинением в совершении преступления, направить прокурору субъекта РФ обращении о принятии мер по удалению указанной информации или блокировке распространяющих их интернет-ресурсов[35].

На методах правового регулирования базируются механизмы правовой защиты. Они представляют собой комплекс правовых средств, служащих для регулирования и установления порядка в общественных отношениях. Соответственно в качестве правых механизмов от информационно-психологического воздействия можно выделить:

- Закрепление правовых запретов и иных ограничений на распространение определенных видов негативной информации. Данные ограничения могут выражаться в установление правовых норм, которые устанавливают либо временные ограничения на определённый круг лиц, либо постоянные. Правовой запрет характеризуется установлением рамок для той или иной деятельности физических и юридических лиц при реализации их деятельности. Примером может служить статья 4 Закона о СМИ «злоупотребления свободой массовой информации» [45].

- Установление специальных правил оборота информационной продукции определенных видов. В пример можно привести статью ст. 13 Федерального закона от 29.12.2010 года №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Согласно ей информационная продукция, содержащая информацию определённого контента, перечень которого закреплён в том же законе, «не подлежит распространению посредством теле- и радиовещания с 4 часов до 23 часов по местному времени, за исключением теле- и радиопрограмм, теле- и радиопередач, доступ к просмотру или прослушиванию которых осуществляется исключительно на платной основе с применением декодирующих технических устройств, обеспечивающих доступ к указанной информационной продукции только лиц, достигших восемнадцатилетнего возраста, путем введения кодов или совершения иных действий, подтверждающих возраст этих лиц»[38]. Для части сведений категории «16+» допустимый временной интервал показа определен с 7 до 21 часа.

- Закрепление обязанностей субъектов информационных правоотношений по обеспечению ИПБ. Примером будет являться Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» регламентирующий обязанности: организатора в распространении информации в сети «Интернет» (ст. 10.1), оператора поисковой системы (ст. 10.3); новостного агрегатора (ст. 10.4), владельца аудиовизуального сервиса (ст. 10.5), владельца социальной сети (ст. 10.6) [35]. Все приведённые статьи, во-первых, дают определение указанным понятием, кроме того закрепляют их обязанности в области защиты российских граждан от информационно-психологического воздействия. Правовая норма, закрепляющая обязанности владельца социальной сети, стала важным шагом для преодоления негативного воздействия на российских граждан во Всемирной сети Интернет. Ранее защита пользователей информационной среды была нестойкой, сейчас же законодательный орган установил запрет на

недопущение владельцами сайтов размещение себя экстремистских призывов, информации порочащих честь и достоинство граждан и другие.

- Возрастная классификация и маркировка информационной продукции. Статьёй 12 Федерального закона от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» установлена маркировка информационной продукции для детей, не достигших возраста шести лет (0+); информационная продукция для детей, достигших возраста шести лет (6+); информационная продукция для детей, достигших возраста двенадцати лет (12+); информационная продукция для детей, достигших возраста шестнадцати лет (16+); информационная продукция, запрещенная для детей (18+)[38]. Данная норма как раз сформировалась благодаря диспозитивному методу. Гражданин заходя на сайт или просматривая определённый контент встречается с оповещением о возрастной маркировке, предупреждающей о содержании того или иного продукта. Тем самым гражданину предоставляется выбор, хочет ли он смотреть размещённую информацию или нет. Конечно, представленный механизм не всегда работает, поэтому с целью уберечь детей от противоправного контента в развитых странах были созданы программы «родительский контроль». В России такая программа называется Kaspersky Safe Kids, создана Kaspersky Lab и базируется на нормативно-правых актах, касающихся защиты детей.

- Экспертиза информационной продукции. Основным нормативным правовым актом, регламентирующим экспертную деятельность в РФ, выступает Федеральный закон от 31 мая 2021 г. № 73-ФЗ «О государственной судебно-экспертной деятельности»[54]. Закон об экспертизе регламентирует производство экспертизы в рамках уголовного, гражданского и административного судопроизводства. Такие экспертизы проводятся по делам о преступлениях, административных правонарушениях или гражданско-правовых деликтах, связанных с оказанием деструктивного ИПВ (например, дела о возбуждении ненависти либо вражды, а равно унижении человеческого достоинства). Однако в правоприменительной практике также проводятся

экспертизы вне рамок судопроизводства по заданиям правоохранительных органов, организаций, частных физических и юридических лиц. Так, Закон об информации закрепляет возможность проведения экспертизы информационной продукции в целях проверки обоснованности присвоенной возрастной классификации. Порядок проведения такой экспертизы регламентирован приказом Минкомсвязи России. Основным видом экспертиз в сфере ИПБ выступает лингвистическая экспертиза текста.

- Идентификация личности абонентов, пользователей сети Интернет и цифровых сервисов. Согласно статье 2 Федерального закона от 29.12.2022 N 572-ФЗ « идентификация - совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с идентификатором»[37]. Идентификация личности играет важную роль в защите от информационно-психологического воздействия, так как способствует быстрому вычислению правонарушителя. Сама анонимность является хорошим прикрытием и даёт лишний повод для негативного информационного вброса, поэтому запрос данных необходим для соблюдения порядка. Однако, запрос данных должен быть сбалансированным и осуществляться только в рамках закона. Государственные органы, действующие в рамках российского законодательства и осуществляющие информационно-психологическую безопасность, должны учитывать право на конфиденциальность и защиту личных данных граждан.

- Удаление или ограничение доступа к противоправному контенту. Основные правовые механизмы ограничения доступа к противоправному контенту регламентированы Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ. Например, в 2012 году законодательным органом была введена статья 15.1 о реестре доменных имён, куда стали вносить все интернет-ресурса нарушающие законы Российской Федерации[35]. В 2019 года в Федеральный

закон об информации была введена статья, регламентирующая порядок ограничения информации, оскорбляющей человеческое достоинство и выражающаяся в неприличной форме[35]. Нормативно-правовая норма также закрепляет полномочия специальных органов в сфере информационно-психологической безопасности. В частности удалением и ограничением доступа нежелательной информации занимается Роскомнадзор. Кроме того, контроль за противоправным контентом осуществляется также самими гражданами, местным самоуправлением и общественными организациями. При обнаружении противоправного контента они могут подать жалобу в Генеральную прокуратуру, Роскомнадзор или в Министерство внутренних дел Российской Федерации.

- Установление юридической ответственности за правонарушения, посягающие на ИПБ. В прошлой главе были указаны виды ответственности за деструктивно-информационно-психологическое воздействие. В большей степени при выявлении правонарушения используются уголовная и административная ответственность. По мимо указанных видов ответственности используется гражданско-правовая. За небольшой отрезок XXI века мы увидели, что российское законодательство не стоит на мете и идёт по пути развития в сфере информационно-психологической безопасности. В тоже время не стоят на месте и акторы, спектр угроз расширяется, поэтому создаются новые дополнения составов правонарушений.

- Правовое регулирование мер контрпропаганды. Под данным термином понимается применение мер противоположных пропаганде актора в целях нейтрализации источника деструктивной информационной активности. В российском информационном законодательстве отсутствуют нормы, комплексно регулирующие данное направление деятельности. Фрагментарное правовое регулирование по данному вопросу имеется в Федеральном законе «О противодействии терроризму»[55] и ряде иных законодательных актов, относящихся к сфере административного права.

- Правовое стимулирование развития цифровой грамотности и формирования культуры информационной безопасности в наше время является достаточно важным механизмом для защиты общества от негативного информационно-психологического воздействия. Осознанное потребление информации должно воспитываться в человеке с детства. Исходя из этого Правительством Российской Федерации 28 апреля 2023 года была утверждена концепция информационной безопасности детей, в который государство ставит перед собой такие задачи как: проведение мероприятий, направленных на повышение грамотности детей по вопросам информационной безопасности, формирование навыков законопослушного и ответственного поведения в цифровой среде; формирование у детей навыков самостоятельного и ответственного потребления информационной продукции»[26] и так далее.

Указанные положения являются достаточно важными для определения направления, в котором будет развиваться защита молодого поколения от негативного информационно-психологического воздействия. Однако, пропаганда здорового информационного потребления должна быть направлена не только на детей, но и на взрослое поколение.

Таким образом, завершая данный параграф, хочется отметить, что несмотря на отсутствие нормативно-правового акта о информационно-психологической безопасности в российской Федерации успешно применяются механизмы защиты от информационно-психологического воздействия, однако, в условиях модернизации информационного общества и совершенствования новых технологий требуются новые, дополнительные методы. При анализе, как уже было упомянуто выше, было замечено, что Российская Федерация не останавливается, а идёт по пути развития механизмов защиты в информационно-психологической безопасности.

Глава 3 Проблемы и перспективы развития системы правового обеспечения информационной безопасности от деструктивно-психологического воздействия в России

3.1 Анализ влияния деструктивного информационно-психологического воздействия на граждан Российской Федерации

Ранее нами была представлена статистика ВЦИОМ, отражающая кто из граждан и каким источником информации пользуется. В следствии был сделан вывод, что гибридная модель медиапотребления преобладает в российском обществе, но всё-таки Всемирная сеть Интернет является тем средством, которым потребитель пользуется чаще всего. Согласно опросу ВЦИОМ за май 2023 год процент пользователей, кто обращается к Интернету, практически ежедневно, составляет 73%[57]. Многие СМИ используют сейчас Всемирную сеть как платформу для работы, так как бумажный вариант журналов и газет постепенно уходят на второй план. Соответственно агрессивные акторы не отстают от времени и в основном воздействуют на свой объект через Всемирную сеть, нежели чем через другие средства. Из этого следует, что в основном российские граждане подвергаются деструктивно-информационно-психологическому воздействию, проводя время на интернет-платформах.

Сейчас животрепещущей темой являются фейковые новости. Они уже были затронуты в прошлых главах. Теперь стоит дать оценку их влияния на российское общество. Фактчекинговой компанией «Лапша Медиа» были выявлены три темы, которые подвергаются фальсификации: в сфере здравоохранения, специальная военная операция, политика и государственная безопасность[65]. Компания Rambler&Co с 1 по 4 марта 2023 год среди 458 525 пользователей провели опрос с целью выявить, могут ли граждане РФ отличить ложь от правды[19]. В итоге большинство граждан РФ, а именно 62%, уверенны, что могут распознать фейк. При этом в качестве признаков достоверной информации в СМИ пользователи назвали непредвзятость(59%),

ссылка на источники информации(18%), профессиональный и лаконичный язык(10%), а также наличие профессионального слога (7%) и отсутствие эмоциональной окраски (6%)[19]. Данное исследование наводит на мысль о том, что в российском обществе есть устойчивость к фейкам. Однако, нужно понимать, что опрос Rambler&Co проводился среди 458 525 пользователей из 146 424 729 граждан, проживающих на территории РФ. Вместе с тем стоит отметить, что борьба с ложными новостями не пускается на самотёк. Наоборот, на территории Российской Федерации развернулась сеть фактчекинговых компаний, которые анализируют информацию и выявляют фейки. Примером такой компании может послужить «Лапша Медиа», образованная АНО «Диалог Регионы» в 2022 году. Компания поддерживает связь с гражданами и реагирует на присланную информацию с просьбой о проверке на достоверность. Кроме того, есть определённые интернет-платформы, которые проверяют сайты, информацию, а также лиц, выкладывающих определённую статьи или посты.

К сожалению, не все граждане знают о таких сайтах и компаниях. Помимо этого не многие люди могут владеть собой в силу своих психологических особенностей. Примером может быть ситуация, которую мы затрагивали в прошлой главе касаемо введения новых условий для выезда за границу «всех автомобилей без исключения». Мы обратились к новостному источнику, что бы проанализировать реакцию граждан на подобную новость. Лента.ру в VK в январе 2023 года опубликовали пост о принятие новых положений, закрепляющих требование, бронировать дату и время для выезда за границу [18]. Многих пользователей взволновала подобная новость. Кто-то отнёсся к ней скептически, но всё-таки их число составляет малый процент. Ко всему прочему активизировались так называемые «интернет-тролли», которые провоцировали и подстрекали других. В результате чего разгорелся спор. «Интернет-тролль» это жаргонное слово, давно вошедшее в обиход пользователей интернета. С акторами они похожи тем, что их задачей является расшатать человека, вывести его из равновесия. Только, если перед актором

стоит определённая цель (нарушение общественного порядка и устройства государства), то «интернет-тролль» чаще всего провоцирует конфликт ради собственного удовольствия. Примечательно, что после аккаунты «интернет-троллей» были удалены из социальной сети. Вероятно, благодаря жалобам пользователей или жалобам администраторов группы.

Популярным фейком на 2022 год-2023 год также является вторая волна мобилизации[61]. Как мы выявили из нашего исследования, фальшивая информация чаще всего вбрасывается не просто так. В большинстве случаев актор использует тревожащие события мирового масштаба или в пределах страны. Таким примером и стала новость о повторной мобилизации в феврале 2023 года. В результате мнения снова разделились. Кто-то изначально не верил во вторую волну мобилизации, приводя конкретные аргументы против. Кто-то находился в состоянии паники. Так как информация распространилась по всем социальным сетям, общество взволновалось ещё сильнее. После опровержения государственными властями данного фейка уровень беспокойства немного снизился.

Анализируя приведённые выше ситуации, мы сделали вывод, что помимо новостных источников информации акторы, подобно «интернет-тролям», используют комментарии для вброса фейка. Примером может служить ситуация с постом о введение условий для выезда за границу. При этом мы также можем заметить, как быстро активизировался механизм общественного контроля, так как аккаунты агрессивных комментаторов были удалены из социальной сети VK. Согласно правилам социальных сетей пользователи обязаны соблюдать российское законодательство. Например, такие положения как запрет на нецензурную брань, разжигание розни, унижение достоинства человека и гражданина. Аккаунты тех, кто не соблюдает пользовательские соглашения, удаляются разработчиками. Каждая социальная сеть и интернет-сообщество предусматривает свои правила, которые в свою очередь не должны противоречить законодательству РФ. Исходя из этого, можно сделать вывод о том, что помимо нормативно-

правовых актов на законодательном уровне, в сети интернет действуют так называемые локальные акты, вроде соглашений «подписываемых» пользователями при регистрации, а также правила отдельных сообществ. Деятельность самих сообществ регулируется как правилами, установленными разработчиками, так и нормативно-правовыми актами на законодательном уровне. Например, в 2020 году в Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» была введена статья 10.6, с требованием к владельцам не допускать использование их сайтов с целью распространения нецензурной брани, распространение информации, способной разжечь конфликт и других запрещённых действий[35]. Нарушение владельцем сайта информационного законодательства влечёт за собой дисциплинарную, уголовную, гражданско-правовую и административную ответственность. Тем временем правилами социальных сетей, например VK, также предусмотрено ряд запретных действий, например, нельзя публиковать сомнительный и запрещенный контент, запрещенные услуги и другое. Санкция, которую может применить администрация социальной сети – блокировка аккаунта.

На самом деле популярность Всемирной сети Интернет не значит, что акторы не пользуются другими средствами для негативно-информационно-психологического воздействия. Ярким примером является объявление по радио- и телеканалам об угрозе ракетного удара в Белгороде, Воронеже, Уфе, Казани и других городах России[73]. Исследуя представленную ситуацию, мы заметили разный уровень воздействия на жителей РФ. Например, горожане Уфы предположили, что был осуществлён взлом, так как тревога прозвучала только с одной радиостанции в их городе, с Comedy Radio. В большей степени фейковое оповещение напугало жителей приграничных областей. Граждане, проживающие дальше от границы с Украиной, воспринимали информацию более спокойно и были способны адекватно оценить обстановку в отличие от тех, кто проживал у самой границы. Однако, благодаря оперативному реагированию со стороны МЧС ситуация быстро прояснилась.

Если оценивать произошедшее в целом, то можно сделать вывод – в большинстве своём россияне смогли быстро распознать атаку актора. Однако, удачная попытка взлома радио- и телестанций наводит на мысль о пробеле в защите информационных систем. Примечательно, что взлом произошёл на коммерческих станциях, что говорит о действиях целенаправленного характера. Как отмечают эксперты, это произошло из-за неподготовленности сотрудников к подобным атакам. В отличие от частных станций, государственные каналы хорошо защищены, и их безопасность регулируется Федеральным законом «О безопасности критической информационной инфраструктуры российской Федерации » от 26.07.2017 № 187-ФЗ. Согласно ст.4 ФЗ «О безопасности критической информационной инфраструктуры российской Федерации » от 26.07.2017 № 187-ФЗ принципами обеспечения безопасности критических инфраструктур являются: законность, непрерывность и комплексность обеспечения безопасности критических инфраструктур, а также приоритет предотвращения компьютерных атак. Под объектами критической информационной инфраструктуры подразумевается информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической инфраструктуры[42]. Указанным федеральным законом регламентируются права и обязанности субъектов критической инфраструктуры, требования по обеспечению безопасности значимых объектов КИИ (критической информационной инфраструктуры). В свою очередь требования по безопасности КИИ подробно раскрываются в Приказе ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»[48]. Кроме того, за нарушение требований ФЗ «О безопасности критической информационной инфраструктуры российской Федерации» от 26.07.2017 № 187-ФЗ предусмотрена уголовная ответственность. В частности, ст. 274.1. УК РФ предусмотрена ответственность за «неправомерное воздействие на критические информационную инфраструктуры РФ» [70], а также «нарушение правил

эксплуатации средств хранения, обработки и передачи охраняемой информации»[70].

То есть в случае хакерской атаки объекты информационной государственной инфраструктуры остаются под защитой законодательства РФ, следовательно, сохраняется и информационно-психологическая безопасность населения Российской Федерации. При нарушении требований сотрудниками информационной безопасности государственных информационных инфраструктур следует ответственность, предусмотренная законодательством о защите КИИ. Таким образом, возвращаясь к проблеме коммерческих радио- и теле- сетей, мы выявили, что защита некоторых из них представляется куда слабее, чем защита государственных сетей. Причиной является отсутствие специальной подготовки сотрудников и, возможно, отсутствие инструкций к подобным взломам. В то же время стоит упомянуть, что за вторжение в теле- и радиоэфир в независимости от того, кому принадлежит данная сеть предусмотрена административная ответственность согласно ст. 13.18. КоАП РФ влечёт наложение штрафа. Однако, размер штрафа составляет для граждан - от пятисот до одной тысячи рублей; для должностных лиц – от одной тысячи до двух тысяч; на юридических лиц- о десяти тысяч двадцати тысяч [22].

Подводя итоги произошедшей ложной тревоги можно сделать определённые выводы. Данная ситуация произошла из-за слабой защиты коммерческих радио- и теле- сетей. Касаем граждан, как мы уже отмечали, реакция была разная и зависела от расположения города, то есть от обстоятельств, в которых находились люди. Тем не менее, многие россияне смогли быстро распознать фейк, так как согласно инструкции гражданской обороны существуют определённые сигналы для оповещения. Например, «воздушная тревога», «отбой воздушной тревоги»[20]. Помимо, этого в случае реальной угрозы оповещение передаётся по всем каналам, а не по их ограниченному количеству. На основе приведённых положений большинство граждан отмечали не состыковки с оповещением 22 февраля 2023 года, что ещё

раз подтверждает наличие определённого уровня устойчивости граждан РФ к фейкам.

В первой главе были выделены такие методы деструктивно-информационно-психологического воздействия, как убеждение и внушение. Эти методы не раз применялись на гражданах разных стран, включая и Российскую Федерацию. Данные методы применяются при создании фейковых статей, постов, рекламы, а также в речи актора. Для того, что бы повлиять на сознание общества той или иной страны в речи актора используется призывы к чему либо, выставление в плохом свете своего оппонента, давление на жалость и прочее. Влияние таких методов зависит, как было сказано в прошлой главе, от степени образованности, осведомлённости граждан в той или иной сфере.

В период информационных войн, как между странами, так и внутри страны чаще всего в качестве средства применяется вброс ложной информации или хакерские атаки. Также не стоит забывать о тематической рекламе. Так с начала СВО было выпущено множество тематической рекламы. Примером является ролик, в котором российских военных призывали сдаваться и обещали им безопасность на территории Украины[72]. В рекламе был использованы видео якобы с пленными российскими военными, лаконичные призывы к действию. В основном многие россияне отнеслись скептически к таким роликам, однако, уровень тревожности был повышенный, особенно в начале специальной операции. Многие сайты с подобной рекламой, после жалоб граждан РФ, стали блокироваться Роскомнадзором. Также были найдены опровержения тематических роликов. Сейчас отношение к подобным роликам среди российского общество чаще всего встречается негативное.

Таким образом, исследуя реакцию граждан на деструктивно-информационно-психологическое воздействие, мы сделали определённые выводы. Во-первых, устойчивость граждан РФ к фейкам зависит от обстоятельств, в которых человек находится, и от его психологических особенностей. Кроме того, зависит от образованности граждан и осведомлённости. Во-вторых, стоит отметить действие общественного

контроля в первой ситуации, которая доказывает важность данного механизма в жизни общества. В-третьих, в сравнении с другими платформами для информации, сеть Интернет является наиболее популярной. Можно сказать, что Всемирная сеть Интернет стала отдельным миром, в котором права граждан защищены, но частично.

3.2 Развитие системы органов обеспечения информационно-психологической безопасности

Эксперты подразделяют систему безопасности на две подсистемы – государственную и негосударственную. Чтобы исследовать систему органов обеспечения информационно-психологической безопасности, мы обратились к Федеральному закону «О безопасности» от 28.12.2010 года № 390-ФЗ, согласно которому в систему государственных органов по обеспечению безопасности Российской Федерации входят Президент РФ, палаты Федерального Собрания РФ, Правительство РФ, а также федеральные органы исполнительной власти[41]. Изучив, подробно деятельность каждого государственного органа, мы выявили, что каждый из них так или иначе задействован в обеспечении информационно-психологической безопасности, но непосредственное участие принимают лишь несколько органов, в частности федеральные исполнительные органы государственной власти, в число которых входит Минцифры РФ, Роскомнадзор, МВД РФ, ФСБ РФ, Минобороны и МИД РФ.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации является федеральным органом исполнительной власти подотчётным Правительству Российской Федерации. Данный государственный орган можно назвать важной составляющей в обеспечение информационно-психологической безопасности, так как именно он осуществляет функции «по выработке и реализации государственной политики и нормативно-правому регулированию в сфере информационных технологий»[52], а также массовых коммуникаций и средств массовой информации. Важно отметить, что

Минцифры РФ занимается разработкой политики и нормативных проектов по защите детей от информации, которая может нанести вред их психологическому здоровью. Примером может являться разработка концепции цифровой защиты детей. Как отмечается в информации на сайте самого министерства, цель концепции – защитить детей от информационных угроз. В качестве одной из задач приводится приучить детей к безопасному поведению в интернете и социальных сетях, а также научить их распознавать мошенников[32]. Данный документ является достаточно значимым для того, чтобы воспитать в новом поколении устойчивость к информационно-психологическому воздействию. Кроме того, Минцифры РФ разрабатывают требования к защите сетей связи от несанкционированного доступа, а также осуществляет координацию и контроль деятельности, находящихся в её введении службы, то есть Роскомнадзора РФ[52].

Федеральная служба в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор РФ) «осуществляет функции по контролю и надзору в сфере средств массовой информации, в том числе в сфере электронных и массовых коммуникаций, информационных технологий»[53]. Это федеральный орган исполнительной власти, непосредственно осуществляющий защиту граждан Российской Федерации от деструктивно-информационно-психологического воздействия. Согласно, постановлению Правительства РФ от 16.03.2009 года «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» к полномочиям Роскомнадзора относится контроль за:

- «соблюдением законодательства РФ о защите детей от информации, причиняющей вред их здоровью и развитию;

- соблюдением требований в связи с распространением информации и информационно-телекоммуникационных сетях, в том числе в сети «Интернет»;

- в области телевизионного вещания и радиовещания»[53];

Также к деятельности Роскомнадзора относится «создание реестра домённых имён, указателей страниц сайтов и сетевых адресов, содержащих

информацию, запрещённую к распространению на территории РФ» и «принятие мер по ограничению доступа к информационным ресурсам, нарушающим законодательство РФ»[53]. В качестве ограничительных мер Роскомнадзор блокирует сайты, распространяющие недостоверную информацию, призывающие совершать граждан РФ противоправные деяние и массовые беспорядки.

Что касается Министерства внутренних дел Российской Федерации, то он является основным органом в противодействии преступности в сфере информационных технологий. В частности в структуре министерства есть отдел именуемый Управлением по организации борьбы с противоправным использованием информационно-коммуникационных технологий. В компетенцию отдела входит противодействие преступности в сфере информационных технологий и анализ данных информационно-телекоммуникационных сетей, в целях выявления запрещённого контента, что также влияет на информационно-психологическую безопасность граждан. Кроме того, в полномочия МВД РФ входит противодействие административным правонарушениям в сфере ИПБ и противодействие терроризму и экстремизму[47].

Если говорить о Федеральной службе безопасности Российской Федерации, то в отличие от МВД РФ, его основной деятельностью является защита информации и информационных систем. В целях защиты государства и российского общества от деструктивно-информационно-психологического воздействия ФСБ РФ исполняет функции, касающиеся разведывательной и контрразведывательной деятельности. Например, органы безопасности проводят контрразведывательные мероприятия в целях противодействия «разведывательной и иной деятельности специальных служб и организаций иностранных государств, а также отдельных лиц, направленной на нанесение ущерба безопасности Российской Федерации»[43].

Деятельность Минобороны России в сфере обеспечения информационно-психологического воздействия можно проследить в отдельных правовых

нормах. Согласно г.II ч.7. п.40 Указа Президента РФ от 16.08.2004 года № 1082 «Вопросы Министерства обороны РФ» в полномочия министерства входит совершенствование системы Вооружённых сил РФ, в число которых включена защита военнослужащих от психологического воздействия со стороны противника[7]. Так же на Минобороны РФ возложена ответственность за сохранение и приумножение патриотических традиций. То есть, можно сказать, что данное Министерство принимает непосредственное участие в борьбе с деструктивно-информационно-психологическим влиянием, осуществляя как внешнее, так и внутреннее противодействие агрессивным акторам.

Говоря о полномочиях Министерства иностранных дел РФ[8], можно отметить, что основной функцией данного органа выступает информационное обеспечение внешней политики и противодействие негативным информационным вбросам в адрес Российской Федерации, а также международных организаций. Роль МИД в сфере обеспечения информационно-психологической безопасности состоит в продвижении национальных интересов России на международной арене, организации международного сотрудничества в области противодействия информационным угрозам.

Исследуя нормативно-правовую базу касаемо изучаемых государственных органов, мы выявили, что каждый из них выполняет определённую функцию для обеспечения информационно-психологической безопасности. Эксперты отмечают, что в нынешнее время нет потребности создавать отдельный орган по борьбе с информационно-психологическим воздействием. Мы согласимся с данным утверждением, так как вопрос информационно-психологического воздействия проникает во многие отрасли и сейчас создание отдельного государственного органа представляется нам нецелесообразным. Однако, подготовка специалистов, которые будут специализироваться на выявлении информационно-психологического воздействия, является важным шагом к борьбе против данного явления.

Помимо этого мы предлагаем также образовать отдел по борьбе с деструктивно-информационно-психологическим воздействием на базе Министерства внутренних дел Российской Федерации, состоящий из специалистов, располагающих нужными знаниями в сфере информационных технологий, психологии, профайлинга и тог далее. Создание такого отдела позволит быстрее реагировать на действия агрессивных акторов. Кроме того, позволит выработать определённые методы борьбы в целях обеспечения информационно-психологической безопасности.

Помимо государственной системы обеспечения, в Российской Федерации действует негосударственная система, которая подразумевает под собой средства массовой информации, общественные объединения, образовательные организации, ИТ-компании и самих граждан. В прошлом параграфе был исследован случай общественного контроля, который доказывает важность участия негосударственных институтов в обеспечении информационно-психологической безопасности. Не только частные компании, но и сами граждане способны противостоять акторам, используя механизмы, предоставляемые социальными сетями, например, жалобы. Сейчас на просторах российского Интернета действует кибердружина – сообщество волонтёров, которое помогает правоохранительным органам бороться с правонарушениями в информационной среде. В функции объединения входят: мониторинг сети Интернет в целях выявления противоправного контента; направление сведений в правоохранительные органы; осуществление исследовательской и просветительской деятельности. Под противоправной информацией, которую ищут волонтёры, подразумевается: пропаганда запрещённых веществ, призывы к насилию; подстрекательство к самоубийству; распространение контента «18+»; распространение детской порнографии и другое. При выявлении противоправного контента, волонтёры либо обращаются к администраторам социальной сети с просьбой заблокировать контент, либо в прокуратуру.

Ещё в 2019 году в Государственную Думу был внесён проект федерального закона о кибердружине. Предполагалось, что в каждой области будет основана кибердружина, в состав которой входили бы граждане не моложе 18 лет, не страдающие алкогольной и наркотической зависимостью. Финансирование должно было производиться из регионального бюджета. В конце концов, после нулевого чтения, проект закона отправили на доработку, так как были выявлены некоторые пробелы, касающиеся пределов полномочий кибердружины.

На самом деле, возведение кибердружины в статус общественной организации значительно облегчило бы работу в выявлении правонарушений. При этом нужно проработать систему кибердружины, то есть схему их методов, функций и требования к кибердружиникам. Мы согласны с требованиями, приведёнными в законопроекте, но также хотелось бы добавить о специализации волонтёров. Данная организация подразумевает деятельность на добровольных началах, в независимости от того какими образованием обладает член объединении, однако, для успешной работы в сфере информационно-психологической безопасности также должны быть граждане, обладающие психологическим образованием и ИТ-образованием. Кроме того, стоит сказать о том, что мы поддерживаем идею просветительской деятельности кибердружины и именно для этого в составе объединения должны быть граждане, обладающие соответствующей профессиональной подготовкой, а также для успешного установления признаков деструктивно-информационно-психологического воздействия.

Также для нормального функционирования кибердружин, как и для любой системы, требуется координирующий орган, который будет регулировать деятельность волонтёров. В качестве такого органа можно рассматривать организацию «Лига безопасного интернета», так как она и является создателем этого проекта.

Кроме всего вышеперечисленного, предлагается повысить качество психологической помощи, так как при информационно-психологическом

воздействии большую роль играет психологическая устойчивость со стороны гражданина РФ. В первую очередь нужно обратить внимание на общеобразовательные учреждения. Проблема состоит в том, что чаще всего дети бояться обращаться за психологической помощью из – за неуверенности и страха. На протяжении исследования было выявлено, что одной из категорий подверженной информационно-психологическому воздействию являются подростки. Следовательно, в случае проблемы, связанной с семьёй, сверстниками, деструктивными сообществами, подросток должен понимать, куда он может обратиться за помощью кроме семьи, если родственники не могут ему помочь. В большей степени здесь играет роль «здоровая пропаганда» психологической помощи со стороны государства. Конечно, важной составляющей является и принятие закона о психологической помощи, который мог бы защитить граждан Российской Федерации от мошенников, именуемых себя психологами.

Также если говорить об общеобразовательных учреждениях, предлагается разработать программу по воспитанию осознанного интернет-потребления. В прошлых главах нами было установлено, что проблема нового поколения – клиповое мышление. При таком виде мышления человек не способен анализировать информацию, восприятие реальности основано в большей степени на эмоциях. Следовательно, человек становится легко внушаемым и актор может легко им манипулировать. Проблема нашего времени состоит в том, что дети в большей степени проводят время в интернете. Таким образом, чтобы предотвратить разрушение аналитического мышления предлагается в общеобразовательных учреждениях разработать интерактивны для школьников, которые отвлекали бы их от гаджетов и объясняли, что такое осознанное интернет-потребление.

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

3.3 Приоритетные направления совершенствования законодательства Российской Федерации в сфере обеспечения информационно-психологической безопасности

Исследовав проблему деструктивно-информационно-психологического воздействия, мы выделили несколько направлений для улучшения правовой защиты граждан Российской Федерации:

- Разработка Федерального закона об информационно-психологической безопасности. Прежде чем, начинать работать над улучшением системы органов обеспечения информационно-психологической безопасности, нужно чётко понимать, что представляет собой данная деятельность. Кроме того, нужно понимать в пределах каких принципов должны работать органы безопасности, а также кто и что является угрозой для российских граждан. Исходя из этого, на федеральном уровне предлагается разработать Федеральный закон об информационно-психологической безопасности, который позволит структурировать принципы, полномочия государственных и негосударственных органов и определить угрозы воздействия. За основу можно взять уже разработанный проект нормативно-правового документа. Единственное, законопроект требует дополнения, так как мир меняется, соответственно угрозы видоизменяются, а вместе с ними и методы борьбы. Ко всему прочему в содержании федерального закона должен быть описан предмет правового регулирования, а также субъекты и объекты воздействия;

- Создание « Информационного Кодекса». Проводя анализ влияния деструктивно-информационно-психологического воздействия на граждан РФ, и основываясь на исследованиях ВЦИОМ, мы убедились, что большую часть своего времени россияне проводят во Всемирной сети Интернет. Соответственно акторы пользуются тем, что интернет-пространство слаборегулируемо, и в основном атакуют пользователей через комментарии, с помощью глубоких фейков, ложных ссылок. Среди акторов и мошенников распространенным методом является взлом страниц, когда они незаконно

проникают в аккаунты граждан, и, выдавая себя за них, пишут родственникам, отправляют им сомнительные ссылки, в результате чего могут списаться деньги с электронного кошелька или данная ссылка может содержать нелицеприятные фото или видео. Многие современные пользователи уже научились выявлять взломщиков, однако, правонарушители всё равно продолжают взламывать страницы. Кроме того, их методы становятся всё изощреннее, поэтому вычислять становится всё труднее. Поэтому в целях защиты российских граждан от деструктивно-информационно-психологического воздействия принятие Информационного кодекса является важным этапом, так как он способствует урегулированию интернет-пространства. Нормативно-правовой документ должен содержать определение предмета и метода правового регулирования, а также субъекты и объекты;

- Создание Федерального закона «О психологической помощи». Во второй главе уже упоминалось попытке создания данного закона. На самом деле, вопрос о регулировании психологической помощи поднимался ещё в 1993 году, но тогда законопроект был отклонён по причине того, что в первую очередь нужно было разобраться с вопросом о психиатрической помощи. В 2022 году эксперты из МГУ и МЧС разработали два варианта законопроекта. Законодатели ставят перед собой цель установить чёткие требования к психологам, а именно его полномочия, права и обязанности, и то, какими знаниями и уровнем образования должен обладать специалист, дабы защитить граждан от «самозванцев». Также важно прописать в законе права клиентов. Мы поддерживаем идею федерального закона о психологической помощи, но при этом считаем важным учитывать нормы профессиональной этики психологов. На протяжении исследования нами была приведена статистика количества граждан, обращавшихся за психологической консультацией. В приграничных областях с Украиной наблюдается самый большой рост спроса на психолога. Таким образом, исходя из приведённых данных, делаем вывод, что нормативно-правовой акт о психологической помощи как никогда важен.

- «Здоровая пропаганда» психологической помощи. Мир меняется и отношение к психологии со стороны граждан сейчас более серьёзное, нежели двадцать лет назад. Однако, многие до сих пор бояться идти к специалистам и предпочитают не замечать проблемы. Одна из причин такого отношения связана с предыдущей - отсутствие защиты клиента от «психолога-самозванца». Помимо этого есть люди, которые до сих пор считают психологию не нужной и пустой тратой времени. Следовательно, с целью улучшения ментального здоровья граждан, важно со стороны государства оказать поддержку психологической помощи и подготовить хороших специалистов для воспитания здорового поколения.

- Воспитание осознанного интернет-потребления. Под «осознанным интернет-потреблением» мы понимаем воспитание в молодом поколении умения поглощать информацию размеренно, не перегружая свой мозг, и учиться использовать Всемирную сеть с пользой. Данное направление важно во избежание формирования ряда поколений с клиповым мышлением. Такой тип мышления опасен потерей способности выделять суть, анализировать и критически оценивать ситуацию. Чаще всего люди с клиповым мышлением становятся лёгкой мишенью для манипуляций и внушения. К сожалению, в XXI веке фрагментным мышлением обладают не только дети, но и взрослые, так как многие проводят большее количество времени в таких социальных сетях как TikTok, Вконтакте. Подобные видео не являются опасными сами по себе, но злоупотребление их просмотром приводит человека к клиповому мышлению, а также потери большого количества времени.

В качестве решения, запрещать доступ к социальным сетям не представляется нам верным решением, так как «запретный плод сладок» и чаще всего самый быстрый путь не самый верный. Кроме того, ограничения доступа не помогает человеку осознать настоящую угрозу клипового мышления. В большей степени это вызовет агрессию. Мы предлагаем использовать мягкую силу посредством пропаганды осознанного потребления интернета, проведение в общеобразовательных учреждениях интерактивов с целью отвлечение детей

от «гаджетов» на переменах, а также формировать у детей способность высказывать своё мнение и дискутировать не те или иные темы;

- Признание противоправными негативные субкультуры. Молодёжные движения негативного характера – это неформальные движения, разрушающие личность молодого человека, подменяющие понимание моральных ценностей. Примером таких движений можно назвать «АУЕ», Колумбайн, группы смерти, «М.К.У.». Каждая из этих групп имеет большое количество последователей. В 2022 году отметка достигла 10,5 миллионов детей, согласно информации Лиги безопасности интернета. В качестве основных тенденций, продвигаемых среди детей и подростков в социальных медиа, представителем компании «Лига безопасного интернета» были названы: социопатия, сатанизм и культы, наркомания, нацизм и национализм, массовые и серийные убийства, обесценивание собственной жизни и стремление к смерти, ритуальные убийства и так далее[4]. Мало того среди подростков снова стала популярна такая игра как «беги или умри». Суть её заключается в том, что жертве даётся задание пробежать дорогу в неположенном месте, прямо перед проезжающей на высокой скорости машиной. Факт успешно выполненного задания снимается на камеру.

Борьба с распространением групп смерти представляет большую сложность. Если брать в пример такие группировки как «АУЕ» и «М.К.У», то они по своей сути близки к организованной экстремисткой организации. Под экстремисткой деятельностью понимается насильственное изменение конституционного строя, нарушение территориальной целостности РФ. Кроме того за экстремистскую деятельность принимается пропаганда исключительного превосходства одних над другими, а также разжигание межнациональной розни. Все перечисленные критерии подходят организациям «МКУ» и «АУЕ» в отличие от других деструктивных субкультур, которых сложно назвать организованными группами, исходя из действующего законодательства, но при этом имеющих деструктивно-информационно-психологическое воздействие на подрастающее поколение. Примером может

являться игра «беги или умри», последователи Колумбайна и другие субкультуры. Сейчас негативные объединения перетекли в социальные сети, на имиджборды и на другие интернет-платформы. Представители деструктивных групп создают отдельные паблики, которые чаще всего закрыты от других пользователей и, увидеть всю информацию можно, только если администратор даст разрешение на доступ. Также они используют треш-стримы в качестве трансляции своих убеждений и совершение негативных действий.

В связи с этим мы предлагаем учредить в российском законодательстве правовой механизма признания противоправными деструктивных субкультур. Представляется, что оптимальной формой его реализации было бы внесение соответствующих изменений в Закон о противодействии экстремистской деятельности (соответственно, это будет механизм признания субкультур экстремистскими). Но для этого потребуется расширение определения форм экстремистской деятельности в Федеральном законе «О противодействии экстремистской деятельности» от 27.07.2002 года № 114-ФЗ.

- Совершенствование и возведение Кодекса этики в сфере искусственного интеллекта в нормативно-правовой акт на федеральном уровне. На протяжении всего исследования не раз отмечалась проблема искусственного интеллекта. Научное сообщество обеспокоено тем фактом, что нейросеть в скором времени может стать средством для информационно-психологического воздействия, а после получить и статус субъекта. Примером того насколько далеко зашёл искусственный интеллект является ситуация, произошедшая на крупном конкурсе Sony World Photography Awards 2023 года, на котором немецкий фотограф, Борис Эльдагсен, представил снимок на конкурс, созданный с помощью нейросети. Данная акция была сделана специально, что бы проверить смогут ли судьи отличить настоящий снимок от подделки. По итогу работа искусственного интеллекта одержала победу, но Борис Эльдагсен отказался от награды.

Приведённые примеры лишь малая часть того, что может искусственный интеллект. В том же 2022 году компания Alphabet заявила о создании агента

под названием Gota. При тестировании агент показал достаточно хороший результат. Разработчики заявили о том, что Gota при решении 450 задач смог обойти экспертов-людей. Малого тог он способен легко переключаться с одного навыка на другой, не забывая, чему он научился ранее. Ещё одним примером успешной разработки искусственного интеллекта является аватар AI Yoon, созданный для предвыборной компании, нынешнего президента Южной Кореи, Юн Сок Ёля. Аватар AI Yoon представляет собой неотличимую копию Юн Сок Ёля, он может спокойно общаться с людьми и быть в разных местах одновременно. В результате чего AI Yoon значительно повлиял на предвыборную компанию и послужил победе Юн Сок Ёля. Цитаты аватара президента стали использоваться СМИ, а сам веб-сайт, где «жил» аватар посетили семь миллионов человек. Это говорит о том, что возможности современного искусственного интеллекта уже позволяют влиять на общественное мнение, и в дальнейшем использование подобного рода методов в предвыборных компаниях может послужить ложному восприятию кандидата, укрепляющие в сознании общественности более выгодные качества, которыми реальный человек не обладает. Мало того, в руках агрессивных акторов искусственный интеллект может стать опасным оружием для деструктивно-информационно-психологического воздействия. Сейчас он уже способен создавать глубокие фейки, совершенно неотличимые от реальности. Кроме того, как уже говорилось, искусственный интеллект с его быстрым развитием может вполне стать субъектом правоотношений и информационно-психологического воздействия. В связи с эти мы предлагаем усовершенствовать Кодекс этики искусственного интеллекта и придать ему юридическую силу, дабы регулировать отношения между искусственным интеллектом и человеком в будущем.

Таким образом, нами были выделены основанные направления развития в области информационно-психологической безопасности. Развиваясь в представленных областях, Российская Федерация сможет защитить своих граждан от деструктивно-информационно-психологического воздействия.

Заключение

Тема деструктивно-информационно-психологического воздействия ещё не до конца изучена, и, к сожалению, точного определения данному термину нет. Однако, мы проследили схожесть в работах разных видных учёных и выявили, что деструктивно-информационно-психологическое воздействие - это негативное информационное и психофизическое воздействие на психику объекта, способное изменять его восприятие мира, отношение к чему бы то ни было, и как следствие, может менять и поведение человека. Целью актора при негативном воздействии является покушение на человеческую жизнь, разжигание конфликтов внутри общества, в целом дестабилизация порядка в стране и в мире. Так же мы выявили, что деструктивно-информационно-психологическое влияния имеет свои методы и средства. Основные методы – убеждение, внушение и манипуляция сознанием. Также к второстепенным методам относятся неосознаваемая акустическая и зрительная информация. Чаще эти методы используются в комбинации друг с другом. Основные же средства составляют: всемирная сеть Интернет, СМИ, теле- и радиоканалы. Помимо этого деструктивно-информационно-психологическое воздействие имеет свой объект – человек, общество и государство. Субъект, по сути, определён теми же составляющими, но имеет своё название – актор.

Для того, чтобы противостоять информационно-психологическому воздействию, следует обеспечить информационно-психологическую безопасность граждан РФ не только внутри страны, но и на международном уровне. Сделать это можно посредствам совершенствования российского законодательства, а также благодаря развитию международных отношений между государствами.

Если говорить о правовой защите российского общества от деструктивно-информационно-психологического воздействия на уровне Российской Федерации, то для начала стоит понять что такое информационно-психологическая безопасность. Согласно проведённому исследованию

информационно-психологическая безопасность – это состояние защищённости личности, общества и государства от внутренних и внешних угроз не только информационного, но и психофизического воздействия. Кроме того, были выявлены принципы информационно-психологической безопасности для понимания её сущности. Анализируя нормативно-правовые акты РФ, мы выяснили, что данная сфера регулируется, но также как и на международном уровне, не имеет единого нормативно-правового акта. В тоже время, нельзя сказать, что в Российской Федерации нет методов борьбы с негативно-информационно-психологическим воздействием. Тем не менее, из-за отсутствия чёткого понимания, что представляет собой информационно-психологическая безопасность, трудно определить и зафиксировать степень угроз информационно-психологического воздействия и построить хорошую систему защиты граждан РФ. В связи с этим возникает ряд проблем, требующих своего решения.

В третьей главе мы исследовали реакцию граждан РФ на негативно-информационно-психологическое воздействие, вследствие чего был сделан вывод о том, что устойчивость граждан РФ к фейкам зависит от обстоятельств, в которых человек находится, и от особенностей его психики. Кроме того, устойчивость зависит от образованности граждан и осведомлённости. Также мы убедились, что в сравнении с другими платформами для информации, сеть Интернет является основным средством воздействия. Ко всему прочему мы сделали вывод, что основными и явными методами воздействия является убеждение, внушение, манипуляция сознанием, комбинированный метод и… Остальное применяется достаточно редко.

Исходя из анализа реакции населения РФ на информационно-психологическое воздействие и исследование данной проблемы, мы выделили несколько путей решения. Во втором параграфе третьей главы мы предложили систему развития государственной и негосударственной системы обеспечения информационно-психологической безопасности. Её основной является подготовка кадров в сфере информационно-психологического воздействия, а

также был сделан упор на молодое поколение и воспитание осознанного интернет-потребления. Ко всему прочему на протяжении всей работы мы обращали большое внимание на психологическую составляющую, так как психологическое здоровье гражданина РФ является его личной защитой от информационно-психологического воздействия.

Наконец мы выделили несколько направлений для успешного развития правовой защиты информационно-психологической безопасности граждан Российской Федерации. В их число входит развитие информационного законодательства, законодательства о психологической помощи. Также мы обратили внимание на искусственный интеллект, так как он постепенно становится частью человеческого мира, и, следовательно, в будущем потребует своего правового регулирования как внутри стран, так и на международном уровне. Конечно, главной составляющей является разработка федерального закона об информационно-психологической безопасности.

Таким образом, если углубиться в систему информационно-психологической безопасности и безопасности человека в целом, можно сказать, что она состоит из трёх уровней. Первый – международная безопасность. Второй – национальная безопасность. Третий – личная безопасность гражданина. Последняя должна воспитываться с малых лет. Каждый из уровней составляет важную часть одного целого, но последние две относятся непосредственно к Российской Федерации. Соответственно идя по пути развития национального законодательство и успешно адаптируясь к новым реалиям, в Российской Федерации получится создать действующую правовую защиту российского общества от деструктивно-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/informatsionno-psihologicheskaya-bezopasnost-osnovnye-polozheniya/viewer (дата обращения: 7.10.2022).
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: 29.11.2022)
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-pravovogo-regulirovaniya/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/v-poiskakh-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: 21.12.2022)
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: 12.10.2022)
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: 25.12.2022)
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: 22.12.2022)
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: 29. 12.2022)
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-ot-chrezvychaynyh-situaci/instruktazh-po-grazhdanskoy-oborone-i-zashchite-ot-chrezvychaynyh-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: 12.10.2022)

22. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 28.04.2023). [Электронный ресурс]: URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 10.12.2023)
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-vozdeystvie-v-informatsionnom-protivoborstve/viewer (дата обращения: 7.10.2022).
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: 17.02.2023)
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: 1.05.2023)

27. Конвенция Шанхайской организации сотрудничества по противодействию экстремизму от 9 июня 2017 года. [Электронный ресурс]: URL:https://docs.cntd.ru/document/542655220 (дата обращения:20.12.2022)
28. Кодекс этики в сфере искусственного интеллекта [Электронный ресурс]: URL:https://ethics.a-ai.ru/ (дата обращения:25.12.2022)
29. Латынов В.В. Психологическое воздействие: принципы, механизмы, теории [Электронныйресурс]/Латынов.В.-Режим доступа: URL: https://lib.ipran.ru/upload/ papers/paper_21662912.pdf (дата обращения:6.10.2022)
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.ru%2f (дата обращения: 16.05.2023)
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?id=733 (дата обращения: 19.10.2022)

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» [Электронный ресурс]: Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 14.07.2022). URL:https://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения:8.10.2022)
36. «О рекламе» [Электронный ресурс]: Федеральный закон от 13 марта 2006 г. № 38-ФЗ (последняя редакция). URL:https://www.consultant.ru/document/cons_doc_LAW_58968/ (дата обращения:8.10.2022)
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» [Электронный ресурс]: Федеральный закон от 29.12.2022 N 572-ФЗ URL: https://www.consultant.ru/document/cons_doc_LAW_436110/ (дата обращения: 25.04.2023)
38. «О защите детей от информации, причиняющий вред их здоровью и развитию» [Электронный ресурс]: Федеральный закон от 29.12.2010 года № 436-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 7. 10.22)
39. «О защите населения и территорий от чрезвычайных ситуация природного и техногенного характера» [Электронный ресурс] Федеральный закон от 21.04.1994 года №68-ФЗ (последняя редакция).

URL: https://www.consultant.ru/document/cons_doc_LAW_5295/ (дата обращения 26.04.2023)

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://e-ecolog.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: 18.11. 2022)
42. «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: Федеральный закон от 26.07.2017 N 187-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 18.05.2023)
43. «О федеральной службе безопасности» [Электронный ресурс]: Федеральный закон от 03.04.1995 N 40-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_6300/ (дата обращение: 18.05.2023)
44. «Об информационно-психологической безопасности» [Электронный ресурс]: Проект Федерального закона. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=42883#4arlgdTSQRe6gmz41 (дата обращения 10.04.)
45. «О средствах массовой информации» [Электронный ресурс]: Закон Российской Федерации от 27 декабря 1991 г. № 2124-1(ред.от05.12.2022).URL:https://www.consultant.ru/document/cons_doc_LAW_1511/ (дата обращения:8.10.2022)
46. «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]: Указ Президента от 02.07.2021

года № 400. URL:https://www.consultant.ru/document/cons_doc_LAW_389271/49e275533c7512b66bfcaa9bd9eef6d046da8060/ (дата обращения: 7.10.2022)

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» [Электронный ресурс]: Указ Президента РФ от 21.12.2016 N 699 (ред. от 11.02.2023).URL: https://www.consultant.ru/document/cons_doc_LAW_209309/ (дата обращения: 7.05.2023)
48. «Об утверждении Требований по обеспечению безопасности значимых объектов критической инфраструктуры Российской Федерации» [Электронный ресурс]: Приказ ФСТЭК России от 25.12.2017 № 239 (ред. От 20.02.2020): http://publication.pravo.gov.ru/Document/View/0001201803270041 (дата обращения: 17.05.2023)
49. «О развитии искусственного интеллекта в Российской Федерации» (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") [Электронный ресурс]: Указ Президента РФ от 10.10.2019 N 490. URL:https://www.consultant.ru/document/cons_doc_LAW_335184/0063cb7961941b5727b92eaa4dc68a9e91a8d1fb / (дата обращения: 7.10.2022).
50. «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс]:Указ Президента РФ от 09.05.2017 N 203 URL: https://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 10.03.2023)
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: 10.03.2023)

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).URL:https://www.consultant.ru/document/cons_doc_LAW_77387/5da062376983375b2ede9975f1f1c90a56d4a5de/ (дата обращения: 15.05.2023)
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) https://www.consultant.ru/document/cons_doc_LAW_85889/ (дата обращения: 15.05.2023)
54. «О государственной судебно-экспертной деятельности» [Электронный ресурс]: Федеральный закон от 31 мая 2021 г. № 73-ФЗ .URL:https://www.consultant.ru/document/cons_doc_LAW_31871/ (дата обращения: 20.04.2023)
55. «О противодействии терроризму» Федеральный закон от 06.03.2006 N 35-ФЗ [Электронный ресурс]: (последняя редакция) URL: https://www. consultant. ru/ document/cons_doc_LAW_58840/ дата обращения: 20.04.2023)
56. Пашенцев Е.Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации//Государственное управление. Электронный вестник.2019. № 76. С. 279-300. - Режим доступа: URL:file:///C:/Users/User/Downloads/zlonamerennoe-ispolzovanie iskusstvennogo-intellekta-novye-ugrozy-dlya-mezhdunarodnoy-informatsionno-psihologicheskoy-bezopasnosti-i-puti-ih-neytralizatsii.pdf (дата обращения 19.10.2022)

57. Пользование Интернетом [Электронный ресурс]/ ВЦИОМ – Режим доступа: URL: https://wciom.ru/ratings/polzovanie-internetom (дата обращения: 7.05.2023)
58. Проект Федерального закона о психологической помощи [Электронный ресурс]: URL: https://oppl.ru/up/files/files/2022/zakonoproekt.pdf (дата обращения: 20.03.2023)
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: 23.10.2022)
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: 17.04.2023)
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: 28.11. 2022)
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-sistemypravovogo-obespecheniya-informatsionno-psihologicheskoy-bezopasnosti/ viewer (дата обращения: 28.03.2023)

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-feyki-suschnost-i-otsenkapotentsialn ogo -vliyaniya-na-natsionalnuyu-bezopasnost (дата обращения: 7.03.2023)
65. Самые популярные фейки января 2023[Электронный ресурс]/ Лапша Медиа.- Режим доступа: URL: https://dzen.ru/a/Y90ULjJrUCGWSOeA (дата обращения: 20.04.2023)
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 (20.12.2022)
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/analiticheskii-obzor/trendy-mediapotreblenija-2022 (дата обращения: 25.12.2022)
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: 28.10.2022)
70. Уголовный Кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 21.11.2022, с изм. от 08.12.2022). [Электронный ресурс]: URL:https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения:8.10.2022)
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:30.10.2022)

72. Украинская военная реклама на российских сайтах. [Электронный ресурс]: URL: https://sladkowa.livejournal.com/513184.html (дата обращения:30.05.2023)
73. Угроза ракетного удара [Электронный ресурс]/ Лента.РУ. – Режим доступа:URL:https://lenta.ru/news/2023/02/22/hackers_radio/ (дата обращения: 30.05.2023)