Смирнов А. А.

ФОРМИРОВАНИЕ СИСТЕМЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

монография

Санкт-Петербург
2022

УДК 34
ББК 66.4 (2Рос)
ББК 67.4
С 50

Рецензенты:

Овчинский В. С., Заслуженный юрист Российской Федерации, д-р юрид. наук, профессор;

Кочубей М. А., д-р юрид. наук, доцент.

Смирнов А. А.

С50 **Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации.** Монография. СПб.: Издательство «Русь», 2022. – 272 с.

ISBN 978-5-8090-0109-0

УДК 34
ББК 66.4 (2Рос)
ББК 67.4

В монографии исследуются вопросы правового обеспечения информационно-психологической безопасности. Изложена авторская концепция информационно-психологической безопасности, проанализированы содержание и формы деструктивного информационно-психологического воздействия, систематизированы информационные угрозы в данной сфере.

Рассмотрены международные стандарты и зарубежный опыт правового обеспечения информационно-психологической безопасности. Проведен анализ российского законодательства в области обеспечения информационно-психологической безопасности и системы субъектов ее обеспечения, изложены авторские предложения по их совершенствованию. Отдельное внимание уделено вопросам цифровой грамотности и культуры информационной безопасности.

Издание носит научный характер и ориентировано преимущественно на исследователей, занимающихся проблемами обеспечения информационной безопасности, но может представлять интерес и для широкого круга читателей. Нормативный материал монографии изложен по состоянию на 20 февраля 2022 года.

ISBN 978-5-8090-0109-0

СОДЕРЖАНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

Военная доктрина – Военная доктрина Российской Федерации
ГК РФ – Гражданский кодекс Российской Федерации
Доктрина ИБ 2000 – Доктрина информационной безопасности Российской Федерации (2000 г.)
Доктрина ИБ 2016 – Доктрина информационной безопасности Российской Федерации (2000 г.)
ЕС – Европейский союз
Закон о безопасности – Федеральный закон «О безопасности»
Закон о защите детей от информации – Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»
Закон о связи – Федеральный закон «О связи»
Закон о СМИ – Закон Российской Федерации «О средствах массовой информации»
Закон об информации – Федеральный закон «Об информации, информационных технологиях и о защите информации»
Законопроект об ИПБ – проект Федерального закона «Об обеспечении информационно-психологической безопасности»
ИИ – искусственный интеллект
ИКТ – информационно-коммуникационные технологии
ИП – информационное противоборство
ИПБ – информационно-психологическая безопасность
ИПВ – информационно-психологическое воздействие
ИТВ – информационно-техническое воздействие
КМСЕ – Комитет министров Совета Европы
КоАП РФ – Кодекс Российской Федерации об административных правонарушениях
Концепция ВП – Концепция внешней политики Российской Федерации
Концепция ОБ – Концепция общественной безопасности в Российской Федерации
МИБ – международная информационная безопасность
МПА ОДКБ – Межпарламентская ассамблея Организации Договора о коллективной безопасности
МПА СНГ – Межпарламентская ассамблея государств – участников СНГ
НКО – некоммерческая организация
ОДКБ – Организация Договора о коллективной безопасности
ОРИ – организатор распространения информации в сети Интернет
ПАСЕ – Парламентская ассамблея Совета Европы
РФ – Российская Федерация

СЗ РФ – Собрание законодательства Российской Федерации
СМИ – средства массовой информации
СНГ – Содружество Независимых Государств
Стратегия ГАП – Стратегия государственной антинаркотической политики Российской Федерации на период до 2030 года
Стратегия ГНП – Стратегия государственной национальной политики Российской Федерации на период до 2025 года
Стратегия НБ 2009 – Стратегия национальной безопасности до 2020 года (2009 г.)
Стратегия НБ 2015 – Стратегия национальной безопасности (2015 г.)
Стратегия НБ 2021 – Стратегия национальной безопасности (2021 г.)
Стратегия ПЭ – Стратегия противодействия экстремизму в Российской Федерации до 2025 года
Стратегия РИО – Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы
УК РФ – Уголовный кодекс Российской Федерации
ЦИСМ – Центр изучения и сетевого мониторинга молодежной среды
ШОС – Шанхайская организация сотрудничества

ВВЕДЕНИЕ

Активное развитие глобального информационного общества и процессов цифровой трансформации существенно повысило значимость информационной сферы. Наряду с уникальными возможностями для социального прогресса цифровая среда породила новые вызовы и угрозы для национальной и международной безопасности, требующие адекватного реагирования. Вызовы «цифровой революции» обуславливают необходимость проведения фундаментальных исследований правового обеспечения информационной безопасности и системной модернизации правового регулирования отношений в данной сфере.[1]

Новая Стратегия национальной безопасности Российской Федерации[2] определила информационную безопасность в качестве стратегического национального приоритета, то есть важнейшего направления обеспечения национальной безопасности. При этом в числе ключевых национальных интересов России выделены развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия (пп. 4 п. 25).

Открытые новой информационной реальностью возможности были использованы в целях оказания деструктивного информационно-психологического воздействия на индивидуальное, групповое и общественное сознание. Существенно возросла активность в информационном пространстве иностранных спецслужб, террористических и экстремистских организаций, преступников и иных злоумышленников. Сеть Интернет и мобильная связь вывели на новый беспрецедентный уровень угрозы распространения негативной информации и ведения деструктивной коммуникации, мультиплицировав количество их источников и кратно расширив уязвимую для их воздействия аудиторию.

Анонимная цифровая среда с каждым годом все активнее генерирует риски распространения экстремистских, криминальных и иных антисоциальных идей, разжигания ненависти и вражды, распространения противоправного контента, обмана и манипуляции сознанием, вовлечения в террористическую и экстремистскую деятельность, потребления наркотиков, подстрекательства к агрессии, суицидам и иным видам общественно опасного поведения. Пандемия COVID-19 резко обострила проблему распространения недостоверной общественно значимой

[1] Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. Т. А. Поляковой. Саратов: Амирит, 2020. С. 36.

[2] Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 2 июля 2021 г. № 400) // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001 (дата обращения: 08.07.2021).

информации в СМИ и интернет-ресурсах. Технологии искусственного интеллекта, виртуальной и дополненной реальности способны вывести информационно-психологические угрозы на новый уровень опасности.

В связи с этим требуют новых научно обоснованных подходов и правового осмысления проблемы обеспечения информационно-психологической безопасности.

Реализация поставленных в Стратегии национальной безопасности Российской Федерации, Доктрине информационной безопасности Российской Федерации[3] и иных документах стратегического планирования задач по обеспечению надежной защиты личности, общества и государства от растущих информационных угроз детерминирует необходимость на основе системного анализа российского законодательства в рассматриваемой сфере разработки концептуальных предложений по дальнейшему формированию системы правового обеспечения информационно-психологической безопасности Российской Федерации с учетом международных стандартов и зарубежного опыта.

Целью настоящего исследования является разработка теоретико-методологической концепции формирования системы правового обеспечения информационно-психологической безопасности в Российской Федерации и практических предложений по ее развитию в условиях глобального информационного общества и цифровой трансформации.

[3] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) // СЗ РФ. 2016. № 50. Ст. 7074.

ГЛАВА I. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВАНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

§ 1. Историко-гносеологические аспекты информационно-психологической безопасности

Проблематика информационной безопасности выделилась в обособленный блок в системе национальной и международной безопасности относительно недавно, в конце XX в. Отдельные ее аспекты, такие как защита государственной тайны, борьба с дезинформацией, клеветой и другими информационными угрозами, уходят корнями в глубь веков.

Поэтому, приступая к исследованию правовых аспектов информационно-психологической безопасности, считаем необходимым провести краткий анализ генезиса и эволюции информационных угроз. Это позволит понять истоки изучаемой научной проблемы и проследить путь ее развития во всемирно-историческом контексте. Также исключительно важно изучить характеристики современного социального контекста, обозначаемого маркерами «глобального информационного общества», «информационной революции» и «цифровой трансформации». Это необходимо для формирования «координатной сетки», в пределах которой можно позиционировать объект нашего исследования и понять окружающий его «ландшафт».

Т. А. Полякова подчеркивала, что для осмысления проблемы цифровой трансформации и новых вызовов необходимо «изучение развития информационно-коммуникационных технологий в их исторической ретроспективе с древних времен до анализа современных проблем развития информационного общества и формирования системы правового обеспечения информационной безопасности».[4]

Признавая уникальность современного состояния информационной сферы, обозначаемого как «информационное общество», необходимо отметить, что ему предшествовал длительный процесс эволюции инструментов коммуникации как составляющей исторического развития человечества. П. В. Ушанов выделил четыре «коммуникационные революции», когда происходил скачкообразный рост развития СМИ: 1) развитие периодической печати (XIX – начало XX в.); 2) появление радио (конец

[4] *Полякова Т. А.* Актуальные проблемы развития правового обеспечения информационной безопасности в цифровую эпоху и юридическое образование // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 12. С. 38.

XIX – начало XX в.); 3) возникновение и «триумфальное шествие» телевидения (вторая половина XX в.); 4) развитие спутниковых и кабельных телекоммуникаций, компьютерных сетей (конец XX в. – н. в.).[5]

Каждая новая веха развития технологий коммуникации оказывала значительное воздействие как на систему общественной организации, так и на мировосприятие людей. М. Маклюэн выразил сущность этого процесса в известном выражении: «средство коммуникации есть сообщение» («the medium is the message»), означающем, что «личностные и социальные последствия любого средства коммуникации – то есть нашего расширения вовне – вытекают из нового масштаба, привносимого каждым таким расширением, или новой технологией, в наши дела».[6]

Одним из направлений социального влияния новых коммуникационных технологий выступало возникновение и развитие информационных угроз. Ниже будет приведена авторская периодизация основных этапов эволюции информационных угроз, выстроенная нами на основе анализа научных трудов по истории информационного противоборства.[7] Необходимо оговориться, что появление на каждом этапе эволюции новых информационных вызовов происходит при сохранении угроз предыдущего периода, которые также трансформируются под влиянием инновационных технологий коммуникации. Изложенная классификация основных этапов на претендует на статус эталона, однако позволяет четко увидеть *направленность* и *тенденции* эволюции информационных угроз в длительной исторической перспективе. Тем самым закладывается прочный фундамент для осмысления современных вызовов в информационной сфере.

Генезис информационных угроз происходит с зарождением и развитием человеческого общества. В этот период такие угрозы исходили прежде всего от самого человека и групп людей, а также от примитивных форм документов и иных творений человека. К их числу относились: обман, дезинформация противника, перехват секретных сведений, распространение опасных идей и взглядов и др. Данные угрозы носили преимущественно локальный характер.

Психологические методы воздействия использовались в вооруженной борьбе племен еще в первобытном обществе в целях запугивания противника и поднятия боевого духа своего войска. Тактика

---

[5] *Ушанов П. В.* Основные аспекты взаимодействия СМИ и public relations: учебное пособие. М.: Флинта: Наука, 2009. С. 49–57.

[6] *Маклюэн Г. М.* Понимание Медиа: внешние расширения человека / Пер. с англ. В. Николаева. 2-е изд. М.: Гиперборея; Кучково поле, 2007. С. 9.

[7] *Волкогонов Д. А.* Психологическая война: Подрывные действия империализма в области общественного сознания. М.: Воениздат, 1984; *Воронцова Л. В., Фролов Д. Б.* История и современность информационного противоборства. М.: Горячая линия – Телеком, 2006; *Панарин И. Н.* Информационная война и геополитика. М.: Поколение, 2006; Информационные, специальные, воздушно-десантные и аэромобильные операции армий ведущих зарубежных государств: информационно-аналитический сборник / А. Н. Сидорин, И. А. Рябченко, В. П. Герасимов и др. М.: Воениздат, 2011.

распространения слухов о своей несокрушимой мощи и беспощадности продолжает активно применяться и в последующий период.[8] Но с возникновением государств приемы психологической борьбы начинают широко применяться не только для военных целей, но и в качестве способов ведения противоборства в сферах политики, дипломатии, экономики, в том числе для подавления своих политических противников внутри страны.[9] Появляются и первые концептуальные попытки осмысления роли и значения психологических методов противоборства, а также их систематизации, в частности в древнекитайских трудах.[10]

Второй этап эволюции информационных вызовов (XV–XVIII вв.) обусловлен развитием печатных технологий. Начало «коммуникационной революции» на данном этапе положило появление в Европе технологий типографского книгопечатания в середине XV в., что существенно расширило масштабы издания книг и возможности их психологического влияния на индивида и население. В связи с доминированием религиозных форм общественного сознания «духовное воздействие на противника было облачено преимущественно в религиозные формы».[11] В этот период Ватикан создал Конгрегацию пропаганды веры в целях популяризации католицизма и контролем за инакомыслием.[12]

В противостоянии мировых держав начинают шире применяться методы психологического воздействия на население.[13] Власти Российского государства активно боролись с вражеской подрывной пропагандой, используя для этих целей структуры разведки и контрразведки.[14] В этот период в ходе военных конфликтов стали применяться листовки.

Третий этап развития информационных угроз (XIX – начало XX в.) связан с развитием прессы,[15] а также появлением телеграфа и радио.

---

[8] Д. А. Волкогонов приводит пример с римлянами, которые перед совершением военных походов распространяли слухи о превосходстве своих легионов, невиданной храбрости римлян и их неодолимой решимости добыть победу. См.: *Волкогонов Д. А.* Психологическая война: Подрывные действия империализма в области общественного сознания. М.: Воениздат, 1984. С. 44.

[9] *Воронцова Л. В., Фролов Д. Б.* История и современность информационного противоборства. М.: Горячая линия – Телеком, 2006. С. 5.

[10] *Сунь-цзы.* Искусство стратегии. М.: Эксмо; СПб.: Мирград, 2007; *Зенгер Х. фон.* Стратагемы. О китайском искусстве жить и выживать. В 2 т. М.: Эксмо, 2006.

[11] *Волкогонов Д. А.* Психологическая война: Подрывные действия империализма в области общественного сознания. М.: Воениздат, 1984. С. 45.

[12] *Беглов С. И.* Внешнеполитическая пропаганда. Очерк теории и практики. М.: Высшая школа, 1980. С. 41.

[13] Так, авторы издания указывают на распространение иностранными шпионами в России в XVII в. так называемых клеветнических «переметных писем», содержащих призывы к измене государству. См.: *Воронцова Л. В., Фролов Д. Б.* История и современность информационного противоборства. М.: Горячая линия – Телеком, 2006. С. 18–22.

[14] Там же.

[15] Следует отметить, что печатные газеты стали регулярно выходить в Европе с начала XVII в. Однако массовые периодические печатные издания получают распространение только в XIX в. С этим пониманием связано и происхождение термина

Газеты и журналы становятся влиятельным источником воздействия на общественное мнение, в том числе деструктивного.[16] Поэтому пресса активно вовлекается в противоборство ведущих держав. Попытки влиять на зарубежное население через газеты предпринимались российским и французским правительствами. Во Франции в структуре секретной службы были созданы подразделения, занимавшиеся ведением пропаганды и контрпропаганды с использованием возможностей прессы и театра.[17]

Телеграф и радио существенно увеличили скорость передачи информации на большие расстояния, что оказало существенное влияние на военные конфликты. «Возросла опасность угроз перехвата такой информации, ее уничтожения или искажения, а также дезинформации».[18]

В ходе Первой мировой войны начали широко применяться листовки и иные печатные средства влияния на военнослужащих и население противника. По свидетельству Д. А. Волкогонова, в этот период в войсках европейских держав создаются специальные пропагандистские подразделения. Однако, несмотря на широкий размах психологической войны, она не сыграла определяющей роли во влиянии на моральных дух военнослужащих.[19]

В связи с развитием телеграфии в конце XIX – начале XX в. в России и Европе учреждаются телеграфные агентства, которые задействуются для ведения информационной борьбы.[20]

Четвертый этап эволюции информационных угроз (1920–1940-е гг.) обусловлен дальнейшим развитием прессы и радиовещания, а также появлением кинематографа и телевидения. Все указанные средства массовой коммуникации начинают активно применяться в пропагандистских целях. Именно в этот период публикуются ставшие впоследствии классическими научные работы У. Липмана,[21] Г. Лассуэла[22] и Э. Бернейса,[23] посвященные теории пропаганды и технологиям влияния на общественное мнение.

«пресса» от названия первой массовой газеты La Presse, вышедшей в Париже в 1836 г. См.: Пресса // Большая советская энциклопедия. В 30 т. М.: Советская энциклопедия, 1969–1978. URL: http://bse.sci-lib.com (дата обращения: 14.03.2012).

[16] В этой связи часто приводится высказывание Наполеона о том, что «четыре газеты смогут причинить врагу больше зла, чем стотысячная армия». Цит. по: *Беглов С. И.* Внешнеполитическая пропаганда. Очерк теории и практики. М.: Высшая школа, 1980. С. 52.

[17] *Воронцова Л. В., Фролов Д. Б.* История и современность информационного противоборства. М.: Горячая линия – Телеком, 2006. С. 25.

[18] *Смирнов А. А.* Эволюция угроз информационной безопасности // Информационные войны. 2015. № 2. С. 70.

[19] *Волкогонов Д. А.* Психологическая война: Подрывные действия империализма в области общественного сознания. М.: Воениздат, 1984. С. 47–48.

[20] *Воронцова Л. В., Фролов Д. Б.* История и современность информационного противоборства. М.: Горячая линия – Телеком, 2006. С. 29–30.

[21] Public Opinion. By Walter Lippmann. New York: Harcourt, Brace and Company. 1922.

[22] *Lasswell, H. D.* Propaganda Technique in the World War. Peter Smith, 1927.

[23] *Bernays, E. L.* Propaganda. Routledge, 1928.

Мощная система государственной пропаганды формируется в нацистской Германии, которую Д. А. Волкогонов охарактеризовал как «особую систему духовного насилия».[24] Именно в Германии в 1933 г. впервые в мире создается министерство народного просвещения и пропаганды, под контроль которого были поставлены печатные издания, кинематограф и радиовещание. В его задачи входило осуществление пропаганды как внутри страны, так и за рубежом.[25]

Сильный аппарат пропаганды был создан и в Советском Союзе в 1920–1930-е гг. В его состав входили управления и отделы пропаганды и агитации ЦК ВКП(б) и ВЛКСМ, Политуправление РККА, Радиокомитет, Телеграфное агентство (ТАСС), другие органы и учреждения.

Вторая мировая война стала ареной не только военного, но и информационно-психологического противостояния двух военно-политических коалиций. Следуя стратегии Гитлера о войне «психологическим оружием», руководство нацистской Германии задействовало потенциал пропагандистского аппарата военного и гражданских ведомств для психологической обработки своего населения и военнослужащих, а также воздействия на противника. Для этой цели в войсках были специально созданы роты пропаганды.[26] Средствами ведения психологической борьбы выступали листовки, радиовещание и кинематограф.

В СССР решение задач противодействия пропаганде нацистской Германии обеспечивали органы государственной безопасности (НКГБ и НКВД). Помимо борьбы с паникерами и распространителями слухов внутри страны они противодействовали пропаганде противника и дезинформировали его путем ведения радиоигр и иными способами. Военную пропаганду и контрпропаганду осуществлял отдел по работе среди войск противника («7-й отдел») Главного политического управления РККА. Важную роль в информационном противостоянии противнику сыграло также Советское информационное бюро при СНК СССР, созданное летом 1941 г. В качестве средств психологической борьбы применялись агитационные печатные материалы, радиовещание, громкоговорители и др.[27]

---

[24] *Волкогонов Д. А.* Психологическая война: Подрывные действия империализма в области общественного сознания. М.: Воениздат, 1984. С. 47–48.

[25] *Панарин И. Н.* Информационная война и геополитика. М.: Поколение, 2006. С. 153.

[26] По данным исследователей, отдел пропаганды вермахта создан в 1939 г. В начале 1943 г. его войска пропаганды объединяли 21 роту пропаганды сухопутных войск, 7 взводов военных корреспондентов «Великой Германии», 8 батальонов пропагандистов-добровольцев на оккупированной территории. См.: *Воронцова Л. В., Фролов Д. Б.* История и современность информационного противоборства. М.: Горячая линия – Телеком, 2006. С. 47; *Панарин И. Н.* Информационная война и геополитика. М.: Поколение, 2006. С. 157.

[27] *Мощанский И. Б.* Информационная война. Органы спецпропаганды Красной армии. М.: Вече, 2010. С. 5–12, 18–64.

Как подчеркивается составителями тематического сборника, «именно в период Второй мировой войны использование всеми воюющими сторонами пропагандистского воздействия на свое население и на население противника вышло на новый качественный уровень».[28]

Кроме того, в рассматриваемый период зарождаются информационно-технические угрозы, воздействующие средства и каналы радиосвязи. Начинает формироваться направление радиоэлектронной борьбы.[29]

Пятый этап эволюции информационных угроз (вторая половина XX в.) связан с развитием радио- и телевещания, кинотеатров, а также появлением и совершенствованием ЭВМ.

Расширение сети кинотеатров, рост популярности телевидения и радио среди населения обусловили существенное увеличение силы их влияния.[30] Особенно мощным было влияние телевидения. Как выразился в 1968 г. американский ученый Р. Макнейл, «ничто до распространения телевидения не вносило таких чудовищных перемен в технику убеждения масс».[31]

Осознание опасностей негативного влияния СМИ на общество, особенно подростковую аудиторию, приводит к принятию в Европе первых законов о защите от вредной информации – Закона ФРГ «О распространении произведений и медиаконтента, вредных для молодежи» 1953 г.[32] и Закона Великобритании «О детях и молодежи (вредные публикации)» 1955 г.[33] Понимание опасностей СМИ имелось и у советских властей. Как отмечает Пристанская О. В.,[34] еще в Постановлении СНК и ВКП(б) СССР

---

[28] Советская пропаганда в годы Великой Отечественной войны: «коммуникация убеждения» и мобилизационные механизмы / Авт.-сост. А. Я. Лившин, И. Б. Орлов. М.: Российская политическая энциклопедия, 2007. С. 6.

[29] *Воронцова Л. В., Фролов Д. Б.* История и современность информационного противоборства. М.: Горячая линия – Телеком, 2006. С. 7.

[30] «Бурное развитие массовой коммуникации в последние десятилетия, – писал советский ученый Ю. А. Шерковин в 1973 г., – превратило ее в необходимый компонент общественного бытия, в источник постоянной информации в виде идей, представлений и образов, дополняющих собой и обогащающих непосредственный опыт человека, формирующих его ценности и нормы, активно влияющих на функционирование его личности». См.: *Шерковин Ю. А.* Психологические проблемы массовых информационных процессов. М.: Мысль, 1973. С. 7.

[31] *Кара-Мурза С. Г.* Манипуляция сознанием: учебное пособие. М.: Алгоритм, 2004. С. 395.

[32] Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte 1953 // Bundesanzeiger Verlag. URL: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl153s0377.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl153s0377.pdf%27%5D__1644853976806 (дата обращения: 17.12.2019).

[33] Children and Young Persons (Harmful Publication) Act 1955 // Legislation.Gov.UK. URL: http://www.legislation.gov.uk/ukpga/1955/28/pdfs/ukpga_19550028_en.pdf (дата обращения: 17.12.2019).

[34] *Пристанская О. В.* Правовое регулирование информационной безопасности детей // Информационная и психологическая безопасность в СМИ. В 2 т. Т. I: Телевизионные и рекламные коммуникации / Под ред. А. И. Донцова, Я. Н. Засурского, Л. В. Матвеевой, А. И. Подольского и др. М.: Аспект Пресс, 2002. С. 74.

1935 г. № 1047 «О ликвидации детской беспризорности и безнадзорности» содержался раздел «О детской литературе и кинофильмах», в котором устанавливался запрет пропаганды преступного образа жизни и распространения иной информации, способной оказать негативное влияние на детей.[35]

В международных отношениях этот период характеризовался идеологическим противостоянием двух сверхдержав – СССР и США, получивший в историографии наименование «холодной войны». Информационная война между данными государствами велась через все доступные средства массовой коммуникации того периода (печатные издания, радио- и телевещание). Также активно задействовались литература, музыка, театр, образовательные и культурные обмены, проведение выставок и конференций. В США основными органами психологической борьбы выступали Информационное агентство США, ЮСИА (United States Information Agency, USIA)[36] и Центральное разведывательное управление,[37] в СССР – Международный отдел и Отдел агитации и пропаганды ЦК КПСС,[38] КГБ СССР.[39] Важную роль во внешнеполитической пропаганде Советского Союза играло созданное на базе Совинформбюро Агентство печати «Новости» (АПН).[40]

В военных конфликтах все активнее стали применяться методы психологической и радиоэлектронной борьбы. В частности, войсками США были проведены успешные психологические операции в ходе военных действий в Панаме и Персидском заливе.[41]

---

[35] *Пристанская О. В.* Правовое регулирование информационной безопасности детей // Информационная и психологическая безопасность в СМИ. В 2 т. Т. I: Телевизионные и рекламные коммуникации / Под ред. А. И. Донцова, Я. Н. Засурского, Л. В. Матвеевой, А. И. Подольского и др. М.: Аспект Пресс, 2002. С. 74.

[36] The United States Information Agency. A Commemoration. USIA. 1999; USIA: an overview". USIA. August 1998. URL: http://dosfan.lib.uic.edu/usia/usiahome/oldoview.htm#overview (дата обращения: 04.10.2013).

[37] *Волкогонов Д. А.* Психологическая война: Подрывные действия империализма в области общественного сознания. М.: Воениздат, 1984. С. 176–180; *Сондерс Ф. С.* ЦРУ и мир искусств: культурный фронт холодной войны. М.: Институт внешнеполитических исследований и инициатив. М.: Кучково поле, 2013.

[38] Советские активные мероприятия. Доклад об активных мероприятиях и пропаганде, 1986–87. Государственный департамент США. URL: http://www.pseudology.org/information/Active/index.htm (дата обращения: 12.02.2014).

[39] *Жирнов Е.* Дезинформбюро. 80 лет советской службе дезинформации // Коммерсант. 2003, 13 января; *Хлобустов О.* КГБ – шаги становления // ФСБ России. 01.11.2004. URL: http://www.fsb.ru/fsb/history/author/single.html!id%3D10318038@fsbPublication.html (дата обращения: 11.09.2019).

[40] Создание на базе АПН Информационного агентства «Новости» // РИА Новости. 29.10.2013. URL: http://ria.ru/media_Russia/20131029/973317995.html (дата обращения: 09.09.2019); *Морев Г.* Волин: пулемет был перенацелен вовнутрь // РИА Новости. 29.10.2013. URL: http://ria.ru/media_Russia/20131029/973081329.html (дата обращения: 24.12.2013).

[41] Информационные, специальные, воздушно-десантные и аэромобильные операции армий ведущих зарубежных государств: информационно-аналитический сборник / А. Н. Сидорин, И. А. Рябченко, В. П. Герасимов и др. М.: Воениздат, 2011. С. 15–78.

Именно в рассматриваемый период начинают развиваться электронно-вычислительные машины, а позже – и компьютерные сети, включая ARPANET, будущую основу Интернета.[42] Соответственно, возникают угрозы, связанные с вредоносным воздействием на компьютерную технику и сети передачи данных, зарождается киберпреступность.[43]

Комплекс прорывных технологий, включая компьютеры, средства мобильной связи, информационно-телекоммуникационные сети, устройства хранения данных, и их интеграция на единой цифровой платформе в конце XX – начале XXI в. вызвали «информационный взрыв» и обусловили начало формирования глобального информационного общества.[44]

Ключевым драйвером развития информационного общества стала сеть Интернет.[45] Во втором десятилетии XXI в. этот тренд еще более усилился. В. В. Архипов подчеркивает, что сеть Интернет на сегодняшний день является одним из наиболее значимых культурных артефактов.[46] Благодаря Всемирной паутине «реальностью стали такие составляющие глобального информационного общества, как электронное правительство, трансграничная электронная торговля, глобальные социальные сети, потоковое вещание теле- и радиопрограмм и еще много сервисов».[47]

В настоящее время цифровые технологии продолжают активно развиваться. Ключевыми трендами цифрового развития на современном этапе выступают[48]: 1) технологии искусственного интеллекта; 2) аналитика больших данных; 3) облачные технологии; 4) интернет вещей; 5) мобильный интернет, включая новое поколение мобильной связи 5G; 6) беспилотный транспорт и робототехника; 7) технологии виртуальной и дополненной реальности; 8) технология блокчейна; 9) социальные сети

---

[42] *Борн Д.* Интернету – 40 лет. Как все начиналось… // 3DNews. 30.10.2009. URL: http://www.3dnews.ru/news/internetu_40_let_kak_vssh_nachinalos/ (дата обращения: 11.05.2012).

[43] Понимание киберпреступности: явление, задачи и законодательный ответ / М. Герке. Международный союз электросвязи, 2012. С. 13.

[44] *Паршин П.* Глобальное информационное общество и мировая политика: аналитический доклад Института международных исследований МГИМО (У) МИД России. М., 2009. № 2 (23). С. 9–10.

[45] *Михеев А. Н.* Информационно-коммуникационные технологии: глобальные проблемы и/или глобальные возможности // Современные глобальные проблемы мировой политики: учеб. пособие для студентов вузов / Под ред. М. М. Лебедевой. М.: Аспект Пресс, 2009. С. 139.

[46] *Архипов В. В.* Интернет-право: учебник и практикум для вузов. М.: Издательство Юрайт, 2021. С. 123.

[47] Актуальные проблемы информационного права: учебник / Коллектив авторов; под ред. И. Л. Бачило, М. А. Лапиной. М.: Юстиция, 2016. С. 274.

[48] Мониторинг глобальных трендов цифровизации 2020 // Ростелеком. URL: https://www.company.rt.ru/upload/iblock/6e0/ROSTELECOM_TRENDS2020_INTERACTIVE_FINAL.pdf (дата обращения: 10.02.2021); CNews: ИТ-тренды 2021 // CNews. 29.12.2020. URL: https://www.cnews.ru/reviews/cnews_trendy_2021 (дата обращения: 02.02.2021).

и др. Глобальная пандемия COVID-19 еще больше ускорила цифровую трансформацию.[49]

Комплекс новейших ИКТ оказывает революционное воздействие на общественную жизнь и международные отношения, что подчеркнуто в Окинавской хартии глобального информационного общества от 22 июля 2000 г.[50] Массовое распространение Интернета, по мнению Э. Шмидта и Дж. Коэна, «привело к одной из наиболее поразительных социальных, культурных и политических трансформаций в истории», в результате чего «мы сталкиваемся с поистине глобальными переменами».[51] А. А. Карцхия цифровые технологии вкупе с анализом больших данных называет «технологическими драйверами цифровых инноваций, которые определяют глобальные трансформации современного мира, формируют вектор основного технологического, экономического и социального развития в современную эпоху».[52]

Развитие глобального информационного общества и процессов цифровой трансформации повлекло появление и развитие вызовов и угроз, связанных с «возрастанием уязвимости общественных процессов от информационного воздействия».[53] За последние несколько десятилетий произошел резкий рост количества и общественной опасности таких угроз, многие из них получили поистине глобальный характер.[54]

Реакцией на эти процессы стало «концептуальное и нормативное выделение информационной безопасности в отдельный вид безопасности сначала на национальном, а затем и на международном уровне».[55] Информационная безопасность при этом рассматривается как «атрибутивное условие выживания и развития информационного общества».[56]

---

[49] Digital trends in Europe 2021. ICT trends and developments in Europe, 2017–2020 // International Telecommunication Union, 2021. URL: https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC21/Documents/RPM/EUR/Digital-Trends_Europe-E.pdf (дата обращения: 10.02.2021).

[50] Дипломатический вестник. М., 2000. № 8. С. 51–56.

[51] Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств / Эрик Шмидт, Джаред Коэн; пер. с англ. С. Филина. М.: Манн, Иванов и Фербер, 2013. С. 12.

[52] *Карцхия А. А.* Цифровизация в праве и правоприменении // Мониторинг правоприменения. 2018. № 1. С. 37.

[53] Информационная безопасность России / Ю. С. Уфимцев, Е. А. Ерофеев и др. М.: Издательство «Экзамен», 2003. С. 6.

[54] *Полякова Т. А., Минбалеев А. В., Кроткова Н. В.* Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. 2021. № 12. С. 98.

[55] *Смирнов А. А.* Эволюция угроз информационной безопасности // Информационные войны. 2015. № 2. С. 73.

[56] *Усанов В. Е., Кириллов Н. П.* Психологическая безопасность российского общества и проблемы ее социально-правового обеспечения: учебник. М.: Издательство «Элит», 2009. С. 59.

Палитра современных угроз информационной безопасности чрезвычайно разнообразна. Она включает в себя как информационное измерение традиционных угроз безопасности (преступности, терроризма, военных действий), так и «чистые» информационные угрозы (сетевые атаки, применение вредоносного программного обеспечения, ложные новости). Анализ всей совокупности имеющихся информационных угроз позволяет выделить две основные группы таких угроз по критерию объектов воздействия: 1) связанные с деструктивным информационно-психологическим воздействием на человека и общество; 2) связанные с вредоносным информационно-техническим воздействием на информационную инфраструктуру.

Угрозы первой группы будут интересовать нас в настоящем исследовании. Как было показано выше, они имеют древний генезис и прошли длительную эволюцию. Однако именно в последние десятилетия произошла их резкая актуализация и повышение значимости в связи с расширением возможностей деструктивного психологического воздействия на человека, социальные группы и население страны в целом.[57] Это обусловлено комплексом факторов.

Во-первых, накоплен и апробирован комплекс «когнитивных технологий»[58] влияния на индивидуальное и общественное сознание.[59]

Во-вторых, произошло резкое увеличение количества субъектов и каналов массовой информации и коммуникации.

В-третьих, современные ИКТ сделали возможными мгновенную передачу информации в глобальном масштабе и ведение коммуникаций в режиме реального времени.

В-четвертых, цифровая среда создала возможности для анонимности пользователей, что затрудняет идентификацию субъектов информационно-психологического воздействия и «растормаживает» их поведение в онлайне.

В-пятых, новые технологии мониторинга и анализа сетевой активности пользователей Интернета еще больше расширили возможность

---

[57] *Шиловцев А. В.* Современные информационные технологии как фактор угроз безопасности личности в современной России: аксиологический аспект // Информационное право. 2012. № 2. С. 14; *Бурняшева Л. А.* Духовное пространство в условиях трансформации современного российского общества: дис. … д-ра философ. наук. Ставрополь, 2014. С. 20; Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. д. ю. н., профессора Т. А. Поляковой. Саратов: Амирит, 2020. С. 23.

[58] *Сундиев И. Ю.* Когнитивные технологии: темная сторона прогресса // Научный портал МВД России. 2012. № 1. С. 79–84.

[59] Как отмечается в статье, «индивидуальное и социальное сознание находятся в фокусе политтехнологий, использующих всю мощь современных средств информационного воздействия». См.: *Велихов Е. П., Котов А. А., Лекторский В. А., Величковский Б. М.* Междисциплинарные исследования сознания: 30 лет спустя // Вопросы философии. 2018. № 12. С. 12.

манипулирования ими за счет персонализации и таргетирования коммуникационного воздействия.[60]

Глобальные потрясения еще больше усиливают остроту проблемы. Так, охватившая мир пандемия коронавирусной инфекции COVID-19 породила огромное количество спекуляций, слухов и дезинформации, заставивших ООН и Всемирную организацию здравоохранения говорить о возникновении «инфодемии» – нарастающей волне фейков о коронавирусе.[61]

Процесс погружения человечества в цифровую реальность непрерывно ускоряется. Все больше времени тратится на создание и потребление медиаконтента, человеческое общение все чаще протекает в форматах виртуальной коммуникации. Мы уже стоим на пороге широкого внедрения технологий виртуальной и дополненной реальности, искусственного интеллекта, способных довести процесс виртуализации общества до его логического завершения. Однако ни сам человек, ни социум оказались не готовы к данной ситуации. Психика человека не способна «отфильтровать» все возрастающий информационный поток, а потому страдает от информационной перегрузки и лавины фейковой информации.[62] Традиционные ценностные ориентиры и социальные регуляторы объективно отстают от галопирующей динамики развития информационно-технологической сферы. В этих условиях исследование современных вызовов цифровой среды и выработка методологических подходов к их нейтрализации на основе адекватных правовых инструментов становятся архиважными.

Научное осмысление проблем обеспечения информационно-психологической безопасности в постсоветской России шло волнообразно, и представители юридической науки играли в этом процессе ключевую роль. Драйвером научных исследований информационно-психологической безопасности зачастую выступали законотворческие инициативы. Первым мощным импульсом к изучению данной проблематики послужила разработка проекта федерального закона «Об информационно-психологической безопасности» (далее – Законопроект об ИПБ), в рамках которой в 1990-е гг. было проведено множество солидных научных конференций

---

[60] *Черешнев Е.* Форма жизни № 4. Как остаться человеком в эпоху расцвета искусственного интеллекта. М.: Альпина Паблишер, 2022.

[61] *Полякова Т. А., Минбалеев А. В., Кроткова Н. В.* Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 79.

[62] С. В. Чугров очень точно описывает ситуацию с фейковой информацией: «Да, манипулирование коллективным сознанием в массмедиа не является чем-то новым. Но новизна ситуации в том, что засоренность СМИ и особенно социальных сетей сфальсифицированными фактами превысила критический порог, что привело к появлению качественно нового феномена – искривленного информационного пространства». См.: *Чугров С. В.* Post-truth: трансформация политической реальности или саморазрушение либеральной демократии? // Полис. Политические исследования. 2017. № 2. С. 54.

и издан ряд важных научных трудов членов рабочей группы.[63] Проведенная в этот период работа заложила весомый научный фундамент для изучения теоретических, правовых и психологических аспектов темы информационно-психологической безопасности.

В 2000 г. был принят первый документ стратегического планирования в сфере информационной безопасности – Доктрина информационной безопасности Российской Федерации,[64] значение которой трудно переоценить. В документе существенное внимание было уделено вопросам защиты от информационно-психологических угроз.

Следующий этап исследования проблем правового обеспечения информационно-психологической безопасности был связан с разработкой еще одного законодательного акта – проекта федерального закона «О защите детей от информационной продукции, причиняющей вред их здоровью, нравственному и духовному развитию». Его подготовка велась длительное время на базе НИИ проблем укрепления законности и правопорядка при Генеральной прокуратуре РФ авторским коллективом под руководством В. Н. Лопатина и О. В. Пристанской с привлечением широкого круга экспертов.[65] Итогом данной работы стало сначала принятие такого акта в формате модельного закона СНГ,[66] а затем – Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[67] (далее – Закон о защите детей от информации).

Принятие нового закона, в свою очередь, стимулировало дальнейшие научные исследования проблемы обеспечения информационной безопасности детей,[68] наиболее фундаментальным из которых стала научная

---

[63] *Смолян Г. Л., Зараковский Г. М., Розин В. М., Войскунский А. Е.* Информационно-психологическая безопасность (определение и анализ предметной области) // М.: Институт системного анализа РАН, 1997; *Лопатин В. Н.* Концепция развития законодательства в сфере обеспечения информационной безопасности. М.: Изд. Гос. Думы РФ, 1998; *Тер-Акопов А. А.* Безопасность человека: Теоретические основы социально-правовой концепции. М.: Изд-во МНЭПУ, 1998; *Цыганков В. Д., Лопатин В. Н.* Психотронное оружие и безопасность России. М.: Синтег, 1999; *Смирнов И., Безносюк Е., Журавлев А.* Психотехнологии: Компьютерный психосемантический анализ и психокоррекция на неосознаваемом уровне. М.: Издательская группа «Прогресс» – «Культура», 1995; *Бухтояров А. А.* Психоэкология реальности; Русское Бардо; Ключ Творения. Архангельск: Правда Севера, 2003.

[64] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895) (утратила силу) // Российская газета. 2000. 28 сент.

[65] *Лопатин В. Н., Пристанская О. В.* О проекте Федерального закона «О защите детей от информационной продукции, причиняющей вред их здоровью, нравственному и духовному развитию» // Информационное право. 2007. № 4. С. 7–13.

[66] Модельный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (принят постановлением МПА СНГ от 3 декабря 2009 г. № 33–15) // Информационный бюллетень МПА СНГ. 2010. № 46. С. 190–228.

[67] СЗ РФ. 2011. № 1. Ст. 48.

[68] *Горбачева Е. В.* Административно-правовое обеспечение информационной безопасности несовершеннолетних: дис. … канд. юрид. наук. Ростов-на-Дону, 2011;

Концепция информационной безопасности детей, разработанная большим исследовательским коллективом по заказу Роскомнадзора.[69]

С начала 2010-х гг. в связи с широким проникновением Интернета в России резко актуализируется проблема защиты пользователей сети от негативного контента. Фокус научного интереса здесь постоянно изменяется, включая все новые аспекты: детскую порнографию, интернет-травлю (буллинг), пропаганду терроризма, разжигание розни, подстрекательство к массовым беспорядкам, фейковые новости и т. д. Активно изучаются проблемы информационного противоборства в сети Интернет. Все перечисленные вопросы характеризуют современное предметное поле информационно-психологической безопасности.

Не стояло на месте и правовое регулирование. Начиная с июля 2012 г., когда впервые был учрежден правовой механизм блокировки интернет-ресурсов с противоправным контентом, по настоящее время в базовый Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[70] (далее – Закон об информации) было внесено большое количество поправок, направленных на противодействие различным угрозам информационно-психологического характера. Многочисленные изменения были внесены и в иные законодательные акты. Все они требуют системного научного осмысления.

Революционным шагом в плане переоценки значения роли информационной безопасности в официальной системе взглядов стало принятие в 2021 г. новой Стратегии национальной безопасности Российской Федерации[71] (далее – Стратегия НБ 2021). В документе информационная безопасность впервые выделена в качестве стратегического национального приоритета. Данный приоритет направлен на обеспечение реализации национальных интересов РФ, связанных с развитием безопасного информационного пространства, защитой российского общества от деструктивного информационно-психологического воздействия (пп. 4 п. 25 Стратегии НБ 2021). Таким образом, в базовом документе стратегического планирования в области безопасности информационно-психологическая безопасность (лингвистически обозначенная несколько иначе) получила четкое закрепление в качестве национального интереса РФ.

Информационная безопасность детей: российский и зарубежный опыт: монография / Л. Л. Ефимова, С. А. Кочерга. М.: ЮНИТИ-ДАНА, 2013; *Богатырева Ю. И.* Подготовка будущих педагогов к обеспечению информационной безопасности школьников: дис. … д-ра педагог. наук. Тула, 2014; *Трухачева М. А.* Культура детства в информационном обществе: дис. … канд. культурологии. Саратов, 2019.

[69] Концепция информационной безопасности детей // Роскомнадзор. 25.11.2013. URL: http://rkn.gov.ru/mass-communications/p700/p701/ (дата обращения: 27.12.2013).

[70] СЗ РФ. 2006. № 31. Ст. 3448.

[71] Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 2 июля 2021 г. № 400) // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001 (дата обращения: 08.07.2021).

Рассмотрев эволюцию информационных угроз и показав современный контекст и новые формы их проявления, мы первично очертили предметный блок информационно-психологической безопасности и законодательную базу ее правового регулирования. Перейдем к непосредственному изучению ее сущностных характеристик и содержания.

§ 2. Методологические основания исследования информационно-психологической безопасности в информационном праве

В науке информационного права сложился определенный алгоритм анализа проблем правового обеспечения информационной безопасности. Он предполагает определение понятийного аппарата в рассматриваемой сфере, места и роли информационной безопасности в системе национальной безопасности, установление национальных интересов в данной области, раскрытие содержания принципов, задач и функций обеспечения информационной безопасности, а также характеристик системы правового регулирования общественных отношений в рассматриваемой сфере.[72]

Начнем наше исследование информационно-психологической безопасности (далее – ИПБ) с определения ее места в системе национальной безопасности. В соответствии со Стратегией НБ 2021 национальная безопасность есть «состояние защищенности национальных интересов РФ от внешних и внутренних угроз» (пп. 1 п. 5).

В документах стратегического планирования и законодательстве Российской Федерации наблюдаются различные подходы к определению видов безопасности. В Стратегии НБ 2021 выделены государственная, общественная, информационная, экологическая и иные виды безопасности (п. 26). В предыдущих документах – Стратегии национальной безопасности 2015 г.[73] (далее – Стратегия НБ 2015) и Стратегии национальной безопасности до 2020 г.[74] (далее – Стратегия НБ 2009) – перечислялись военная (оборона), государственная, общественная, информационная, экологическая, экономическая, транспортная, энергетическая безопасность, безопасность личности и др. В ст. 1 Федерального закона от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[75] указаны общественная и экологиче-

[72] *Бачило И. Л.* Информационное право: учебник для магистров. 3-е изд., перераб. и доп. М.: Юрайт, 2015. С. 481–504; Актуальные проблемы информационного права. С. 358–411.

[73] Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31 декабря 2015 г. № 683) (утратила силу) // СЗ РФ. 2016. № 1. Ст. 212.

[74] Стратегия национальной безопасности Российской Федерации до 2020 года (утв. Указом Президента РФ от 12 мая 2009 г. № 537) (утратила силу) // СЗ РФ. 2009. № 20. Ст. 2444.

[75] Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // СЗ РФ. 2011. № 1. Ст. 2.

ская безопасность, а также безопасность государства и личности. Схожая картина имеет место и в научной литературе, поскольку исследователи не всегда заботятся о соблюдении логических правил их классификации.[76]

Выделение информационной безопасности (*англ.* information security) в системе видов безопасности является общепризнанным как в России, так и за рубежом. Как отмечает В. Н. Лопатин, термин «информационная безопасность» впервые был выведен на государственный уровень в нашей стране в 1989 г., когда решением Президиума Верховного Совета СССР была организована рабочая комиссия по совершенствованию системы национальной безопасности под руководством академика Ю. А. Рыжова.[77]

Признание субстантивной роли информационной безопасности в системе национальной безопасности в России произошло в 2000 г. с принятием Доктрины информационной безопасности Российской Федерации (далее – Доктрина ИБ 2000), которая определила ее как «состояние защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» (пп. «б» п. 6).

В 2016 г. утверждена новая Доктрина информационной безопасности Российской Федерации»[78] (далее – Доктрина ИБ 2016), которая закрепила дефиницию информационной безопасности как «состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз» (пп. «в» п. 2).

Обе изложенные дефиниции носят достаточно широкий характер и наполняются конкретным содержанием через определение национальных интересов России в информационной сфере. Изучение их перечня (разделы II Доктрины ИБ 2000 и Доктрины ИБ 2016) прямо не обнаруживает искомый психологический компонент информационной безопасности. Однако его сущностные признаки просматриваются в положениях, касающихся сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа РФ, доведения до российской и международной общественности достоверной информации о государственной политике РФ и ее официальной позиции по социально значимым событиям в стране и мире, а также применения информационных технологий в целях обеспечения национальной безопасности РФ в области культуры.

Кроме того, анализ разделов данных документов стратегического планирования, определяющих угрозы и состояние информационной безопасности и основные направления ее обеспечения (разделы III, IV Доктрины ИБ 2000 и Доктрины ИБ 2016), обнаруживает гораздо более четкую

[76] Правовая основа обеспечения национальной безопасности Российской Федерации: монография / Под ред. проф. А. В. Опалева. М.: ЮНИТИ-ДАНА, 2004. С. 16.

[77] *Лопатин В. Н.* Информационная безопасность России: дис. … д-ра юрид. наук. СПб., 2000. С. 86.

[78] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) // СЗ РФ. 2016. № 50. Ст. 7074.

фиксацию блока вопросов ИПБ. Так, в Доктрине ИБ 2016 среди направлений обеспечения информационной безопасности в области обороны страны выделена «нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества» (пп. «д» п. 21).

В российской науке среди исследователей информационной безопасности долгое время доминировал узкий подход к ее пониманию как защиты информации и информационных систем.[79] Такое усеченное видение легло в основу базового законодательного акта для информационной сферы 1990-х гг. – Федерального закона от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации».[80] Во многом подход сохранился и в пришедшем ему на смену Законе об информации 2006 г. В этой связи О. С. Макаров обоснованно сетовал на то, что «проблема информационной безопасности часто искусственно сужается до технических аспектов защиты информации, при этом опускаются прежде всего ее социально-гуманитарные аспекты».[81]

Однако начиная с 1990-х гг. рядом исследователей развивался и альтернативный подход. Среди них следует выделить одного из основоположников теории правового обеспечения информационной безопасности В. Н. Лопатина.[82] В дальнейшем широкий подход к трактовке информационной безопасности, предполагающий включение в ее содержание психологических аспектов, находит все больше сторонников. В 2006 г. Р. М. Юсупов пришел к выводу о том, что «в теории и практике информационной безопасности уже начинают выкристаллизовываться два направления (две проблемы), которые можно определить (возможно, еще в некоторой степени условно) как информационно-психологическая безопасность и защита информации».[83]

В диссертационных исследованиях по политико-правовым аспектам ИБ авторы также придерживаются расширенной парадигмы ее понимания.[84] В специализированном словаре в качестве основы информационной

---

[79] См.: *Приходько А. Я.* Информационная безопасность в событиях и фактах. М.: СИНТЕГ, 2001; *Ярочкин В. И.* Информационная безопасность: учебник для студентов вузов. 2-е изд. М.: Академический Проект; Гаудеамус, 2004; *Филин С. А.* Информационная безопасность: учебное пособие. М.: Альфа-Пресс, 2006; *Макаренко С. И.* Информационная безопасность: учебное пособие для студентов вузов. Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009; *Борисов М. А., Романов О. А.* Основы организационно-правовой защиты информации. М.: Книжный дом «Либроком», 2012 и др.

[80] СЗ РФ. 1995. № 8. Ст. 609.

[81] *Макаров О. С.* Актуальные аспекты обеспечения информационной безопасности государств – участников Содружества Независимых Государств: монография. Минск: Ин-т нац. безопасности Респ. Беларусь, 2013. С. 6.

[82] *Лопатин В. Н.* Информационная безопасность России: дис. … д-ра юрид. наук. СПб., 2000.

[83] *Юсупов Р. М.* Наука и национальная безопасность. СПб.: Наука, 2006. С. 119.

[84] *Полякова Т. А.* Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … д-ра юрид. наук. М., 2008. С. 83,

безопасности общества определена «безопасность индивидуального, группового и массового сознания граждан при наличии информационных угроз, к которым в первую очередь следует отнести информационно-психологические воздействия».[85]

Важнейшее значение для утверждения ИПБ в качестве составляющей предмета правового регулирования в области информационной безопасности имело ее отражение в двух знаковых научных правотворческих инициативах.

Во-первых, в изданной в 2014 г. Концепции Информационного кодекса Российской Федерации, разработанной авторским коллективом ИГП РАН, среди основных принципов в области правового обеспечения ИБ названо «сдерживание распространения информации террористического, экстремистского и сепаратистского характера, а также подрывающей политическую, экономическую и социальную стабильность государства, культурный и духовный уклад общества».[86]

Во-вторых, в 2014 г. Межпарламентской ассамблеей СНГ был принят Модельный закон «Об информации, информатизации и обеспечении информационной безопасности».[87] Такое название документа было предложено видными российскими учеными И. Л. Бачило и М. А. Вусом, которые обосновывали его необходимостью включения в закон норм «о защите открытой информации от возможного ее деструктивного воздействия на сознание и поведение массового потребителя распространяемых сведений».[88] Этот содержательный блок нашел отражение в тексте данного документа: в число объектов обеспечения информационной безопасности

94; *Андреев П. Г.* Институциональное развитие правового обеспечения информационной безопасности в российском информационном праве: дис. … канд. юрид. наук. Екатеринбург, 2012. С. 22–23; *Кучерявый М. М.* Информационное измерение политики национальной безопасности России в условиях современного глобального мира: дис. … д-ра полит. наук. М., 2014. С. 96–97.

[85] Абрис проблемы информационной безопасности // Словарь-справочник по информационной безопасности для Парламентской Ассамблеи ОДКБ / Под общ. ред. М. А. Вуса и М. М. Кучерявого. СПб.: СПИИ РАН, 2014. С. 14.

[86] Концепция Информационного кодекса Российской Федерации / Под ред. И. Л. Бачило. М.: ИГП РАН, 2014. С. 93.

[87] Модельный закон «Об информации, информатизации и обеспечении информационной безопасности» (принят постановлением Межпарламентской ассамблеи государств – участников СНГ № 41–15 от 28 ноября 2014 г.) // МПА СНГ. URL: http://www.iacis.ru/upload/iblock/25c/prilozhenie_k_postanovleniyu_15.pdf (дата обращения: 14.01.2015).

[88] *Бачило И. Л., Вус М. А.* Аналитическая записка к вопросу о проекте изменений в Модельный закон «Об информации, информатизации и защите информации», представленная по пункту 8 Повестки дня заседания Объединенной комиссии при Межпарламентской ассамблее СНГ по гармонизации законодательства в сфере безопасности и противодействия новым вызовам (17 апреля 2014 г.). Следует отметить, что данную позицию разделяет А. А. Чеботарева, обосновавшая необходимость внесения аналогичных изменений в название Федерального закона «Об информации, информационных технологиях и о защите информации». См.: *Чеботарева А. А.* Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: дис. …д-ра юрид. наук. М., 2017. С. 121–122.

отнесены индивидуальное и общественное сознание (ч. 2 ст. 18); отдельная статья посвящена защите от распространения вредной и использования деструктивной информации (ст. 25).

Логичным, но революционным по своему значению шагом стало отнесение защиты российского общества от деструктивного информационного-психологического воздействия к числу основополагающих национальных интересов РФ в новой Стратегии национальной безопасности (пп. 4 п. 25). В документе определен ряд задач по обеспечению ИПБ в тематическом подразделе «Информационная безопасность» (п. 57).

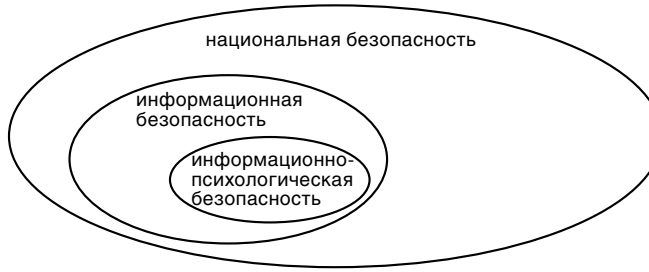


Рис. 1. Место информационно-психологической безопасности в структуре национальной безопасности

Таким образом, в настоящее время можно уверенно сделать вывод о том, что ИПБ входит в содержание информационной безопасности (см. рис. 1). Из этого следует вывод, что ИПБ «обладает общими признаками, присущими данному виду безопасности, важнейшими из которых являются информационный характер угроз безопасности и информационная сфера как область проявления данных угроз».[89]

В действующем законодательстве РФ сформировались следующие правовые институты в структуре подотрасли правового обеспечения информационной безопасности:

1) защита информации, включая защиту отдельных видов информации ограниченного доступа[90];

2) защита критически важных объектов информационной инфраструктуры[91];

3) защита детей от информации, причиняющей вред их здоровью и развитию[92];

---

[89] *Смирнов А. А.* К вопросу о понятии, объекте и содержании информационно-психологической безопасности // Административное право и процесс. 2013. № 1. С. 35.

[90] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне», Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»; Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

[91] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[92] Федеральный закон от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»; Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

4) противодействие распространению противоправной информации в СМИ и сети Интернет.[93]

Последние два пункта характеризуют сферу ИПБ.

Обратим внимание на вопросы терминологии. Сам термин «информационно-психологическая безопасность» пока не получил общепризнанного статуса ни в информационном праве, ни в других науках,[94] хотя он встречается в диссертационных исследованиях[95] и иных научных трудах российских ученых.[96]

Анализ действующего российского законодательства показывает, что данный термин в нем не употребляется. Даже в важнейшем для исследуемой области Законе о защите детей от информации для характеристики «состояния защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» используется понятие «информационная безопасность детей», а не информационно-психологическая безопасность. Законопроект «Об информационно-психологической

[93] Закон РФ от 27 декабря 1991 г. № 2124–1 «О средствах массовой информации»; Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»; Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 13 марта 2006 г. № 38-ФЗ «О рекламе» и др.

[94] В этом плане вряд ли можно согласиться с В. Е. Усановым и Н. П. Кирилловым, утверждавшими в 2009 г., что понятие ИПБ на практике стало «фактически общепризнанным и основным терминологическим обозначением в литературе для психологической разновидности информационной безопасности». (См.: *Усанов В. Е., Кириллов Н. П.* Психологическая безопасность российского общества и проблемы ее социально-правового обеспечения: учебник. М.: Издательство «Элит», 2009. С. 60.) К сожалению, даже в настоящий период общепризнанного статуса это понятие не приобрело.

[95] *Грачев Г. В.* Информационно-психологическая безопасность личности: теория и технология психологической защиты: дис. … д-ра психол. наук. М., 2000; *Некляев С. А.* Участие средств массовой информации в обеспечении информационно-психологической безопасности в условиях локальных войн и международного терроризма: дис. … канд. филолог. наук. М., 2003; *Чистяков Д. В.* Управление информационно-психологической защитой социальной организации как фактор обеспечения безопасности личности: социологический аспект: дис. … канд. социолог. наук. М., 2007; *Мельницкая Т. Б.* Информационно-психологическая безопасность населения в условиях риска радиационного воздействия: концепция, модель, технологии: дис. … д-ра психол. наук. Обнинск, 2009; *Рыдченко К. Д.* Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации: дис. … канд. юрид. наук. Воронеж, 2011; *Вольнов Р. В.* Психолого-правовые особенности обеспечения информационно-психологической безопасности личности: дис. … канд. психол. наук. М., 2011 и др.

[96] *Смолян Г. Л., Зараковский Г. М., Розин В. М., Войскунский А. Е.* Информационно-психологическая безопасность (определение и анализ предметной области). М.: Институт системного анализа РАН, 1997; *Емельянов Г. В., Лепский В. Е., Стрельцов А. А.* Проблемы обеспечения информационно-психологической безопасности России // Информационное общество. 1999. № 3. С. 47–51; *Сапожникова А.* Информационно-психологическая безопасность России: состояние и тенденции // Власть. 2008. № 2. С. 8–14; *Степанов А. М., Бухтояров А. А., Бутенко Д. В.* Проблемы правовой политики обеспечения информационно-психологической безопасности // Информационное право. 2012. № 1. С. 30–35; Информационно-психологическая и когнитивная безопасность: коллективная монография / Под ред. И. Ф. Кефели, Р. М. Юсупова. СПб.: ИД «Петрополис», 2017.

безопасности»[97] как исключение из общего тренда не был принят. В Стратегии НБ 2021, Доктрине ИБ 2016 и других действующих документах стратегического планирования искомый термин также отсутствует.

Автор видит необходимость введения понятия «информационно-психологическая безопасность» в юридические науки и правовую практику по следующим причинам:

а) потребность в рельефном обозначении «психологической» составляющей информационной безопасности;

б) присутствие ярко выраженной специфики в системе информационной безопасности;

в) наличие четкой грани между защитой информации и информационно-психологической безопасностью по критериям объекта и методов воздействия;

г) существование комплекса специфических угроз;

д) преимущество перед другими конкурирующими терминами (духовная,[98] идеологическая,[99] культурная,[100] информационно-коммуникационная[101] безопасность), позволяющими интегрировать психологические компоненты информационной безопасности в целостный объект правового регулирования;

е) общность правового инструментария, используемого для защиты от различных форм деструктивного информационно-психологического воздействия.

---

[97] Проект федерального закона № 99114515–2 «Об информационно-психологической безопасности» (ред., внесенная в ГД ФС РФ, текст по состоянию на 03.12.1999) // СПС «КонсультантПлюс».

[98] *Возьмитель А. А.* Духовная безопасность: актуальные теоретико-методологические и практические вопросы // Безопасность Евразии. 2005. № 3. С. 229–253; *Беспаленко П. Н.* Духовная безопасность в системе национальной безопасности современной России: проблемы институционализации и модели решения: дис. … д-ра полит. наук. М., 2009; *Тонконогов А. В.* Духовная безопасность российского общества в условиях современного геополитического соперничества (социально-философский анализ): дис. … д-ра философ. наук. М., 2011; *Саенко Н. Р., Саенко А. В.* Духовная безопасность как составляющая национальной безопасности России // Успехи современной науки. 2016. № 1. С. 94–97.

[99] *Маршак А. Л.* Идеологическая безопасность нации: к вопросу о формировании новой идеологии российского общества // Общество и право. 2004. № 4 (6). С. 141–144; *Солодовник Л. В.* Идеологическая безопасность российского общества в контексте трансформационных вызовов современности: дис. … д-ра философ. наук: Ростов-на-Дону, 2013.

[100] *Романова А. П., Хлыщева Е. В., Якушенков С. Н., Топчиев М. С.* Чужой и культурная безопасность. М.: РОССПЭН, 2013; *Сергеев В. В.* Формирование культурной безопасности в условиях модернизации российского общества: дис. … д-ра социол. наук. М., 2011; *Щукина Е. Л.* Культурная безопасность современной России как элемент национальной безопасности // Государственное и муниципальное управление. Ученые записки СКАГС. 2015. № 3. С. 346–350; *Ершов Н. В.* Культурная безопасность общества и государства и ее основные угрозы // Управленческое консультирование. 2017. № 12. С. 111–119.

[101] Массмедиа в условиях глобализации: Информационно-коммуникационная безопасность: монография / Под общ. ред. В. И. Василенко. М.: Проспект, 2015.

Принципиальное отличие ИПБ от традиционного блока информационной безопасности состоит в том, что ее содержанием выступает не защита информации, а *защита от информации*. Защита кого/чего? Прежде всего самого человека и общества в целом. С учетом этого ИПБ можно определить как защиту личности и общества от негативного информационно-психологического воздействия. Такой подход поддерживается рядом исследователей. Так, ученые из Института системного анализа (далее – ИСА) РАН еще в 1997 г. писали о том, что «исследования вокруг проблематики ИПБ так или иначе фокусировались вокруг понятия информационно-психологического воздействия, а информационно-психологическая безопасность трактовалась как защищенность от этих воздействий».[102] Такой позиции придерживались и другие ведущие исследователи того периода, включая В. Н. Лопатина, Г. В. Емельянова, В. Е. Лепского и А. А. Стрельцова.[103]

Разделяем данное мнение. Здесь, на наш взгляд, проходит грань между ИПБ и «психологической безопасностью», которая в психологии во многом связывается с внутренними состояниями и процессами, например интегрированностью бессознательных желаний и установок личности, согласованностью сенсорного опыта и Я-концепции и т. д.[104] Эти вопросы находятся за рамками изучаемой нами проблематики.

В качестве базового методологического подхода к изучению ИПБ считаем необходимым использовать *междисциплинарный подход*. В философии междисциплинарные исследования трактуются как «способ организации исследовательской деятельности, предусматривающий взаимодействие в изучении одного и того же объекта представителей различных дисциплин».[105] Автор рассматривает междисциплинарный подход как методологический принцип проведения индивидуального научного исследования, предполагающий заимствование и применение знаний и методов из других сфер научного знания. Ученые из ИГП РАН называют развитие междисциплинарных правовых знаний одним из ключевых направлений трансформации права, подчеркивая потребность нахождения юридической наукой взаимосвязи с другими научными

[102] *Смолян Г. Л., Зараковский Г. М., Розин В. М., Войскунский А. Е.* Информационно-психологическая безопасность (определение и анализ предметной области). М.: Институт системного анализа РАН, 1997.

[103] *Лопатин В. Н.* Информационная безопасность России: дис. … д-ра юрид. наук. СПб., 2000; *Емельянов Г. В., Лепский В. Е., Стрельцов А. А.* Проблемы обеспечения информационно-психологической безопасности России // Информационное общество. 1999. № 3. С. 47–51.

[104] Психологическая безопасность личности: имплицитная и эксплицитная концепции. М.: Институт психологии РАН, 2017. С. 13–29.

[105] *Мирский Э. М.* Междисциплинарные исследования // Новая философская энциклопедия. В 4 т. Институт философии РАН; Национальный общественно-научный фонд; председатель научно-редакционного совета В. С. Степин. М.: Мысль, 2000–2001. Интернет-версия издания. URL: https://iphlib.ru/library/collection/newphilenc/document/HASHf38bc2e78334014b0106f3?p.s=TextQuery (дата обращения: 12.01.2020).

дисциплинами технического и гуманитарного профиля.[106] В этом же ключе высказывается Г. Г. Камалова.[107]

Акцент на междисциплинарность связан с тем, что рассматриваемая предметная область ИПБ изначально носит гибридный характер и находится на стыке ряда сфер: информационных технологий, психологии и безопасности.[108] Поэтому для изучения проблемы правового обеспечения ИПБ, помимо базовой юридической науки, наибольший интерес представляют три области научного знания: психология, социология массовой коммуникации и науки об информационных технологиях.

Психология изучает содержание и механизм работы индивидуальной и коллективной психики – основных объектов ИПБ, а также механизм информационно-психологического воздействия. Именно психологические знания позволяют выявить потенциальную опасность определенной информации/коммуникации для людей и социальных групп различных категорий, например для детей разных возрастных групп.

Социология массовой коммуникации исследует особенности современной информационной среды общества, ее влияние на социум, а также изучает основные институты и типы массовой коммуникации. Знания из данной научной области помогают правильно подобрать инструментарий для нейтрализации угроз ИПБ и их источников и ранжировать по значимости объекты для его применения.

Информатика и прочие науки об информационных технологиях изучают каналы и способы технической передачи информации, посредством которой оказывается деструктивное информационно-психологическое воздействие. Данная область науки позволяет понимать особенности технических каналов распространения негативной информации и, соответственно, выбирать адекватные способы и средства воздействия на них.

---

[106] Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. д. ю. н., профессора Т. А. Поляковой. Саратов: Амирит, 2020. С. 30; *Полякова Т. А.* Цифровизация и синергия правового обеспечения информационной безопасности // Информационное право. 2019. № 2. С. 4–7.

[107] *Камалова Г. Г.* Правовые аспекты обеспечения доступности и достоверности информации в цифровую эпоху в условиях пандемии COVID-19 // Аграрное и земельное право. 2021. № 10. С. 149.

[108] Значимость использования «междисциплинарной рефлексии» при изучении информационно-психологической безопасности подчеркивают в своих трудах такие авторитетные российские психологи, как Л. В. Матвеева и А. Е. Войскунский. См.: *Матвеева Л. В.* Гуманитарная составляющая информационной безопасности в СМИ // Информационная и психологическая безопасность в СМИ. В 2 т. Т. I: Телевизионные и рекламные коммуникации / Под ред. А. И. Донцова, Я. Н. Засурского, Л. В. Матвеевой, А. И. Подольского и др. М.: Аспект Пресс, 2002. С. 34; *Войскунский А. Е.* Информационная безопасность: психологические аспекты // Национальный психологический журнал. 2010. № 1. С. 49.

Применение междисциплинарного подхода позволяет нам составить представление об объектах ИПБ. Объекты безопасности являются одной из ключевых характеристик любого вида безопасности, которые во многом определяют стратегию и инструменты ее обеспечения. В теории безопасности под ними понимаются «реально существующие явления, процессы и отношения, предупреждение или устранение угроз которым составляет цель и основное содержание политики безопасности».[109] Применительно к сфере ИПБ речь идет об объектах деструктивного информационно-психологического воздействия.

Среди исследователей отсутствует единое мнение относительно объектов ИПБ. В. Н. Лопатин относит к ним «отдельных лиц и группы лиц»,[110] К. Д. Рыдченко – «индивидуальную психику и общественное сознание»,[111] Т. Б. Мельницкая – «индивидуальное, групповое и общественное сознание»,[112] Г. В. Грачев – «индивидуальную, групповую и общественную психологию и, соответственно, социальные субъекты различных уровней общности, масштаба, системно-структурной и функциональной организации»,[113] представители психоэкологического направления – «внутренний мир человека».[114] В проекте федерального закона «Об информационно-психологической безопасности» в качестве объектов ИПБ назывались «человек и группы лиц» (ст. 1, 2), хотя в ряде норм отдельно упоминается «психика человека». В Стратегии НБ 2021 объектом защиты от деструктивного информационно-психологического воздействия названо «российское общество» (пп. 4 п. 25).

В представленных вариантах наблюдается двойственность объектов ИПБ: к ним относят как самого человека, группы людей и общество в целом, так и их психологические составляющие – индивидуальную психику и общественное сознание. На наш взгляд, здесь нет противоречия, а отмеченный дуализм обусловлен разным уровнем детализации при характеристике объектов ИПБ. Более того, по нашему мнению, следует также выделить и третий уровень детализации, на котором в качестве

---

[109] Безопасность Евразии-2002: энциклопедический словарь-ежегодник / Автор идеи и концепции, руководитель проекта В. Н. Кузнецов. М., 2003. С. 255.

[110] *Лопатин В. Н.* Информационная безопасность России: дис. … д-ра юрид. наук. СПб., 2000. С. 262.

[111] *Рыдченко К. Д.* Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации: дис. … канд. юрид. наук. Воронеж, 2011. С. 10.

[112] *Мельницкая Т. Б.* Информационно-психологическая безопасность населения в условиях риска радиационного воздействия: концепция, модель, технологии: дис. … д-ра психол. наук. СПб., 2009. С. 8.

[113] *Грачев Г. В.* Информационно-психологическая безопасность личности: теория и технология психологической защиты: дис. … д-ра психол. наук. М., 2000 С. 61, 63.

[114] *Степанов А. М., Бухтояров А. А., Бутенко Д. В.* Проблемы правовой политики обеспечения информационно-психологической безопасности // Информационное право. 2012. № 1. С. 32–34.

объектов ИПБ будут рассматриваться отдельные индивидуальные и групповые психические процессы и явления.

В плане правового регулирования выбор требуемого уровня детализации будет зависеть от характера и предмета правового акта: для базового закона или документа стратегического планирования целесообразнее использовать первый и второй уровни, тогда как для более узкого предмета правового регулирования подойдет третий уровень детализации. Так, в Доктрине ИБ 2016 говорится о «наращивании информационного воздействия на население России» (п. 12) и использовании экстремистами механизмов «информационного воздействия на индивидуальное, групповое и общественное сознание» (п. 13); в главе 25 Уголовного кодекса Российской Федерации[115] (далее – УК РФ) в качестве видового объекта преступлений выделена общественная нравственность, а непосредственным объектом административного правонарушения, предусмотренного ч. 1 ст. 13.15 Кодекса Российской Федерации об административных правонарушениях[116] (далее – КоАП РФ), определено подсознание людей.

Представим собственное видение объектов ИПБ на трех уровнях детализации, использовав научные знания из общей и социальной психологии и социологии.

На первом уровне объектами ИПБ выступают личность, большие и малые социальные группы**.** Очевидно, что первичным объектом ИПБ является *личность*, на которую оказывается информационно-психологическое воздействие. Как точно отмечает Г. В. Грачев, «именно человек как личность и активный социальный субъект, его психика подвержены непосредственному действию информационных факторов, которые, трансформируясь через его поведение, действия (или бездействие), оказывают дисфункциональное влияние на социальные субъекты разного уровня общности, различной системно-структурной и функциональной организации».[117]

Объектом деструктивного информационно-психологического воздействия может выступать конкретный индивид при целенаправленном влиянии либо некий абстрактный человек при оказании воздействия неизбирательного типа.

Следующим объектом ИПБ выступают *социальные группы*. П. Штомпка дает определение социальной группы как «группы людей, в которой общность общественно значимых черт выражается в коллективной идентичности и сопровождающих ее контактах, взаимодействиях

[115] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

[116] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СЗ РФ. 2002. № 1. Ст. 1.

[117] *Грачев Г. В.* Информационно-психологическая безопасность личности: теория и технология психологической защиты: дис. … д-ра психол. наук. М., 2000. С. 63.

и социальных отношениях».[118] Социальные группы в науке рассматриваются как *психологические общности людей*, обладающие общей идентичностью и групповой психикой.

В общественных науках существует целый ряд классификаций социальных групп, в соответствии с которыми они подразделяются на большие и малые, первичные и вторичные, формальные и неформальные, устойчивые (прочные) и неустойчивые («мимолетные»), однофункциональные и многофункциональные, открытые и закрытые и т. д.[119] Нами за основу будет взята классификация социальных групп на большие и малые, так как указанные виды групп значительно отличаются друг от друга в плане характеристик их психических структур.

Под большой социальной группой (далее – БСГ) понимается реальная, значительная по размерам и сложно организованная общность людей, вовлеченных в ту или иную общественную деятельность.[120] Именно они, по справедливому замечанию А. И. Донцова, определяют ход истории.[121] Высшим уровнем больших социальных групп является общество в целом, существующее в рамках государственных границ.[122] На следующем уровне выделяются различные виды БСГ в рамках социальной стратификации: социальные классы, социальные слои, этнические группы, гендерные и возрастные группы и т. д.[123] В Доктрине ИБ 2016 главным объектом информационного воздействия на население России в целях размывания традиционных российских духовно-нравственных ценностей названа молодежь (п. 12).

---

[118] *Штомпка П.* Социология. Анализ современного общества / Пер. с польск. С. М. Червонной. М.: Логос, 2005. С. 619.

[119] *Донцов А. И.* О понятии «группа» в социальной психологии // Вестник Московского университета. Сер. 14. Психология. 1997. № 4. С. 24–25; *Штомпка П.* Социология. Анализ современного общества / Пер. с польск. С. М. Червонной. М.: Логос, 2005. С. 208–238; *Яковлев А. М.* Социальные общности и группы // Социология. Основы общей теории: учебник для вузов / Отв. ред. академик РАН Г. В. Осипов, действительный член РАЕН Л. Н. Москвичев. М.: Норма, 2003. С. 269–273.

[120] Группа большая // Психология. Словарь / Под общ. ред. А. В. Петровского, М. Г. Ярошевского. 2-е изд., испр. и доп. М.: Политиздат, 1990 С. 85.

[121] *Донцов А. И.* О понятии «группа» в социальной психологии. // Вестник Московского университета. Сер. 14. Психология. 1997. № 4. С. 17.

[122] Хотя в условиях формирования глобального информационного общества в качестве объекта информационно-психологического воздействия может рассматриваться мировое сообщество в целом. Мировые СМИ и информационные ресурсы сети Интернет влияют на глобальную аудиторию, вызывая отклики в различных частях света. В социологии необходимость расширения масштабов понимания социального пространства до общемирового была заявлена В. А. Ядовым в качестве одного из базовых требований новой научной парадигмы. См.: *Ядов В. А.* Стратегия социологического исследования: описание, объяснение, понимание социальной реальности: учебное пособие. М.: Омега-Л, 2011. С. 19–20.

[123] Так, Д. Волкогонов в качестве приоритетных групповых объектов психологической войны называл молодежь, интеллигенцию и военнослужащих. См.: *Волкогонов Д. А.* Психологическая война: Подрывные действия империализма в области общественного сознания. М.: Воениздат, 1984. С. 6–7.

Под малой социальной группой (далее – МСГ) понимается немногочисленная по составу группа, члены которой объединены общей социальной деятельностью и находятся непосредственно в личном общении, что является основой для возникновения эмоциональных отношений, групповых норм и групповых процессов.[124] Примеры МСГ весьма многочисленны: к их числу можно отнести семью, учебный класс, трудовой коллектив, спортивную команду и т. п.

Большие и малые социальные группы преимущественно выступают объектами воздействия неизбирательного или ограниченно избирательного информационно-психологического воздействия со стороны средств массовой коммуникации или во время массовых офлайновых мероприятий.

Новым видом социальных групп, возникшим благодаря развитию социальных интернет-сервисов, стали *виртуальные группы (сообщества)*. Как отмечает Н. С. Чураева, «формирование и устойчивое существование виртуального сообщества как социальной группы возможно только при наличии у участников сетевого ресурса общих интересов, совместно выработанных целей и организованных действий по их достижению, которые реализуются в рамках единого коммуникативного пространства».[125]

Приоритетным объектом правовой защиты от деструктивного информационно-психологического воздействия на уровне социальных групп выступают дети (несовершеннолетние) по причине их особой уязвимости, обусловленной их психологическими особенностями, включая некритичность восприятия информации, неустойчивость и эластичность ценностных ориентаций и поведенческих установок, высокой степенью бессознательного заражения эмоциональными состояниями, склонностью к подражанию поведению показанных героев, реализмом воображения.[126]

На втором уровне детализации мы переходим к рассмотрению конкретных «психологических составляющих» объектов ИПБ, обозначенных выше. Применительно к личности таким объектом выступает *человеческая психика*. В отечественной науке она определяется как «системное свойство высокоорганизованной материи, заключающееся в активном отражении субъектом объективного мира, в построении субъектом неотчуждаемой от него картины этого мира и саморегуляции на этой основе своего поведения и деятельности».[127] Последний тезис, показывающий значение карты окружающего мира как основы регуля-

---

[124] *Андреева Г. М.* Социальная психология: учебник для высших учебных заведений. 5-е изд., испр. и доп. М.: Аспект Пресс, 2005. С. 183.

[125] *Чураева Н. С.* Социально-психологические механизмы формирования виртуальных сообществ: автореф. дис. … канд. психол. наук. М., 2009. С. 7.

[126] *Новиков К. Ю.* Психология. Дети. СМИ. М.: Издательство ИКАР, 2008. С. 25, 187.

[127] Психика // Психология. Словарь / Под общ. ред. А. В. Петровского, М. Г. Ярошевского. 2-е изд., испр. и доп. М.: Политиздат, 1990. С. 299.

ции поведения человека, представляется нам исключительно важным. Оказывая воздействие на картину мира человека, мы тем самым можем влиять на его поведение.

Выбор для обозначения объекта ИПБ термина «психика» вместо «индивидуального сознания», предлагаемого другими авторами (К. Д. Рыдченко, Т. Б. Мельницкой и др.), связан с тем, что понятие психики является более широким и помимо сознания включает также бессознательное (подсознание), которое также может выступать объектом деструктивного информационно-психологического воздействия. Такой точки зрения придерживались многие ведущие исследователи ИПБ в 1990-е гг. (В. Н. Лопатин, В. Е. Лепский, А. А. Стрельцов и др.).

Сознание рассматривается как высший уровень психического отражения и саморегуляции, присущий только человеку как общественно-историческому существу. Эмпирически сознание выступает как «непрерывно меняющаяся совокупность чувственных и умственных образов, непосредственно предстающих перед субъектом в его «внутреннем опыте» и предвосхищающих его практическую деятельность».[128] Индивидуальное сознание как объект информационного воздействия отмечено в доктринах ИБ 2000 и 2016 г.

Сознание как основная форма человеческой психики не исчерпывает ее содержания, поскольку «у человека имеются и несознаваемые психические явления и процессы, которые скрыты от его самонаблюдения».[129] Понятие *бессознательного* есть «гипотетический конструкт, используемый для описания действий, феноменов, данных, процессов и т. д., выходящих за пределы непосредственного сознавания».[130] Бессознательное трактуется как «совокупность психических процессов, актов и состояний, обусловленных явлениями действительности, о влиянии которых субъект не отдает себе отчета. Отражаемая им реальность сливается с переживаниями субъекта, его отношениями к миру, поэтому в нем невозможны произвольный контроль осуществляемых субъектом действий и оценка их результатов».[131]

Интересно, что в российском законодательстве для обозначения неосознаваемых психических процессов используется термин «подсознание», а не «бессознательное» (ст. 4 Закона РФ «О средствах массовой информации», ст. 13.15 КоАП РФ). Понятие *«подсознательное»* (*англ.* subconscious) в научной литературе по психологии употребляется редко,

---

[128] Там же. С. 368–369.

[129] *Леонтьев А. Е.* Психика // Большая советская энциклопедия. В 30 т. М.: Советская энциклопедия, 1969–1978. URL: http://bse.sci-lib.com (дата обращения: 14.03.2012).

[130] *Кэрич М. С.* Бессознательное // Психологическая энциклопедия. 2-е изд. / Под ред. Р. Корсини, А. Ауэрбаха. СПб.: Питер, 2006. С. 69.

[131] Бессознательное // Психология. Словарь / Под общ. ред. А. В. Петровского, М. Г. Ярошевского. 2-е изд., испр. и доп. М.: Политиздат, 1990. С. 38.

поскольку вместо него для обозначения неосознаваемых систем психики используется категория «бессознательное» (*англ.* unconscious). В этом случае они используются в качестве взаимозаменяемых феноменов, несмотря на попытки разграничить их содержание, в частности в психоанализе.[132]

Бессознательное является весьма значимым объектом ИПБ, поскольку деструктивное воздействие на него не подконтрольно человеку и не может блокироваться инструментами психологической защиты человека. В частности, влияние на бессознательное осуществляется при подпороговом (сублиминальном) воздействии. Показательно, что в законопроекте об ИПБ среди негативных последствий для субъектов, подвергающихся ИПВ, называлось «блокирование на неосознаваемом уровне свободы волеизъявления человека». Недостаток психологических знаний о природе и механизме функционирования бессознательного не умаляет важности задачи обеспечения его надежной защиты от негативного информационно-психологического воздействия.

Переходя к характеристике психологических компонентов социальных групп как объектов ИПБ, мы сталкиваемся с определенными сложностями, вызванными отсутствием устоявшегося терминологического аппарата. Очевидно, что речь, по сути, идет о *групповой психике*. Коллективные психические структуры не сводятся к некой «сумме психик» членов социальных групп, но составляют самостоятельную социальную реальность, а в нашем исследовании рассматриваются как обособленные объекты ИПБ. По словам Г. М. Андреевой, «по отношению к каждому отдельному „сознанию" групповая психология выступает как некая социальная реальность, выходящая за пределы сознания отдельного индивида и воздействующая на него вместе с другими объективными условиями жизни».[133]

Несмотря на то что подавляющее большинство психических характеристик социальных групп рассматриваются как элементы «группового сознания»,[134] в научной литературе выделяются и отдельные групповые психические неосознаваемые элементы,[135] что свидетельствует о сохранении дихотомии «сознательное – бессознательное» на групповом уровне.

Таким образом, *на втором уровне в качестве объектов ИПБ определены: психика человека, включающая сознание и бессознательное,*

[132] *Лейбин В. М.* Психоанализ и философия неофрейдизма. М.: Политиздат, 1977. С. 38.

[133] *Андреева Г. М.* Социальная психология: учебник для высших учебных заведений. 5-е изд., испр. и доп. М.: Аспект Пресс, 2005. С. 150.

[134] Групповое сознание // Оксфордский толковый словарь по психологии / Под ред. А. Ребера, 2002. С. 543.

[135] Бессознательное. Природа, функции, методы исследования / Под общ. ред. А. С. Прангишвили, А. Е. Шерозия, Ф. В. Бассина. Тбилиси: Мецниереба, Т. 1. 1978; *Юнг К. Г.* Психология бессознательного / Пер. с англ. 2-е изд. М.: Когито-Центр, 2010.

и групповые психические структуры, состоящие из группового (общественного) сознания и коллективного бессознательного.

На *третьем уровне детализации* мы должны выделить более мелкие психические компоненты индивидуальной и групповой психики, которые могут выступать объектом информационного воздействия.

Что касается элементов индивидуальной психики, то здесь в современной психологии сформированы устоявшееся представление и достаточно четкий понятийный аппарат. Для его системного изложения в нашем исследовании мы используем два подхода – динамический и статический, дополняющие друг друга.

Динамический подход предполагает выделение в структуре психики составляющих ее психических процессов,[136] которые обычно подразделяются на три основных вида: когнитивные, эмоциональные и регулятивно-волевые.[137] Статический подход исходит из выделения психических образований, являющихся результатами протекающих психических процессов. По словам С. Л. Рубинштейна, «всякое психическое образование (чувственный образ вещи, чувство и т. д.) – это, по существу, психический процесс в его результативном выражении».[138] Несмотря на сложность и трудоемкость задачи построения исчерпывающего перечня психических процессов и образований, ее решение имеет важное значение для правильной идентификации объектов правовой защиты.

Обобщив результаты исследования нами учебной и научной литературы,[139] энциклопедических изданий,[140] представим в табличном виде систему элементов психики человека (таблица 1).

---

[136] Выдающийся советский психолог С. Л. Рубинштейн писал, что «основным способом существования психического является его существование в качестве процесса, в качестве деятельности». См: *Рубинштейн С. Л.* Бытие и сознание. М.: Изд-во Академии наук СССР, 1957. С. 255.

[137] *Веккер Л. М.* Психические процессы. В 3 т. Л.: Издательство Ленинградского университета. Т. 1. 1974; Т. 2, 1976; Т. 3. 1981.

[138] *Рубинштейн С. Л.* Бытие и сознание. М.: Изд-во Академии наук СССР, 1975. С. 255–264.

[139] *Рубинштейн С. Л.* Основы общей психологии; Психология: учебник / В. В. Нуркова, Н. Б. Березанская…; *Веккер Л. М.* Психика и реальность: единая теория психических процессов. М.: Смысл, 1998; *Ильин Е. П.* Мотивация и мотивы. СПб.: Питер, 2011.

[140] Психология. Словарь / Под общ. ред. А. В. Петровского, М. Г. Ярошевского. 2-е изд., испр. и доп. М.: Политиздат, 1990; Большой психологический словарь / Сост. и общ. ред. Б. Г. Мещеряков, В. П. Зинченко. 4-е изд., расширенное. М.: АСТ; СПб.: Прайм-ЕВРОЗНАК, 2009; Оксфордский толковый словарь по психологии / Под ред. А. Ребера. 2002; Философский словарь / Под ред. И. Т. Фролова. 7-е изд., перераб. и доп. М.: Республика, 2001; *Душков Б. А., Королев А. В., Смирнов Б. А.* Энциклопедический словарь: Психология труда, управления, инженерная психология и эргономика. 2005; *Головин С. Ю.* Словарь практического психолога. Мн.: Харвест, 1998.

Таблица 1

Индивидуальные психические процессы и образования, составляющие структуру психики человека

Группа психических процессов	Психический процесс	Психические образования
Сознательные психические процессы и психические образования		
Регулятивно-волевые процессы	мотивация	потребности, мотивы, цели, интерес, желание, стремление, намерение
	воля	
	внимание[141]	–
Эмоциональный процесс	эмоциональный процесс	эмоции, чувства, настроение
Когнитивные процессы	ощущение	ощущения
	восприятие	перцептивные образы
	память	информация, воспоминания, представления памяти
	мышление	мысль, знание, понятие, суждение, умозаключение, решение
Бессознательные психические процессы и психические образования		
Регулятивно-волевые процессы	мотивация	несознаваемые побудители деятельности, неосознаваемые регуляторы способов выполнения деятельности (операциональные установки и стереотипы)
	воля	
	внимание	–
Эмоциональный процесс	эмоциональный процесс	аффекты
Когнитивные процессы	ощущение	проявления субсенсорного (подпорогового) восприятия, надсознательные явления
	восприятие	
	память	
	мышление	

В отличие от общей психологии, социальная психология не обладает устоявшимся категориальным аппаратом для обозначения элементов групповой психики. При этом одни понятия («групповые интересы», «общественное мнение», «групповая идентичность») имеют широкое признание и использование в науке, тогда как другие («групповое мышление», «групповая память») встречаются лишь в отдельных исследованиях и подвергаются сомнению в плане правомерности их употребления. Г. М. Андреева выделяла среди психологических

[141] Внимание как психический процесс регулятивного типа не имеет самостоятельного результата в виде обособленных психических образований, поскольку внимание лишь изменяет результат того психического процесса, к которому присоединяется. Как точно подметил П. Я. Гальперин, «и про себя, и внешнему наблюдателю внимание открывается как направленность, настроенность и сосредоточенность любой психической деятельности, следовательно, только как сторона или свойство психической деятельности». См.: *Гальперин П. Я.* К проблеме внимания // Психология внимания: хрестоматия / Под ред. Ю. Б. Гиппенрейтер, В. Я. Романова. М.: ЧеРо, 2001. С. 534–542.

характеристик группы следующие элементы: групповые потребности, интересы, ценности, нормы, цели, групповое мнение, – подчеркивая при этом, что «современный уровень развития социальной психологии не располагает ни традицией, ни необходимым методическим оснащением для анализа всех этих образований».[142]

На основе проведенного анализа научной литературы по социальной психологии[143] представим структуру психики социальных групп (таблица 2). Как и в предыдущей таблице, мы используем сочетание статического и динамического подходов, учитывая отличительные черты групповой психики. В частности, названия групповых психических процессов нами будут изложены в формулировках, употребляемых в научной литературе по социальной психологии.

Таким образом, на третьем уровне в качестве объектов ИПБ нами выделены индивидуальные и групповые психические процессы и образования сознательного и бессознательного характера и составлена их матрица.

Таблица 2

Групповые психические процессы и образования, составляющие структуру психики социальных групп

Группа психических процессов	**Психический процесс**	**Психические образования**
Групповое (общественное) сознание		
Регулятивно-волевые процессы	социальная мотивация	социальные потребности, социальные ценности, социальные интересы, социальная ориентация личности, социальные роли, социальные обычаи, социальные традиции, социальные нравы, мораль
	социальное внимание	–
Эмоциональный процесс	социальный эмоциональный процесс	социальные настроения, социальные чувства

[142] *Андреева Г. М.* Социальная психология: учебник для высших учебных заведений. 5-е изд., испр. и доп. М.: Аспект Пресс, 2005. С. 139.

[143] *Андреева Г. М.* Социальная психология: учебник для высших учебных заведений. 5-е изд., испр. и доп. М.: Аспект Пресс, 2005.; *Аронсон Э., Уилсон Т., Эйкерт Р.* Социальная психология. Психологические законы поведения человека в социуме. СПб.: Прайм-ЕВРОЗНАК, 2005; *Клецина И. С.* Гендерные группы как субъекты гендерных отношений // Социальная психология: Хрестоматия / Сост. Е. П. Белинская, О. А. Тихомандрицкая. М.: Аспект-Пресс, 2008. С. 209; Массовое сознание и поведение. Тенденции социально-психологических исследований / А. Л. Журавлев, В. А. Соснин, Д. А. Китова, Т. А. Нестик, А. В. Юревич. М.: Изд-во «Институт психологии РАН», 2017; *Стефаненко Т. Г.* Этнопсихология. М.: Институт психологии РАН, Академический проект, 1999. *Агеев В. С.* Межличностное взаимодействие: Социально-психологические проблемы. М.: Издательство МГУ, 1990; *Соломина И. Ю.* Социальная память: структура и феномены: автореф. дис. … канд. философ. наук. Самара, 2005.

Группа психических процессов	Психический процесс	Психические образования
Когнитивные процессы	социальное восприятие	социальная идентичность, социальные стереотипы, социальные установки, социальные ожидания
	социальное познание (мышление)	социальные суждения, социальные представления, менталитет, социальный (национальный) характер, общественное мнение
	социальная память	социальная информация
Групповые бессознательные структуры (коллективное бессознательное)		
Регулятивно-волевые процессы	социальные мотивация и воля	неосознаваемые социальные установки и ценностно-личностные ориентации, социальные инстинкты
Эмоциональный процесс	социальный эмоциональный процесс	социальные аффекты, психический настрой
Когнитивные процессы	социальная память	архетипы коллективного бессознательного

Подводя итог проведенному анализу, следует выделить три основные группы объектов ИПБ (деструктивного информационно-психологического воздействия):

1) личность, большие и малые социальные группы, общество в целом;

2) психика человека, включающая сознание и бессознательное, и групповые психические структуры, состоящие из группового (общественного) сознания и коллективного бессознательного;

3) индивидуальные и групповые психические процессы и образования сознательного и бессознательного характера.

В качестве основы для дефиниции ИПБ полагаем целесообразным использовать первый уровень объектов деструктивного информационно-психологического воздействия.

В заключение, перед тем как сформулировать определение понятия ИПБ, обратимся к вопросу о содержании лежащей в его основе базовой категории «безопасность». В большинстве документов стратегического планирования[144] и законов в сфере безопасности[145] понятие «безо-

[144] Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 2 июля 2021 г. № 400); Военная доктрина Российской Федерации (утв. Президентом Российской Федерации 25 декабря 2014 г. № Пр-2976), Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

[145] Федеральный закон от 21 декабря 1994 г. № 69-ФЗ «О пожарной безопасности»; Федеральный закон от 10 декабря 1995 г. № 196-ФЗ «О безопасности дорожного движения»; Федеральный закон от 21 июля 1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов»; Федеральный закон от 9 января 1996 г. № 3-ФЗ «О радиационной безопасности населения»; Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»; Федеральный закон от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности»; Федеральный закон от 26 июня 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

пасность» определяется как состояние защищенности определенных объектов или интересов от угроз. Такой подход разделяется большинством российских исследователей проблем национальной[146] и информационной[147] безопасности.

Американский военный словарь закрепляет схожее определение безопасности как состояния неприкосновенности (*англ.* state of inviolability) от вредоносного воздействия, обеспечиваемого за счет реализации комплекса защитных мер.[148]

Проведенный нами анализ критических подходов к трактовке безопасности, представленных в научной литературе,[149] позволил прийти к выводу об оптимальности использования конструкции «состояние защищенности» в качестве основы дефиниции базовой категории «безопасности»

---

[146] Безопасность // Война и мир в терминах и определениях / Под общ. ред. Д. О. Рогозина. М.: ПоРог, 2004. С. 20; Безопасность // Безопасность Евразии-2002: энциклопедический словарь-ежегодник / Авт. идеи и концепции, рук. проекта В. Н. Кузнецов. М.: Книга и Бизнес, 2003. С. 236; *Глебов И. Н.* Национальная безопасность Российской Федерации: проблемы правового регулирования: монография. СПб.: Санкт-Петербургский университет МВД России, 1999. С. 27; *Буркин А. И., Возжеников А. В., Синеок Н. В.* Национальная безопасность России в контексте современных политических процессов. 2-е изд., доп. / Под общ. ред. А. В. Возженикова. М.: Изд-во РАГС, 2008. С. 40; *Опалев А. В.* О системе и содержании базовых категорий теории обеспечения национальной безопасности // Национальная безопасность: научное и государственное управленческое содержание: материалы Всеросс. науч. конф., 4 дек. 2009 г., Москва (текст + электронный ресурс) / Центр пробл. анал. и гос.-упр. проект. М.: Научный эксперт, 2010. С. 187.

[147] *Лопатин В. Н.* Информационная безопасность России: дис. … д-ра юрид. наук. СПб., 2000. С. 13; *Филин С. А.* Информационная безопасность: учебное пособие. М.: Альфа-Пресс, 2006. С. 7; *Борисов М. А., Романов О. А.* Основы организационно-правовой защиты информации. М.: Книжный дом «Либроком», 2012. С. 18–19; Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / Под ред. А. И. Петренко. 2-е изд., стереотип. М.: Горячая линия–Телеком, 2011. С. 25–30; Термины и определения в области информационной безопасности. М.: Издательство АС-Траст, 2009. С. 93.

[148] Security // Department of Defense Dictionary of Military and Associated Terms. As of December 2020 // Joint Chiefs of Staff. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (дата обращения: 01.02.2021).

[149] *Иващенко Г. В.* О понятии «безопасность» // Credo. 2000. Вып. 6 (№ 24). URL: http://credonew.ru/content/view/207/25/ (дата обращения: 24.10.2012); *Белов П. Г.* Методологические основы национальной безопасности России. Ч. 1: Базовые категории, методы исследования и обеспечения. СПб.: СПбГПУ, 2004; Национальная безопасность Российской Федерации: проблемы укрепления государственно-правовых основ // Журнал российского права. 2005. № 2; *Вишняков В. Г.* О методологических основах правового регулирования проблем безопасности Российской Федерации // Журнал российского права. 2005. № 9; *Голунов Н. М.* Национальная безопасность России: учеб. пособие. Новосибирск: СибАГС, 2006; *Бельков О. А.* О языке теории и политики национальной безопасности России и *Сулакшин С. С.* Категория «безопасность»: от категориального смысла до государственного управления в сборнике: Национальная безопасность: научное и государственное управленческое содержание: материалы Всеросс. науч. конф., 4 дек. 2009 г., Москва (текст + электронный ресурс). Центр пробл. анал. и гос.-упр. проект. М.: Научный эксперт, 2010.

и отдельных ее видов.[150] При этом само понятие «состояние защищенности» трактуется нами как «совокупность внутренних и внешних условий, предотвращающих или минимизирующих негативное воздействие угроз на объекты безопасности и обеспечивающих тем самым возможность существования последних, сохранения их качественной определенности, выполнения ими своих функций и дальнейшего развития».[151]

На основе вышеизложенного мы определяем *информационно-психологическую безопасность как составную часть системы информационной безопасности, представляющую собой состояние защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.*

§ 3. Содержание и правовая природа деструктивного информационно-психологического воздействия

В условиях активного развития информационного общества и процессов цифровой трансформации повышается значимость изучения правовых проблем защиты российского общества от деструктивного информационно-психологического воздействия.

Как было показано выше, категория деструктивного информационно-психологического воздействия является базовым понятием для обозначения широкого спектра угроз ИПБ. Поэтому научный анализ содержания и правовой природы деструктивного информационно-психологического воздействия является важным этапом правового исследования ИПБ.

Понятие *информационно-психологического воздействия* (ИПВ) охватывает весьма обширный круг явлений, связанных с оказанием психологического влияния на индивида и социум: от попыток воздействия в межличностном общении до широкомасштабных пропагандистских кампаний в политике, бизнесе или профилактической медицине.[152]

В психологии – базовой научной дисциплине, изучающей ИПВ, – чаще употребляется термин «психологическое воздействие»,[153] без приставки «информационно-». В нашей работе мы будем использовать данные понятия как синонимы, хотя при желании между ними можно выявить

---

[150] *Смирнов А. А.* Критический анализ ревизионистских подходов к определению понятия «безопасность» // Административное право и процесс. 2015. № 5. С. 16–20.

[151] Там же. С. 19.

[152] *Латынов В. В.* Психологическое воздействие: принципы, механизмы, теории // Психологическое воздействие: Механизмы, стратегии, возможности противодействия / Под ред. А. Л. Журавлева, Н. Д. Павловой. М.: Изд-во «Институт психологии РАН», 2012. С. 11.

[153] Психологическое воздействие: Механизмы, стратегии, возможности противодействия / Под ред. А. Л. Журавлева, Н. Д. Павловой. М.: Изд-во «Институт психологии РАН», 2012; Психологическое воздействие в межличностной и массовой коммуникации / Под ред. А. Л. Журавлева, Н. Д. Павловой. М.: Изд-во «Институт психологии РАН», 2014.

некоторые отличия. Как отмечает В. В. Латынов, «всепроникающий характер психологического воздействия способствует активному изучению этого явления не только в психологии, но и в ряде других гуманитарных научных дисциплин: социологии, политологии, теории коммуникации, конфликтологии, антропологии, культурологии, лингвистике».[154] Это еще раз убеждает нас в безальтернативности междисциплинарного подхода к исследованию ИПБ.

Вот несколько дефиниций психологического воздействия:

а) «такое воздействие индивидуального или группового субъекта В, которое вызывает или предотвращает изменение психологических характеристик и проявлений индивида-реципиента А, в том числе относящихся к его деятельности (и поведению в целом), к его сознанию (и бессознательной сфере психики), к его личности»[155];

б) «способ оказания влияния на людей (на отдельных индивидов и на группы), осуществляемого с целью изменения идеологических и психологических структур их сознания и подсознания, трансформации эмоциональных состояний, стимулирования определенных типов поведения с использованием различных способов явного и скрытого психологического принуждения»[156];

в) «поведение человека или группы лиц, которое имеет целью (или следствием) изменения поведения, когнитивной и эмоциональной сфер другого человека (группы людей)».[157]

В общей и социальной психологии долгое время доминировал бихевиористский подход к изучению ИПВ. *Бихевиоризм* (от *англ.* behaviour – поведение) представляет собой направление в психологии, сводящее психику к различным формам поведения, понятого как совокупность реакций организма на стимулы внешней среды.[158] Единицей анализа поведения бихевиористами была объявлена конкретная связь стимула (S) и вызываемой им реакции (R).[159]

---

[154] *Латынов В. В.* Психологическое воздействие: принципы, механизмы, теории // Психологическое воздействие: Механизмы, стратегии, возможности противодействия / Под ред. А. Л. Журавлева, Н. Д. Павловой. М.: Изд-во «Институт психологии РАН», 2012. С. 11.

[155] *Балл Г. А., Бургин М. С.* Анализ психологических воздействий и его педагогическое значение // Вопросы психологии. 1994. № 4. С. 56–66.

[156] *Манойло А. В.* Государственная информационная политика в особых условиях: монография. М.: МИФИ, 2003. С. 97.

[157] *Латынов В. В.* Психологическое воздействие: принципы, механизмы, теории // Психологическое воздействие: Механизмы, стратегии, возможности противодействия / Под ред. А. Л. Журавлева, Н. Д. Павловой. М.: Изд-во «Институт психологии РАН», 2012. С. 12.

[158] Бихевиоризм // Психология. Словарь / Под общ. ред. А. В. Петровского, М. Г. Ярошевского. 2-е изд., испр. и доп. М.: Политиздат, 1990. С. 42–43.

[159] Бихевиоризм // Большой психологический словарь / Сост. и общ. ред. Б. Г. Мещеряков, В. П. Зинченко. 4-е изд., расширенное. М.: АСТ; СПб.: Прайм-ЕВРОЗНАК, 2009. С. 68–69.

Соответственно, ИПВ определяется в этой схеме как направленное воздействие определенных стимулов, вызывающих комплекс когнитивных, эмоциональных и поведенческих реакций индивида или социальной группы. В контексте изучения ИПБ нас будут интересовать виды ИПВ, имеющие деструктивный характер. Основным критерием деструктивности выступает общественная опасность вызываемых ими последствий, т. е. способность причинять вред или создавать угрозу его причинения.[160]

Поскольку наше исследование носит юридический характер, для четкого определения предмета правового регулирования требуется установление границ содержания ИПВ и отграничение его от других типов воздействия.

Начнем с того, что в документах стратегического планирования для обозначения деструктивного воздействия на психику человека и общественное сознание употребляется как термин «информационно-психологическое воздействие» (пп. 4 п. 25 Стратегии НБ 2021, п. 12 и пп. «д» п. 21 Доктрины ИБ 2016, п. 26 Стратегии противодействия экстремизму в Российской Федерации до 2025 года[161]), так и «информационное воздействие» (пп. 11 п. 57 Стратегии НБ 2021, п. 12, 14, пп. «к» п. 23 Доктрины ИБ 2016). В указанных случаях данные термины используются как синонимы. Однако в целом понятие информационного воздействия намного шире по своему содержанию, поскольку включает и информационно-техническое воздействие (далее – ИТВ), в частности на объекты критической инфраструктуры (пп. 3 п. 57 Стратегии НБ 2021, пп. «в» п. 23 Доктрины ИБ 2016). Понять, о каком виде воздействия идет речь, можно не только в случае точного его определения (ИПВ/ИТВ), но и по указанному объекту информационного воздействия.

В контексте исследуемой проблемы термин «информационно-психологическое воздействие» мы считаем наиболее точным и информативным, поскольку в нем, по меткому выражению Г. В. Грачева, «акцентируется целевая функция информации как специфического средства воздействия на психику человека».[162] Основное содержание ИПВ состоит *в воздействии определенных сведений на человека*. Такое понимание проистекает из определения информации как «сведений (сообщений, данных) независимо от формы их представления» в нормативном источнике (п. 1 ст. 2 Закона об информации) или как «сведений, передаваемых людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т. д.)»

[160] *Сотсков Ф. Н.* Общественная опасность деяния в уголовном праве России: автореф. дис. … канд. юрид. наук. М., 2009. С. 10–11.

[161] Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Указом Президента РФ от 29 мая 2020 г. № 344) // СЗ РФ. 2020. № 22. Ст. 3475.

[162] *Грачев Г. В.* Информационно-психологическая безопасность личности: теория и технология психологической защиты: дис. … д-ра психол. наук. М., 2000. С. 52.

в доктринальном источнике.[163] Термин «сведения» акцентирует внимание на наличии у информации определенного значения (смысла).[164] В последнее время в качестве синонима «сведений» применительно к сфере массовых коммуникаций употребляется термин «контент».

Обозначенный подход считается общепризнанным: «Большинство авторов отмечают, что информационно-психологическое воздействие, то есть воздействие словом, информацией в целях формирования определенных идеологических (социальных) идей, взглядов, представлений, убеждений, является основным видом психологического воздействия».[165] Соответственно, *базовый блок ИПБ связан с защитой от воздействия негативных сведений (информации, контента)*.

Подобное понимание разделяется многими видными исследователями информационной безопасности. Так, Т. А. Полякова и В. Н. Лопатин выделяют в качестве компонента информационной безопасности защиту человека и общества от воздействия «вредной информации»,[166] П. Г. Андреев – от «вредоносной и недостоверной информации»,[167] ученые из РАГС – от «нежелательной информации».[168] А. А. Тамодлин также рассматривает информационную безопасность личности через призму защиты от негативного воздействия на человека информации (сведений).[169] К. Д. Рыдченко определяет ИПБ как «состояние защищенности индивидуальной психики и общественного сознания от осуществляемого при обороте вредоносной информации негативного психологического воздействия».[170] Все указанные исследователи видят источник деструктивного воздействия на человека и социум в негативной (вредоносной) информации. Данная информация может передаваться человеку устным способом

---

[163] Информация // Большая энциклопедия Кирилла и Мефодия, 2004: Мультимедиа-издание.

[164] Как пишет А. Н. Баранов, «термином сведения называется такая информация, которая понята и усвоена, введена в модель мира конкретного человека – носителя языка». См.: *Баранов А. Н.* Лингвистическая экспертиза текста: теоретические основания и практика: учеб пособие. 7-е изд., стер. М.: ФЛИНТА, 2020. С. 25.

[165] *Баранов Е. Г.* Информационно-психологическое воздействие: сущность и психологическое содержание // Национальный психологический журнал. 2017. № 1 (25). С. 27.

[166] *Полякова Т. А.* Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … д-ра юрид. наук. М., 2008. С. 331; *Лопатин В. Н.* Информационная безопасность России: дис. … д-ра юрид. наук. СПб., 2000. С. 14.

[167] *Андреев П. Г.* Институциональное развитие правового обеспечения информационной безопасности в российском информационном праве: автореф. дис. … канд. юрид. наук. Екатеринбург, 2012. С. 23.

[168] Массмедиа в условиях глобализации: Информационно-коммуникационная безопасность: монография / Под общ. ред. В. И. Василенко. М.: Проспект, 2015. С. 82.

[169] *Тамодлин А. А.* Государственно-правовой механизм обеспечения информационной безопасности личности: дис. … канд. юрид. наук. Саратов: 2006. С. 6–7.

[170] *Рыдченко К. Д.* Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации: автореф. дис. … канд. юрид. наук. Воронеж, 2011. С. 10.

в ходе прямого контакта (устная коммуникация), а также опосредованно через иные каналы коммуникации (письмо, телефон, СМИ, Интернет и др.).

Однако распространение негативной информации не исчерпывает всего содержания деструктивного ИПВ. Второй его базовой формой выступает *деструктивная коммуникация* – непосредственное или опосредованное техническими средствами общение между индивидами или группой лиц, оказывающее негативное влияние.

Грань между контентной и коммуникационной формами деструктивного ИПВ весьма тонкая, поскольку коммуникация между людьми также связана с передачей информации и последующим воздействием ее на человека. В этом смысле коммуникационные угрозы также носят информационный характер, а распространение сведений является формой коммуникации. Основным критерием их дифференциации является наличие прямого или опосредованного техническими средствами контакта между людьми – во второй группе такой контакт наличествует, в первой – отсутствует. Поэтому коммуникационные угрозы преимущественно связаны с межличностным или групповым общением, а контентные – с массовой коммуникацией.

При этом основу обоих форм деструктивного ИПВ составляет речевой (вербальный) дискурс, но оно включает в себя и невербальную коммуникацию – «совокупность неречевых коммуникативных средств – систему жестов, знаков, символов, кодов, использующихся для передачи сообщения с большей точностью и играющих важнейшую роль в смысловом понимании людьми друг друга».[171] При этом невербальные сообщения могут не только дополнять или изменять влияние речевого сообщения, но и нести собственный смысл.

Негативные проявления устной коммуникации (оскорбление, запугивание, принуждение и др.) издревле рассматривались в качестве угроз. Вместе с тем особую опасность формы негативной коммуникации приобрели именно в настоящее время в условиях широкого проникновения мобильной связи, социальных сетей и мессенджеров. Новые технические средства коммуникации сделали возможными свободное общение между малознакомыми людьми, которые к тому же имеют возможность скрывать или искажать свою личность. Как подчеркивает М. Е. Позднякова, «особенности общения подростков в анонимно-виртуальной среде обусловливают деформации социализации в нормативном аспекте и содержат опасности приобщения к девиантным формам поведения как в виртуальной, так и в реальной среде».[172] Данный вывод справедлив не только для подростков.

---

[171] *Андрианов М. С.* Невербальная коммуникация: психология и право. М.: Институт Общегуманитарных Исследований, 2007. С. 12.

[172] *Позднякова М. Е.* Влияние интернет-сообществ на распространение девиантных форм поведения в современной России (на примере наркотизма) // Россия реформирующаяся. Ежегодник / Отв. ред. М. К. Горшков. Вып. 8. М.: Институт социологии РАН, 2009. С. 136.

Описанные тенденции повлекли бурный рост коммуникационных угроз ИПБ в последние два десятилетия. Среди них наиболее актуальными можно назвать: вербовку в террористические и экстремистские организации, вовлечение в совершение преступлений, подстрекательство к аутодеструктивному поведению, обман в целях завладения имуществом (мошенничество). Отдельно стоит упомянуть такие формы речевой агрессии, как троллинг, флейминг и буллинг,[173] получившие очень широкое распространение в онлайн-среде, особенно в социальных сетях.

В исследовании EU Kids online выделены следующие коммуникационные риски (*англ.* contact risk) для детей: а) коммерческие – отслеживание и сбор персональных данных; б) агрессивные – запугивание, приставание (травля) или преследование; в) сексуальные – получение нежелательных сексуальных комментариев, приставание с сексуальными целями, встреча с незнакомцами; г) ценностные – аутодеструктивное поведение, нежелательное общение.[174]

Отметим еще один важный момент. Интернету свойственно наличие особой коммуникативной среды для зарождения и проявления интернет-угроз рассматриваемой нами группы – *деструктивных виртуальных сообществ*, формирующихся на базе социальных сетей, специализированных сайтов и интернет-чатов. Сетевым сообществам присущи признаки агеографичности (пользователи находятся в разных местах), анонимности (трудно установить истинную личность пользователя), кластерности (сообщества являются замкнутыми образованиями для посвященных).[175] К основным видам деструктивных виртуальных сообществ можно отнести следующие сообщества: хакеров,[176] наркоманов,[177] самоубийц,[178]

[173] *Щербинина Ю. В.* Речевая агрессия. Территория вражды: учебное пособие. М.: ФОРУМ, 2013; *Воронцова Т. А.* Троллинг и флейминг: речевая агрессия в интернет-коммуникации // Вестник Удмуртского университета. 2016. Т. 26. Вып. 2. С. 109–116; *Ксенофонтова И. В.* Специфика коммуникации в условиях анонимности: меметика, имиджборды, троллинг // Интернет и фольклор: сборник статей. М.: Государственный республиканский центр русского фольклора, 2009. С. 285–293.

[174] *Hasebrink, U., Livingstone, S., Haddon, L.* (2008) Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. London: EU Kids Online. P. 28.

[175] *Куликов Д. В.* Социальное пространство компьютерно-опосредованной реальности: опыт феноменологической реконструкции: автореф. дис. … канд. философ. наук. Иваново, 2007. С. 8.

[176] *Мурсалиева Г.* Группы смерти // Новая газета. 2016. 16 мая; *Масленченко С. В.* Субкультура хакеров как порождение информатизации общества: автореф. дис. … канд. культурологии. СПб., 2008; *Дремлюга Р. И.* Интернет-преступность: монография. Владивосток: Изд-во Дальневосточн. ун-та, 2008. С. 166–184.

[177] *Позднякова М. Е.* Влияние интернет-сообществ на распространение девиантных форм поведения в современной России (на примере наркотизма) // Россия реформирующаяся. Ежегодник / Отв. ред. М. К. Горшков. Вып. 8. М.: Институт социологии РАН, 2009. С. 129–149.

[178] *Костюковский Я.* Девиантогенные эффекты Интернета // Девиантность в обществе потребления: коллективная монография / Под ред. Я. И. Гилинского и Т. В. Шипуновой. СПб.: Издательский дом «Алеф-Пресс», 2012. С. 265–294.

педофилов,[179] подстрекателей к самоубийствам,[180] колумбайнеров.[181] Большинство этих деструктивных сообществ имеют типовую иерархическую структуру, включающую «идеологов», «кураторов» и «начинающих».[182]

В современных условиях в качестве источника деструктивного ИПВ должен рассматриваться не только человек, но и искусственный интеллект (далее – ИИ). Национальная стратегия развития искусственного интеллекта на период до 2030 года[183] определяет *искусственный интеллект* как «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» (п. 5).

Предметное поле ИИ очень широкое и находится в фокусе исследований многих наук, включая юриспруденцию.[184] Преломляя данную проблематику через призму проблем ИПБ, в первую очередь выделим направление голосовых помощников, имеющих функцию понимания и синтеза речи.[185] К этой же группе мы отнесем чат-ботов, которые реагируют на письменную речь (текст). Все они получили широкое развитие и постоянно совершенствуются. Продвинутые голосовые помощники уже сейчас способны поддерживать длительный диалог с человеком. В этой связи голосовые помощники и чат-боты становятся потенциальным источником коммуникационных угроз ИПБ, в том числе обмана и манипуляции сознанием. На существующем этапе они скорее могут выполнять роль посредника

---

[179] Насилие над детьми. Доклад Всемирной неправительственной организации ECPAT (2006) // Криминальное насилие против женщин и детей: международные стандарты противодействия: сб. документов / Сост. В. С. Овчинский. М.: Норма, 2008. С. 728–804.

[180] *Амелина Я. А.* «Группы смерти» как угроза национальной безопасности России. Аналитический доклад / Кавказский геополитический клуб. М.: Издатель А. В. Воробьёв, 2017; *Архипова А., Волкова М., Кирзюк А., Малая Е., Радченко Д., Югай Е.* «Группы смерти»: от игры к моральной панике. М.: РАНХиГС, 2017.

[181] *Амелина Я. А.* Бенефис ненависти. Как «колумбайнеры» и керченский убийца Владислав Росляков стали «героями» российской деструктивной молодежи (18+) / Кавказский геополитический клуб. М.: Издатель А. В. Воробьёв, 2019.

[182] *Белоусов А. В.* Угрозы сети Интернет для несовершеннолетних пользователей: психологический анализ и профилактика: монография. М.: Проспект, 2021. С. 55–61.

[183] Национальная стратегия развития искусственного интеллекта на период до 2030 года (утв. Указом Президента РФ от 10 октября 2019 г. № 490) // СЗ РФ. 2019. № 41. Ст. 5700.

[184] Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и роботехники: монография / Под общ. ред. к. ю. н. В. Б. Наумова. СПб.: НП-Принт, 2020.

[185] Интересно отметить, что в советском издании 1976 г. отмечалось, что «переход к взаимодействию в режиме реального времени, в режиме диалога на языке, близком к естественному, объективно создает предпосылки для развертывания собственно психологических исследований деятельности человека в режиме взаимодействия с ЭВМ». См.: «Искусственный интеллект» и психология / Отв. ред. О. К. Тихомиров. Институт психологии Академии наук СССР. М.: Наука, 1976. С. 26.

в реализации планов человека-злоумышленника, однако в дальнейшем будут способны самостоятельно воздействовать на человека.

Еще одним аспектом влияния ИИ на ИПБ выступает угроза создания продвинутых подделок фото- и видеоизображений человека, а также его голоса – так называемых «глубоких фейков» (*англ.* deepfakes), открывающих беспрецедентные возможности для манипулирования общественным сознанием.[186] Также ученые говорят о генерации ИИ фейковых текстов.[187]

Характеризуя деструктивное ИПВ, нельзя обойти вниманием вопрос *негативных неосознаваемых влияний*. В. В. Лопатин еще в 2000 г. отмечал потребность в разработке национального законодательства и норм международного права, направленных на защиту психики от неосознаваемых деструктивных информационных воздействий.[188] Действующее российское законодательство содержит такие нормы. Так, Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»[189] в ст. 4 устанавливает запрет на «использование в радио-, теле-, видео-, кинопрограммах, документальных и художественных фильмах, а также в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок и иных технических приемов и способов распространения информации, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье», а Кодекс Российской Федерации об административных правонарушениях[190] в ст. 13.15 устанавливает административную ответственность за нарушение данного запрета. Федеральный закон от 13 марта 2006 г. № 38-ФЗ «О рекламе»[191] запрещает использование и распространение в информационной продукции «скрытой рекламы, оказывающей не осознаваемое потребителями рекламы воздействие на их сознание, в том числе такое воздействие путем использования специальных видеовставок (двойной звукозаписи) и иными способами» (ч. 9 ст. 5). Аналогичные нормы имеются и в международных актах. В частности, в Европейской конвенции о трансграничном телевидении от 5 мая 1989 г.[192] установлен запрет на использование технологий воздействия на подсознание (subliminal techniques) в рекламе (ч. 2 ст. 13).

---

[186] *Смирнов А. А.* «Глубокие фейки». Сущность и оценка потенциального влияния на национальную безопасность // Свободная мысль. 2019. № 5. С. 63–84; *Chesney, R., Citron, D.* Deepfakes and the New Disinformation War. The Coming Age of Post-Truth Geopolitics // Foreign Affairs. January/February 2019. P. 147–155.

[187] Имитация интеллекта. «Цифровая магия» и ее разоблачение // Завтра. 2021. 5 ноября. URL: https://zavtra.ru/blogs/imitatciya_intellekta (дата обращения: 12.12.2021).

[188] *Лопатин В. Н.* Информационная безопасность России: дис. …д-ра юрид. наук. СПб., 2000. С. 258.

[189] Российская газета. 1992. 8 февр.

[190] СЗ РФ. 2002. № 1. Ст. 1.

[191] СЗ РФ. 2006. № 12. Ст. 1232.

[192] European Convention on Transfrontier Television. Strasbourg, 5.V.1989 (amended according to the provisions of the Protocol ETS No. 171) // Council of Europe. URL: http://conventions.coe.int/Treaty/EN/Treaties/Html/132.htm (дата обращения: 12.02.2021).

В психологии описанный тип воздействия именуется *подпороговым* или *сублиминальным (англ. subliminal influence)*. Его механизм основывается на неосознанном восприятии психикой стимулов, не достигающих порога чувствительности.[193] В отечественном словаре такое восприятие названо *субсенсорным* и определено как «форма непосредственного психического отражения действительности, обуславливаемая такими раздражителями, о влиянии которых на его деятельность субъект не может давать себе отчета».[194] Такое восприятие относится к проявлениям бессознательного.

Существуют разные оценки возможностей воздействия на подсознание человека. Однако большинство ученых сходятся во мнении, что «не существует эмпирической документации в отношении значительных подпороговых эффектов, таких как вызов конкретных поведенческих реакций или изменение мотивации».[195] В то же время В. В. Латынов, проанализировавший большое количество западных экспериментальных исследований, пишет о способности неосознаваемых стимулов эффективно воздействовать на мнения и оценки людей, влиять на их эмоциональное состояние и принимаемые решения.[196] Об этом же свидетельствуют иные источники.[197]

Таким образом, исследования психологов подтверждают возможность скрытого сублиминального ИПВ на человека, однако говорят о его ограниченном потенциале. Необходимо также принимать во внимание, что академические психологи исследуют общедоступные способы подпорогового воздействия, тогда как «в недрах» специальных служб могут иметься особые инструменты и методы такого влияния, о чем косвенно свидетельствует обширная литература по данной теме.[198] Поэтому *подпороговое (сублиминальное) воздействие будет включено нами в содержание деструктивного ИПВ, а защита от него – рассматриваться как направление обеспечения ИПБ*.

---

[193] Подпороговое восприятие // Энциклопедия Кругосвет. URL: http://krugosvet.ru/enc/gumanitarnye_nauki/psihologiya_i_pedagogika/PODPOROGOVOE_VOSPRIYATIE.html (дата обращения: 15.12.2021).

[194] Субсенсорное восприятие // Психология. Словарь / Под общ. ред. А. В. Петровского, М. Г. Ярошевского. 2-е изд., испр. и доп. М.: Политиздат, 1990. С. 388–389.

[195] *Пратканис Э. Р.* Подпороговое воздействие (subliminal influence) // Психологическая энциклопедия. 2-е изд. / Под ред. Р. Корсини, А. Ауэрбаха. СПб.: Питер, 2006.

[196] *Латынов В. В.* Подпороговое воздействие на психику человека: возможности и ограничения // Психологическое воздействие: Механизмы, стратегии, возможности противодействия / Под ред. А. Л. Журавлева, Н. Д. Павловой. М.: Изд-во «Институт психологии РАН», 2012. С. 11.

[197] *Шиффман Х. Р.* Ощущение и восприятие. СПб.: Питер, 2003. С. 73–76; *Karremans, J.C., Stroebe, W.&. Claus, J.* Beyond Vicary's fantasies: The impact of subliminal priming and brand choice // Journal of Experimental Social Psychology. 2006. 42. P. 792–798.

[198] См: *Прокофьев В. Ф.* Тайное оружие информационной войны: атака на подсознание. 2 изд., расширенное и доработанное. М.: СИНТЕГ, 2003; *Пугачев В. П.* Управление свободой. М.: КомКнига, 2005; *Перцефф Д.* Атака на мозг. Оскал психотронной войны. СПб.: Вектор В-Н, 2008; *Тейлор Э.* Программирование разума. От манипуляции и промывания мозгов к расширению возможностей и внутренней свобод. М.: Гиппо, 2010.

Еще один значимый аспект. В научной литературе часто говорится о видах информационного воздействия, оказывающих влияние непосредственно на физиологию человеческого организма. В качестве таковых называются световые и звуковые воздействия, специальные воздействия электромагнитных и звуковых колебаний, в том числе в частотно-амплитудных диапазонах, не воспринимаемых человеком осознанно.[199] Такие воздействия индуцируются генераторами специального излучения. Военный эксперт В. Ф. Прокофьев называет их психофизическим оружием.[200] В ст. 6 Федерального закона от 13 декабря 1996 г. № 150-ФЗ «Об оружии»[201] закреплен правовой запрет на оборот на территории РФ «оружия и иных предметов, поражающее действие которых основано на использовании электромагнитного, светового, теплового, инфразвукового или ультразвукового излучения…».[202]

В качестве реально существующего примера такого оружия можно привести американскую военную установку «система активного отбрасывания» (*англ.* Active Denial System, ADS), которая излучает электромагнитные колебания в диапазоне миллиметровых волн и оказывает кратковременное шоковое воздействие на людей.[203] Также следует упомянуть случаи так называемых «акустических атак», которым подверглись более 40 сотрудников посольства США в Кубе в период 2016–2017 гг.[204] Данные случаи стали предметом специального исследования Американской академии наук. Его авторы пришли к выводу о том, что необычные проявления симптомов у сотрудников Госдепартамента вызваны «воздействием направленного импульсного высокочастотного радиоизлучения».[205]

---

[199] *Смолян Г. Л., Зараковский Г. М., Розин В. М., Войскунский А. Е.* Информационно-психологическая безопасность (определение и анализ предметной области). М.: Институт системного анализа РАН, 1997. С. 9.

[200] *Прокофьев В. Ф.* К проблеме формирования основных понятий в области информационной безопасности // Военная безопасность Российской Федерации в XXI веке: сб. научных статей / Под ред. генерала армии Ю. Н. Балуевского. М.: ЦВСИ, 2005. С. 244.

[201] СЗ РФ. 1996. № 51. Ст. 5681.

[202] В конце 1990-х гг., по свидетельству Е. К. Волчинской, была предпринята попытка разработки концепции законопроекта «Об обеспечении энергоинформационного благополучия населения», однако она не увенчалась успехом. См.: *Волчинская Е. К.* О законотворческой деятельности в сфере обеспечения информационно-психологической безопасности // Информационная и психологическая безопасность в СМИ. В 2 т. Т. II: Феномен «разорванной коммуникации»: сб. статей / Под ред. Я. Н. Засурского, Ю. П. Зинченко, Л. В. Матвеевой, Е. Л. Вартановой, А. И. Подольского и др. М.: Аспект Пресс, 2008. С. 124–125.

[203] *Клюев Е.* EMW – электромагнитное оружие: воздействие на биологические объекты // Сверхновая реальность. 2007. № 3. С. 66–72.

[204] *Белянинов К.* Акустическая атака. Названы причины загадочного заболевания американских дипломатов // BBC News. Русская служба. 7 декабря 2020 г. URL: https://www.bbc.com/russian/features-55161883 (дата обращения: 15.04.2021).

[205] National Academies of Sciences, Engineering, and Medicine. 2020. An assessment of illness in U.S. government employees and their families at overseas embassies. Washington, DC: The National Academies Press, 2020. P. 2.

Возникает вопрос – можно ли отнести описанные выше типы воздействия к информационно-психологическим? Полагаем, что лишь отчасти, поскольку в противном случае происходит неоправданное расширение предметной области ИПБ. Автор разделяет точку зрения Г. В. Грачева о том, что понятие ИПВ «позволяет выделить из всего спектра разновидностей психологического воздействия определенную совокупность и тем самым сузить предмет исследования, не рассматривая, например, психофизическое или так называемое энергоинформационное воздействие и некоторые другие».[206]

Изучив соответствующую литературу в области психологии, мы выбрали два критерия, позволяющие отграничить ИПВ от других типов воздействия – сенсорный (тип используемого сенсорного канала восприятия информации) и объектный (объект информационного воздействия).

Исходя из первого критерия, автор пришел к заключению, что к ИПВ относятся дистантные воздействия на зрительный и слуховой сенсорные каналы, тогда как контактные воздействия на человека через тактильный или вкусовой каналы выходят за рамки содержания ИПВ. Последнее также относится и к воздействию на вестибулярные и кинестетические каналы. Отметим, что из данного правила могут быть исключения. Так, в ходе обсуждения указанного тезиса на конференции в Республике Беларусь в 2012 г. внимание автора было обращено на случаи лиц, страдающих нарушением работы зрительного аппарата (слепых или слабовидящих), использующих тактильные ощущения для восприятия информации (шрифт Брайля).

Однако критерия типа сенсорной системы недостаточно для определения четких границ понятия ИПВ, что видно на примере боевого лазера, использующего одновременно зрительный и тактильный каналы восприятия. Поэтому в дополнение к первому считаем необходимым применить также *критерий объекта воздействия*. В соответствии с ним к ИПВ могут быть отнесены только те типы воздействия на человека, которые влияют на его психику, а не на соматические (телесные) элементы. К ним могут относиться оптические, электромагнитные и акустические сигналы[207] (звуки определенной частоты, мерцание экрана, комбинация цветовых пятен и т. п.). Впрочем, данный вывод во многом утрачивает значение в системах виртуальной реальности, в которых оказывается комплексное воздействие на человека в отношении разных сенсорных систем.

Обобщая сказанное, мы обосновываем вывод о том, что *деструктивное информационно-психологическое воздействие включает в себя негативное влияние на личность и социальные группы деструктивного контента или коммуникации, а также сигналов от технических устройств,*

[206] *Грачев Г. В.* Информационно-психологическая безопасность личности: теория и технология психологической защиты: дис. … д-ра психол. наук. М., 2000. С. 52.

[207] Понятие «сигнал» в контексте нашего рассмотрения означает материально-энергетическую форму представления информации, не несущей семантической нагрузки (смысла).

дистанционно воздействующих на психику человека через зрительные и слуховые сенсорные системы, создающее опасность причинения вреда интересам личности, общества и государства.

Далее кратко рассмотрим вопрос о правовой природе деструктивного ИПВ. Проведенный автором анализ действующих документов стратегического планирования и законодательства РФ позволил заключить, что *деструктивное ИПВ в российском праве может идентифицироваться в качестве*: а) угрозы безопасности; б) формы злоупотребления правом на информацию и свободой массовой информации; в) правонарушения (преступления, административного правонарушения, гражданско-правового деликта); г) вида соучастия в совершении преступления (организации, подстрекательства, интеллектуального пособничества); д) обстоятельства, исключающего преступность деяния (психического принуждения); е) смягчающего обстоятельства (совершение преступления в результате психического принуждения, аморальность поведения потерпевшего, явившегося поводом для преступления); ж) основания для признания недействительности сделки (совершение сделки под влиянием существенного заблуждения); з) основания для применения мер государственного принуждения, включая блокировку информационного ресурса.

Это далеко не полный перечень. Однако из его анализа четко просматривается межотраслевая правовая природа проблематики деструктивного ИПВ, проявляющего себя в различных правовых понятиях и институтах в уголовном, административном, гражданском и иных отраслях российского права.

§ 4. Характеристика и правовое закрепление угроз информационно-психологической безопасности

Определяющей предпосылкой построения системы обеспечения ИПБ выступает изучение комплекса существующих и потенциальных угроз в данной области. Как справедливо отмечают авторы научного труда по национальной безопасности России, «характер и уровень угроз определяют основные направления деятельности по их предупреждению и локализации, формы, способы, средства и методы решения задач обеспечения национальной безопасности при рациональном использовании имеющихся ограниченных ресурсов».[208]

В российских документах стратегического планирования в области национальной безопасности используется понятие «*угроза безопасности*». В Стратегии НБ 2021 данное понятие определяется как «совокупность условий и факторов, создающих прямую или косвенную возможность причинения ущерба национальным интересам» (пп. 5 п. 5). В схожем ключе

[208] *Буркин А. И., Возженников А. В., Синеок Н. В.* Национальная безопасность России в контексте современных политических процессов. 2-е изд., доп. / Под общ. ред. А. В. Возженникова. М.: Изд-во РАГС, 2008. С. 51.

в научной литературе трактуется понятие «угроза информационной безопасности»: «фактор или совокупность факторов, создающих опасность функционированию и развитию информационной сферы».[209]

Нас интересует группа информационно-психологических угроз, связанных с оказанием деструктивного ИПВ на человека и социальные группы. Концептуальные рамки последнего понятия мы оговорили в предыдущем параграфе.

С учетом вышеизложенного *угрозу информационно-психологической безопасности* можно определить как фактор или совокупность факторов, способных причинить вред интересам личности, общества и государства посредством оказания деструктивного информационно-психологического воздействия.

Угрозы ИПБ обладают следующими характерными чертами.

1. Латентный (неочевидный) характер начала действия угрозы и трудность ее обнаружения. В отличие от традиционного оружия, факт применения которого достаточно просто зафиксировать (обнаружение звука выстрела, пуска ракеты и т. п.), угрозы ИПБ часто носят неочевидный («невидимый») характер и сложно выявляются.

2. Сложность идентификации. Многие виды деструктивного ИПВ легко маскируются под обычное психологическое влияние либо применяются в совокупности с ним, в силу чего определить их достаточно сложно. Поэтому даже в случае обнаружения факта применения ИПВ часто требуется использование специальных методов идентификации угроз ИПБ (например, экспертизы), чтобы доказать их деструктивный характер.

3. Варьируемый масштаб последствий. Посредством выбора вида ИПВ и канала его трансляции можно в значительной мере изменять территориальный масштаб и объектовый охват воздействия. При этом важно отметить, что некоторые типы ИПВ способны влиять на население целых стран и регионов мира.

4. «Гуманность» воздействия. В отличие от традиционного оружия многие средства и методы ИПВ не наносят прямого и быстро ощутимого вреда человеку (хотя имеются примеры «быстродействующих» методов ИПВ, например применение психологического обмана для завладения денежными средствами) и позволяют достигать целей субъекта воздействия более гуманным способом, снижая человеческие страдания. Однако в более длительной перспективе подобная «гуманность» оказывается во многом мнимой, поскольку деструктивное ИПВ способно детерминировать акты агрессии, рост числа суицидов, социальные

[209] *Приходько А. Я.* Словарь-справочник по информационной безопасности. М.: СИНТЕГ, 2001. С. 64; Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / Под ред. А. И. Петренко. 2-е изд., стереотип. М.: Горячая линия – Телеком, 2011. С. 434; *Комов С. А., Ракитин В. В., Родинов С. Н. и др.* Термины и определения в области информационной безопасности. М.: Издательство АС-Траст, 2009. С. 255.

и даже межгосударственные конфликты и другие общественно опасные последствия.

5. Сложный механизм воздействия. Он состоит в сложном многоступенчатом характере ИПВ на человека и социальные группы, обусловленном в первую очередь особенностями человеческой психики и общественного сознания. Поэтому, в отличие от военных средств поражения, спрогнозировать точный эффект влияния угроз ИПБ зачастую весьма затруднительно.

6. Сопротивляемость объекта воздействию угроз означает наличие у человека и социальных групп «встроенных» механизмов психологической защиты, а также возможность обучения техникам устойчивости внешнему ИПВ. Следствием данного признака выступает значимость укрепления внутренних защитных «фильтров» человека как направления обеспечения ИПБ.

7. Прямая зависимость эффекта воздействия от осведомленности объекта проявляется в возможности значительного снижения, вплоть до блокирования, негативного ИПВ при осведомленности человека/социальной группы о потенциальной опасности и методах такого воздействия. Этим угрозы ИПБ отличаются от некоторых иных типов угроз (военных, экологических и др.), информированность о которых далеко не всегда позволяет снизить вредоносный эффект их влияния.

8. Влияние на другие сферы обеспечения безопасности и государственное управление в целом. Посредством оказания ИПВ на должностных лиц органов власти можно влиять на принятие решений в иных сферах обеспечения безопасности и, шире, государственном управлении (например, решения о развитии определенных систем вооружения, проведении экономических реформ, вступлении в конфликт и даже «решения судного дня» – нанесения ракетно-ядерного удара по противнику). Данная характерная черта является уникальной для рассматриваемого вида безопасности и не имеет аналогов в системе национальной безопасности.

В наиболее общем виде в качестве угроз ИПБ следует рассматривать совокупность всех видов деструктивного ИПВ на человека и социальные группы. В зависимости от их характеристик можно выделить различные виды угроз ИПБ. В целях получения четкого и структурированного видения системы таких угроз автор разработал их собственную типологизацию. Это очень важно в контексте избранного нами целостного ракурса научного исследования, поскольку в науке чаще уделяется внимание анализу отдельных видов угроз ИПБ.

На первом этапе построения типологизации автор в первую очередь провел системный анализ закрепления угроз ИПБ в базовых документах стратегического планирования в области национальной безопасности. Помимо базовых актов – Стратегии НБ 2021 и Доктрины ИБ 2016, мы включим в перечень правовых источников нашего изучения другие

документы стратегического планирования в сферах государственной, общественной, военной, международной безопасности. Полученная матрица угроз ИПБ представлена в приложении 3. Как видно из таблицы, в действующих документах стратегического планирования в области безопасности закреплен широкий спектр угроз ИПБ в политической, социальной, культурной и международной сферах. Также угрозы ИПБ четко просматриваются в рамках государственной, общественной и военной безопасности.

На основе составленной матрицы основных угроз ИПБ, отраженных в документах стратегического планирования, а также с учетом результатов собственных научных изысканий представим авторскую классификацию основных угроз ИПБ.

Типологизация угроз ИПБ

I. В зависимости от природы происхождения:

1) *антропогенные* – виды негативного ИПВ, оказываемого непосредственно человеком или группой людей вербальными и невербальными методами, в том числе с использованием опосредующих контакт технических средств (распространение негативного контента, вредоносная коммуникация и т. д.);

2) *техногенные* – виды негативного ИПВ, оказываемого техникой или иными искусственными объектами без участия человека (определенные типы излучения, голосовые помощники и т. д.).

II. В зависимости от типа ИПВ:

1) *контентные* – угрозы ИПБ, связанные с воздействием негативной информации (контента), получаемой человеком в отсутствие прямой коммуникации между людьми (порнография, изображение насилия или жесткости, материалы, пропагандирующие терроризм, и т. д.);

2) *коммуникационные* – угрозы ИПБ, связанные с негативным межличностным или групповым общением (обман, манипуляция сознанием, подстрекательство к самоубийству и т. д.);

3) *технические* – угрозы ИПБ, связанные с негативным ИПВ на человека сигналов от технических устройств (направленное электромагнитное излучение, звуки определенной частоты и т. д.).

III. В зависимости от степени сформированности:

1) *потенциальные* – угрозы ИПБ, которые находятся на стадии зарождения или формирования (например, манипуляция сознанием со стороны голосовых помощников);

2) *реальные* – угрозы ИПБ, которые уже получили распространение (например, сексуальные домогательства детей в Интернете).

IV. В зависимости от местонахождения источника угрозы:

1) *внутренние* – угрозы ИПБ, источник которых расположен внутри страны (например, распространение экстремистских листовок в населенных пунктах страны);

2) *внешние* – угрозы ИПБ, источник которых находится за рубежом (например, трансляция передачи зарубежным телеканалом);

3) *гибридные (смешанные)* – угрозы ИПБ, имеющие несколько источников, расположенных как внутри страны, так и за ее пределами (например, распространение дискредитирующих главу государства сведений одновременно в мировых и отечественных СМИ).

V. В зависимости от длительности воздействия:

1) *краткосрочные* – формы ИПВ, носящие кратковременный характер и вызывающие определенные когнитивные, эмоциональные и поведенческие реакции человека и социальных групп (например, манипуляция сознанием в ходе оформления кредита в банке);

2) *длительные (лонгитюдные)* – длительные формы ИПВ, преследующие цель поэтапного изменения элементов психики человека, общественного сознания или коллективного бессознательного (например, воздействие деструктивных молодежных субкультур).

VI. В зависимости от пространственного масштаба воздействия:

1) *точечные* – виды негативного ИПВ, пределы влияния которых ограничены конкретным местом (квартира, служебный кабинет и т. п.);

2) *локальные* – виды негативного ИПВ, распространяющегося в пределах ограниченных территориальных зон (населенного пункта, субъекта Федерации и т. п.);

3) *национальные* – виды негативного ИПВ, воздействующие на все население страны в пределах национальных границ;

4) *глобальные* – виды негативного ИПВ, воздействующие на определенные иностранные государства или мировое сообщество.

VII. В зависимости от избирательности воздействия:

1) *неизбирательного воздействия* – виды ИПВ, влияние которых носит массовый неизбирательный (сплошной) характер (сюда относятся прежде всего виды ИПВ, осуществляемые через крупные СМИ и интернет-ресурсы);

2) *относительно избирательного воздействия* – виды ИПВ, оказывающие преимущественное влияние на определенные индивидуальные и групповые объекты, но способные воздействовать и на другие объекты (например, материалы агитационного характера в ходе местных выборов либо проповеди представителя одной из нетрадиционных конфессий);

3) *избирательного воздействия* – виды ИПВ, влияние которых жестко ограничено конкретным индивидуальным или групповым объектом (например, обман конкретного человека в ходе межличностной коммуникации либо воздействие на членов закрытой тоталитарной секты).

В настоящем параграфе мы рассмотрим наиболее распространенные и многочисленные угрозы ИПБ, связанные с негативным влиянием определенной информации (сведений) на личность и общество и вредоносной социальной коммуникацией. В изложенной авторской классификации

видов угроз ИПБ мы обозначили их, соответственно, как контентные и коммуникационные. Рассмотрим их последовательно.

Группа *контентных угроз* охватывает виды информации, имеющей негативный (вредный, опасный) характер.[210] Их идентификация может быть осуществлена посредством применения двух основных методов: аналитического и сущностного.[211]

Аналитический метод требует проведения анализа норм международного права, отечественного и зарубежного законодательства, закрепляющего виды негативной информации. Для этой цели используется инструментарий сравнительно-правовых исследований. При отсутствии в национальном законодательстве определенного вида негативного контента его правовой режим может быть регламентирован на основе международных стандартов или зарубежного опыта при учете внутренней специфики.

Сущностный метод означает выявление и обоснование признаков вредоносности (опасности) сведений,[212] по которым затем выстраивается перечень такого контента. Доказывание общественной опасности сведений может осуществляться на основе научного анализа и реальных последствий влияния таких сведений на личность или социальную группу. По результатам проведенной оценки определяется оптимальный правовой режим для оборота определенного контента, например его полный запрет или введение частичных ограничений.

Полагаем целесообразным применение обоих указанных методов для решения задач правовой идентификации негативного контента. Апробируем их в нашем исследовании и начнем с аналитического метода.

В международно-правовых актах содержится большое количество видов негативной информации, для которых установлены запрет их оборота или правовые ограничения. Кратко изложим результаты проведенного нами анализа релевантных норм международных актов в табличной форме (приложение 4).

---

[210] Отметим, что в январе 2022 г. Президент РФ поручил своей Администрации «рассмотреть представленные президентом акционерного общества «Крибрум» Ашмановым И. С. предложения по реализации проекта создания саморегулируемого реестра токсичного контента в информационно-телекоммуникационной сети Интернет в целях защиты несовершеннолетних и при необходимости принять соответствующие меры поддержки». Полагаем, что изложенные в настоящем параграфе выводы и предложения могут быть использованы для ее решения. См.: Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека // Президент Российской Федерации. 27 января 2022 г. URL: http://kremlin.ru/acts/assignments/orders/67660 (дата обращения: 27.01.2022).

[211] *Смирнов А. А.* Негативный контент: проблемы идентификации в контексте правового регулирования // Информационное право. 2015. № 2. С. 19–21.

[212] В определенном смысле сущностный метод выявления контентных угроз можно сравнить с проактивным принципом работы антивирусных программ, отличающимся от традиционного сигнатурного тем, что вирус обнаруживается не путем сравнения его с эталонным перечнем, а посредством описания и детекции признаков вредоносности.

Гораздо более обширный перечень видов негативной информации закреплен в законодательстве зарубежных стран. Однако базовый набор таких видов преимущественно остается унифицированным в силу имплементации положений рассмотренных выше международных договоров и иных источников международного права.

Важно отметить, что в западных странах применяется подход разграничения негативной информации на две основные категории с различным правовым режимом оборота. Первую категорию составляет *незаконный контент (illegal content)*, оборот которого находится под запретом и квалифицируется как правонарушение (чаще всего как преступление).[213] Вторая категория представлена *вредным контентом (harmful*[214] *content),* под которым понимаются общественно опасные сведения, которые не запрещены законом к обороту. Для таких сведений устанавливаются отдельные ограничения на их производство и распространение.

Однако идентификации контента в качестве незаконного или вредного является суверенным правом государства, которое самостоятельно принимает решение с учетом конституционно закрепленных принципов и ценностей, культурных и исторических традиций.[215] В качестве иллюстрации изложим обобщенные результаты исследования относительно видов запрещенной информации в 56 государствах – членах ОБСЕ[216] (таблица 3).

Таблица 3

Запрещенная информация в зарубежных странах

Действуют ли в пределах вашей юрисдикции конкретные правовые нормы, запрещающие следующий вид контента?			
Вид контента	**Варианты ответов (указано число стран и их процентная доля)**		
	Да	**Нет**	**Ответ не поступил**
Расистский контент, ксенофобия и ксенофобские высказывания	45 (80,4%)	1 страна (Кыргызстан)	10 (17,9%)
Отрицание, умаление, одобрение или оправдание геноцида или преступлений, совершенных против человечества	23 (41,1%)	23 (41,1%)	10 (17,9%)
Подстрекательство к терроризму, пропаганда терроризма и/или использование Интернета в террористических целях	40 (71,4%)	6 (10,7%)	10 (17,9%)
Детская порнография	43 (76,8%)	3 (5,4%)	10 (17,9%)

[213] Данный подход применяется Международной ассоциацией «горячих интернет-линий» INHOPE, которая занимается реагированием на криминальный контент. См.: Illegal content // INHOPE. URL: http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/illegal-content.aspx (дата обращения: 26.09.2019).

[214] Словарь ABBYY Lingvo переводит прилагательное «harmful» как «вредный, пагубный, губительный; тлетворный».

[215] Свобода выражения мнения в Интернете. Отчет представителя по вопросам СМИ ОБСЕ Д. Миятовича. ОБСЕ, 2011. С. 6, 13.

[216] Там же.

Вид контента	Варианты ответов (указано число стран и их процентная доля)		
	Да	Нет	Ответ не поступил
Непристойный или носящий явно сексуальный характер (порнографический) контент	41 (73,2%)	5 (8,9%)	10 (17,9%)
Клевета и оскорбление (диффамация)	36 (64,3%)	8 (14,3%)	10 (17,9%)
Выражение взглядов, предположительно призывающих к экстремизму	20 (35,7%)	26 (46,4%)	10 (17,9%)
«Вредный» контент	19 (33,9%)	26 (46,5%)	11 (19,6%)
Любые иные формы интернет-контента	15 (26,8%)	30 (53,6%)	11 (19,6%)

В аналитическом докладе «Фильтрация контента в Интернете. Анализ мировой практики» 2013 г.[217] представлена более обширная информация по видам негативного контента. В докладе выделены несколько основных групп такого контента, подвергаемого фильтрации: 1) политический контент (информация и ресурсы о деятельности оппозиционных движений, правозащитных организаций, сайты запрещенных религиозных движений и сект, сведения об этнических меньшинствах или критика власти); 2) информация, нарушающая социальные нормы (порнографические сайты, ресурсы тематики ЛГБТ и сексуального просвещения, сайты о наркотиках и алкоголе, онлайн-казино, ресурсы, разжигающие социальную или религиозную ненависть и вражду, распространяющие клевету и др.); 3) контент, блокируемый по соображениям безопасности (сайты экстремистских и террористических организаций, сепаратистских движений, ресурсы военных противников, ресурсы с информацией ограниченного доступа, сайты онлайн-мошенников, спам).[218]

Проведенный автором анализ научной литературы[219] показывает, что учеными выделяются схожие виды негативного контента. При этом они делают акцент на некоторых из них в рамках фокуса научного исследования.

Завершим наше исследование правовых подходов к определению негативного контента анализом российского законодательства. При

[217] Фильтрация контента в Интернете. Анализ мировой практики. Аналитический доклад. Фонд развития гражданского общества, 2013. С. 1.

[218] Там же. С. 11–16.

[219] *Лопатин В. Н.* Информационная безопасность России: дис. … д-ра юрид. наук. СПб., 2000; *Брайант Дж., Томпсон С.* Основы воздействия СМИ. Пер. с англ. М.: Издательский дом Вильямс, 2004; *Кобзева С. В.* Сравнительно-правовой анализ регулирования оборота вредной информации в телерадиовещании и кинопрокате // Информационное право. 2010. № 2. С. 8–13; Информационная безопасность детей: российский и зарубежный опыт: монография / Ефимова Л. Л., Кочерга С. А. М.: ЮНИТИ-ДАНА, 2013; *Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson K.* Comparing children's online opportunities and risks across Europe. Cross-national comparisons for EU Kids Online. LSE, London: EU Kids Online, 2009.

этом будем отталкиваться от отправной нормы, закрепленной в Законе об информации: «Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность» (ч. 7 ст. 10). На основе анализа статей Особенных частей УК РФ и КоАП РФ составим обобщенный перечень информации, распространение которой в России запрещено[220] (приложение 5).

Проведенный анализ показывает, что в российском уголовном и административно-деликтном законодательстве содержится достаточно широкий перечень запрещенного негативного контента, адекватно отражающий международно-правовые стандарты и зарубежный опыт и учитывающий национальную специфику. Данный перечень постоянно дополняется по мере проявления вредоносных свойств новых видов контента.

Помимо запрещенного контента, в РФ в интересах защиты детей и иных категорий граждан реализован подход выделения иного вредного контента. Его оборот полностью не запрещен, однако на него устанавливаются определенные ограничения по критериям возраста, времени и каналов демонстрации. Такие ограничения установлены законами о СМИ и о защите детей от информации.

Подводя итог вышеизложенному, выделим *основные контентные угрозы ИПБ:*

1) информация, пропагандирующая либо оправдывающая войну и иные международные преступления, терроризм;

2) информация, разжигающая ненависть и вражду в социуме;

3) информация, связанная с фальсификацией истории или осквернением исторической памяти;

4) информация, стимулирующая или содействующая совершению преступлений или иных общественно опасных действий;

5) ложная или искаженная информация;

6) информация, унижающая (порочащая) честь, достоинство или репутацию лица либо оскорбляющая общественную нравственность;

7) порнографический и иной сексуально откровенный контент;

8) информация устрашающего характера.

Каждая из названных угроз имеет специфический механизм деструктивного ИПВ на человека и социальные группы. Наиболее изученным является механизм влияния медианасилия.[221] В последнее время резко

[220] При составлении таблицы использованы действующие редакции УК РФ и КоАП РФ по состоянию на 12 декабря 2021 г.

[221] *Ениколопов С. Н.* Средства массовой коммуникации и насилие // Проблемы медиапсихологии / Сост.: канд. психол. наук Пронина Е. Е. М.: РИП-холдинг, 2002. С. 77–78; *Брайант Дж., Томпсон С.* Основы воздействия СМИ. Пер. с англ. М.: Издательский дом Вильямс, 2004. С. 199; National Television Violence Study. Executive

актуализировалась проблема ложной информации (фейков),[222] хотя она имеет давнюю историю.

Выше мы говорили о сущностном методе. На основе изученных перечней выделим *основные критерии вредоносности контента*:

1) способность вводить в заблуждение;

2) способность провоцировать на совершение противоправных или социально опасных действий, в том числе аутодеструктивного плана;

3) способность вызывать страх, оказывать иное негативное воздействие на психологическое состояние личности и причинять вред психическому здоровью;

4) способность порочить честь, достоинство и деловую репутацию;

5) способность оказывать негативное воздействие на индивидуальную и общественную нравственность, иные элементы ценностно-нормативной системы;

6) способность искажать или оскорблять историческую память.

Группа коммуникационных угроз охватывает негативное ИПВ в ходе контакта между людьми. В отличие от предыдущей группы, для которой основным источником угроз являются массмедиа, коммуникационные угрозы исходят из межличностной и групповой коммуникации. Она может включать в себя непосредственные формы «живого общения» (разговор, участие в концерте, демонстрации) либо опосредованные применением технических средств (разговор по телефону, переписка в интернет-чате, общение в режиме видеозвонка или видеоконференции и т. п.). Большинство коммуникационных угроз имеют вербальный характер, однако существуют и невербальные их формы. При этом мы исходим из того, что «функцию воздействия реализует любое высказывание, к какой бы сфере коммуникативной практики оно ни относилось».[223] Предложенные нами методы исследования контентных угроз вполне применимы и для рассматриваемой группы.

Правовая регламентация коммуникационных угроз ИПБ может осуществляться двумя основными способами: 1) посредством определения

Summary, 1998. URL: http://www.academia.edu/944389/National_Television_Violence_Study_Executive_Summary_Editor_University_of_California_Santa_Barbara_ (дата обращения: 17.02.2021).

[222] *Кошкин П. Г.* Американская журналистика и постправда. М.: Издательство «Весь Мир», 2018; *Бон А., Пандерс В.* Фейк. Все, что надо знать о пропаганде, фальшивых новостях и теориях заговора. М.: Манн, Иванов и Фербер, 2020; *Совик Ю. И.* Ограничение распространения недостоверной общественно значимой информации: опыт европейских государств // Конституционное и муниципальное право. 2020. № 8. С. 72–80; *Ильяшенко А. Н., Хисамова З. И.* О некоторых аспектах привлечения к уголовной ответственности за распространение fake news в социальных сетях в условиях пандемии // Российский следователь. 2020. № 9. С. 12–15.

[223] *Павлова Н. Д.* Механизмы и средства оказания субъектом дискурсивного воздействия // Психологическое воздействие: Механизмы, стратегии, возможности противодействия / Под ред. А. Л. Журавлева, Н. Д. Павловой. М.: Изд-во «Институт психологии РАН», 2012. С. 53–54.

вида негативного ИПВ, который может осуществляться как через распространение контента, так и через общение; 2) посредством определения конкретного типа деструктивной коммуникации.

В рассмотренных выше международно-правовых актах в основном используется первый способ (это относится к выступлениям в пользу национальной, расовой или религиозной ненависти, мотивированной угрозе расизма и ксенофобии, публичному подстрекательству к совершению террористического преступления, клеветническим утверждениям и др.). Вместе с тем встречаются юридически закрепленные формы деструктивной коммуникации: а) приставание к детям с сексуальными целями (ст. 23 Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений от 25 октября 2007 г.); б) вербовка террористов (ст. 6 Конвенции Совета Европы о предупреждении терроризма от 16 мая 2005 г.); в) мотивированная угроза расизма и ксенофобии (ст. 4 Дополнительного протокола к Конвенции о киберпреступности в отношении криминализации деяний расистского и ксенофобского характера, совершаемых при помощи компьютерных систем, от 28 января 2003 г.) и т. д.

Проведенный нами анализ норм Особенных частей УК РФ и КоАП РФ позволил построить матрицу запрещенных видов коммуникации (приложение 5). Многие позиции в ней совпадают с видами противоправного контента, однако имеются и уникальные проявления коммуникационных угроз.

В большом массиве проанализированной нами литературы выделяются следующие виды коммуникационных угроз: а) обман;[224] б) дезинформация;[225] в) манипуляция сознанием;[226] г) программирование психики;[227] д) запугивание (угрозы);[228] е) шантаж;[229] ж) подстрекательство

---

[224] *Экман П.* Психология лжи. СПб.: Питер, 2001.

[225] *Волкогонов Д. А.* Психологическая война: Подрывные действия империализма в области общественного сознания. М.: Воениздат, 1984; *Почепцов Г.* (Дез)информация. Киев: ПАЛИВОДА А.В., 2019.

[226] *Доценко Е. Л.* Психология манипуляции: феномены, механизмы и защита. СПб.: Речь, 2003; *Грачев Г. В., Мельник И. К.* Манипулирование личностью. М.: Эксмо, 2003; *Кара-Мурза С. Г.* Манипуляция сознанием: учебное пособие. М.: Алгоритм, 2004; *Зелинский С. А.* Манипуляции массами и психоанализ. Манипулирование массовыми психическими процессами посредством психоаналитических методик. СПб.: СКИФИЯ, 2008; *Шейнов В. П.* Психология манипулирования. Мн.: Харвест, 2009; *Шипова А. Н.* Манипулирование сознанием и его специфика в современном обществе: дис. … канд. философ. наук. Ставрополь, 2007; *Гостев А. А.* Глобальная психоманипуляция: психологические и духовно-нравственные аспекты. М.: Изд-во «Институт психологии РАН», 2017.

[227] *Коледа С.* Моделирование бессознательного. М.: Институт общегуманитарных исследований, 2000; *Пугачев В. П.* Управление свободой. М.: Комкнига, 2005.

[228] Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / Под ред. А. И. Петренко. 2-е изд, стереотип. М.: Горячая линия – Телеком, 2011.

[229] *Манойло А. В., Петренко А. И., Фролов Д. Б.* Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия – Телеком, 2009.

к совершению преступлений[230]; з) сексуальные домогательства и «киберпреследования».[231] Особую группы составляют формы террористической коммуникации, включая вербовку, радикализацию, вовлечение, инструктирование.[232]

Подводя итог проведенному анализу, к *основным коммуникационным угрозам ИПБ* автор относит:

1) обман (дезинформацию);

2) манипуляцию сознанием;

3) коммуникацию, разжигающую ненависть или вражду;

4) публичные призывы и иные формы подстрекательства к совершению противоправных и иных общественно опасных действий;

5) вербовку и иные формы вовлечения в совершение противоправных и иных общественно опасных действий;

6) оскорбление и иные формы унижения человеческого достоинства;

7) запугивание и принуждение;

8) негативную сексуальную коммуникацию;

9) коммуникацию, связанную с фальсификацией истории или оскорблением исторической памяти.

Критерии вредоносности коммуникативных угроз ИПБ полностью совпадают с выделенными критериями для контентных угроз. Однако, учитывая наличие угроз запугивания и принуждения, мы выделим еще один критерий – способность заставлять лицо или социальную группу действовать вопреки своей воле.

При выработке стратегии противодействия контентным и коммуникационным угрозам ИПБ, в том числе при подборе надлежащего правового инструментария для реагирования, требуется их определенное ранжирование. В основе этой процедуры лежит простая и очевидная мысль о том, что степень опасности угроз ИПБ различается, причем довольно существенно.

---

[230] *Абакаров З. А.* Ответственность за подстрекательство к совершению преступления по российскому уголовному праву: автореф. дис. … канд. юрид. наук. Саратов, 2006.

[231] *Войскунский А. Е.* Информационная безопасность: психологические аспекты // Национальный психологический журнал. 2010. № 1. С. 49.

[232] *Гарев В. А.* Информационные угрозы современного международного терроризма. М.: Институт Африки РАН, 2010; *Вейман Г.* Как современные террористы используют Интернет. Специальный доклад № 116 // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/analytics/Tropina_01/ (дата обращения: 12.04.2013); *Горбатова В. В.* Информационно-пропагандистская политика радикальных исламских организаций (на примере Хамас, «Хизбаллы» и «Аль-Каиды»): автореф. дис. … канд. полит. наук. М., 2013; Использование Интернета в террористических целях. Управление Организации Объединенных Наций по наркотикам и преступности, 2013; *Сундиев И. Ю., Смирнов А. А.* Использование информационных сетей в экстремистской и террористической деятельности // Научный портал МВД России. 2014. № 1. С. 84–91; *Арифханова С. Н.* Деструктивные способы воздействия на молодежную аудиторию в сети интернет: монография. Warsaw: RS Global Sp. Z O. O., 2021.

В правовой науке наиболее полно разработан механизм оценки общественной опасности преступлений, которая определяется как «внутреннее свойство деяния, выраженное в объективной способности деятельности человека причинить или создать угрозу причинения вреда».[233] Характер и степень общественной опасности деяния выступают в качестве базовых критериев для криминализации деяния и установления санкции за правонарушение в нормативном акте,[234] назначения наказания за его совершение конкретному лицу.[235]

В информационном праве оценка общественной опасности угроз ИПБ также используется как в нормотворческой, так и в правоприменительной практике. Однако в отличие от уголовного и административно-деликтного права, где предметом оценки выступает опасность деяния, связанного с распространением определенной информации или ведением коммуникации, для информационного права таковым преимущественно является сам контент/коммуникация, вне привязки к конкретному лицу. Хотя оценка его влияния и включает реконструкцию некоторых характеристик автора, таких как цель создания, коммуникативное намерение и т. п.

Наиболее сложным является вопрос о критериях оценки опасности (вредоносности). В уголовном праве, как отмечает Ю. Е. Пудовочкин, «существует широкая зона согласия относительно того, чем определяется опасность преступления, от чего она зависит».[236] В качестве таковых со ссылкой на Н. Д. Дурманова ученый называет: «объект посягательства, причиняемый ему ущерб, степень вероятности наступления этого ущерба и его размеры, пространственно-временные условия и обстановку осуществления посягательства, способ совершения преступления… мотивы и цели действий преступника, признаки субъекта преступления».[237] Схожая позиция отражена в позиции Пленума Верховного Суда РФ, который разграничил критерии характера и степени общественной опасности.[238]

---

[233] *Сотсков Ф. Н.* Общественная опасность деяния в уголовном праве России: автореф. дис. … канд. юрид. наук. М., 2009. С. 10.

[234] *Густова Э. В.* Криминализация и пенализация деяний как формы реализации уголовной политики // Вестник Воронежского института МВД России. 2014. № 1. С. 224–227; *Кузнецов А. П.* Криминализация – декриминализация, пенализация – депенализация как содержание уголовной политики // Вестник Краснодарского университета МВД России. С. 16–18.

[235] Постановление Пленума Верховного Суда РФ от 22 декабря 2015 г. № 58 «О практике назначения судами Российской Федерации уголовного наказания» // Российская газета. 2015. 29 декабря.

[236] *Пудовочкин Ю. Е.* Понятие, критерии и пределы учета общественной опасности преступления судом // Уголовная политика и правоприменительная практика. Сборник материалов VII Международной научно-практической конференции (1–2 ноября 2019 г.). СПб.: Центр научно-информационных технологий «Астерион», 2019. С. 62–63.

[237] Там же. С. 62.

[238] Постановление Пленума Верховного Суда РФ от 22 декабря 2015 г. № 58 «О практике назначения судами Российской Федерации уголовного наказания».

Своя методология оценки угроз существует в области национальной и информационной безопасности.[239] Анализ национальных стандартов в области менеджмента рисков[240] показывает, что оценка риска строится на основе двух базовых факторов – *последствий риска* и *вероятности их наступления*. Они оцениваются на стадии анализа риска, которая предполагает качественный и количественный анализ либо их комбинацию. В научной статье по оценке рисков информационной безопасности на предприятиях в алгоритм такой оценки включена стадия «определения ценности актива».[241] *Ценность актива (охраняемого объекта)* можно считать третьим фактором для оценки риска.

Попробуем применить эту концепцию к сфере ИПБ. Критерий «последствия риска» будет означать негативные последствия для личности, общества или государства, наступающие вследствие оказания ИПВ. Они могут иметь личный (формирование страхов, принятие ошибочного решения), экономический (утрата имущества, упущенная выгода), социальный (возрастание уровня агрессии в обществе, провоцирование массовых беспорядков) и иной характер.

Вероятность наступления последствий определяется, во-первых, вероятностью столкновения с угрозой ИПБ, во-вторых, вероятностью ее вредоносного воздействия на личность/группу. Первый аспект вполне просчитывается, например, на основе изучения показателей медиапотребления, анализа статистики работы горячих интернет-линий и линий помощи. Со вторым все обстоит гораздо сложнее в силу описанных нами особенностей механизма ИПВ. Поэтому для их оценки применимы методы экспертных оценок и изучения конкретных случаев (case study).

Что касается ценности объектов ИПБ, то определить ее весьма сложно, поскольку речь идет не о материальных объектах, а о людях. Тем не менее имеется консенсус относительно признания детей приоритетным объектом правовой защиты.

Такие критерии должны быть положены в основу методологии оценки и ранжирования угроз ИПБ при выборе государственной стратегии противодействия им и правовом регулировании данной сферы отношений. В практике же оперативного управления в первую очередь следует ориентироваться на наиболее подвижные критерии – частоту проявления угроз и количество зарегистрированных случаев наступления негативных последствий.

---

[239] Общая теория национальной безопасности: учебник / Под общ. ред. А. А. Прохожева. 2-е изд., доп. М.: Издательство РАГС, 2005. С. 263–290.

[240] ГОСТ Р 51897–2011. Менеджмент риска. Термины и определения. М.: Стандартинформ, 2012; ГОСТ Р 58771–2019. Менеджмент риска. Технологии оценки риска. М.: Стандартинформ, 2020; ГОСТ Р ИСО 31000–2019. Менеджмент риска. Принципы и руководство. М.: Стандартинформ, 2020.

[241] *Плетнев П. В., Белов В. М.* Методика оценки рисков информационной безопасности // Доклады ТУСУРа. 2012. № 1. Часть 2. С. 85.

Отметим еще один важный момент. Конкретная разновидность угроз ИПБ, обозначаемая соответствующим лингвистическим маркером («ложные сведения», «устрашающая информация» и т. п.), может включать в себя широкий спектр проявлений, отличающихся по степени опасности. Поясним это на примере контента, содержащего сцены насилия. Во-первых, опасность будет зависеть от характера самого изображения (описания) насилия, а именно: степени натуралистичности, уровня жестокости, субъекта и объекта насилия, длительности показа (описания); во-вторых, от сюжетного контекста: характера насильника (герой/злодей/жертва), оправданности насилия, последствий для персонажа и жертвы, оценок со стороны иных участников.

В известном американском исследовании телевизионного насилия[242] были выделены следующие виды деструктивных последствий влияния образов насилия на зрителей: научение насилию, привыкание к насилию и усиление страха подвергнуться насилию в реальной жизни. В качестве «контекстуальных особенностей», влияющих на последствия показа насилия, ученые выделили: а) привлекательность насильника; б) привлекательность жертвы; в) оправданность насилия; г) вид используемого орудия; д) частоту, длительность и план показа; е) реалистичность; ж) поощрение или наказание; з) показ страданий и последствий насилия; и) юмор. При этом они описали корреляционные зависимости между этими факторами и негативными последствиями. Так, научению насилию способствует его изображение оправданным, безнаказанным или совершенным привлекательным персонажем, десенсибилизации – частый или длительный показ насилия либо демонстрация его в юмористическом контексте, запугиванию – показ неоправданного или реалистичного насилия либо насилия, направленного на привлекательную жертву или остающегося безнаказанным.[243]

Поэтому ИПВ определенного вида контента может значительно варьироваться в зависимости от особенностей и контекста его подачи в информационном материале. Данный вывод во многом справедлив и в отношении коммуникационных угроз ИПБ. Эти моменты требуют обязательного учета при правовом регулировании.

[242] National Television Violence Study. Executive Summary. Volume 3. 1998. http://www.academia.edu/944389/National_Television_Violence_Study_Executive_Summary_Editor_University_of_California_Santa_Barbara_ (дата обращения: 11.09.2021).

[243] Ibid.

ГЛАВА II. СИСТЕМА ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

§ 1. Характеристика системы правового обеспечения информационно-психологической безопасности

Экспоненциальное развитие информационно-коммуникационных технологий и процессов цифровой трансформации ставит задачу модернизации системы правового регулирования общественных отношений в различных сферах. Это особенно актуально применительно к новым вызовам цифровой среды, количество и опасность которых стремительно увеличиваются.

Т. А. Полякова отмечала, что с начала нового тысячелетия процесс нормативного регулирования информационной безопасности значительно активизировался, особенно в связи с принятием в 2000 г. Окинавской хартии глобального информационного общества и Доктрины информационной безопасности РФ.[244] За прошедший после этого период была проделана значительная работа, направленная на развитие правового обеспечения информационной безопасности.[245]

Этот вывод касается и сферы обеспечения информационно-психологической безопасности, где за последние двадцать лет правовое регулирование получило мощное развитие. Причем в последние годы данная сфера законодательства является одной из наиболее динамичных. Вместе с тем вносимые фрагментарные изменения в информационное и иное отраслевое законодательство зачастую вызваны текущими проблемами, лишены системности и опоры на научную основу.

Приступая к анализу системы правового обеспечения ИПБ, мы возьмем за основу предложенный А. А. Чеботаревой концептуальный подход к решению правовых проблем обеспечения информационной безопасности. Он предполагает изучение правовых средств обеспечения информационной безопасности в неразрывной связи с целями, задачами и механизмами реализации государственной политики по обеспечению информационной безопасности.[246]

---

[244] *Полякова Т. А.* Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … д-ра юрид. наук. М., 2008. С. 278.

[245] Правовое регулирование обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. Т. А. Поляковой. Саратов: Амирит, 2019. С. 24.

[246] *Чеботарева А. А.* Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: дис. … д-ра юрид. наук. М., 2017. С. 14.

Подробный анализ правовых механизмов и средств обеспечения ИПБ будет представлен ниже. Поэтому в настоящем параграфе мы определим цели, задачи и направления обеспечения ИПБ, место и роль правового регулирования отношений в данной сфере.

В начале своего рассмотрения отметим, что попытка детальной правовой регламентации базовых аспектов обеспечения ИПБ предпринималась в законопроекте об ИПБ. В частности, в нем были определены принципы обеспечения ИПБ (ст. 4), основные задачи государственной политики в области обеспечения ИПБ (ст. 6), функции государственной системы обеспечения ИПБ (ст. 7). Поэтому в настоящем параграфе мы будем удерживать его в фокусе нашего внимания и подвергнем критическому переосмыслению.

Понятие «*обеспечение безопасности*» относится к числу базовых категорий в теории безопасности. Лежащий в его основе термин «обеспечение» ориентирует на активную деятельность определенных субъектов, направленную на достижение состояния защищенности объектов безопасности. Содержанием такой деятельности выступает реализация уполномоченными субъектами «политических, правовых, военных, социально-экономических, информационных, организационных и иных мер, направленных на противодействие угрозам национальной безопасности» (пп. 4 п. 5 Стратегии НБ 2021).

В Доктрине ИБ 2016 обеспечение информационной безопасности определяется как осуществление комплекса взаимоувязанных организационных, правовых и мер по «прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления» (пп. «г» п. 2). Это определение интересно указанием способов выявления угроз (прогнозирование, обнаружение) и реагирования на них (сдерживание, предотвращение, отражение, ликвидация последствий проявления).

В Законе РФ от 5 марта 1992 г. № 2446-I «О безопасности»,[247] равно как и в пришедшем ему на смену Федеральном законе от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[248] (далее – Закон о безопасности), в обеспечении безопасности выделены два уровня: 1) государственная политика в области обеспечения безопасности; 2) деятельность по обеспечению безопасности. Такой подход поддерживается и в научной литературе.[249] Суть данного разграничения сводится к тому, что на первом уровне

[247] Российская газета. 1992, 6 мая.

[248] СЗ РФ. 2011. № 1. Ст. 2.

[249] Общая теория национальной безопасности: учебник / Под общ. ред. А. А. Прохожева. 2-е изд., доп. М.: Издательство РАГС, 2005. С. 163; Основы обеспечения безопасности России: учебное пособие / М. И. Дзлиев, А. Д. Урсул; Рос. гос. торгово-экон. ун-т, НИИ проблем безопасности и устойчивого развития. М.: Экономика, 2003. С. 21–23; Основы теории обеспечения национальной безопасности: курс лекций / В. В. Пузиков и др.; под ред. В. В. Пузикова. Минск: ГИУСТ БГУ, 2013. С. 41–43.

осуществляется стратегическое планирование обеспечения безопасности (постановка целей, задач, определение направлений, субъектов, форм и методов реализации), а на втором – непосредственная реализация системы мер обеспечения безопасности в соответствии с выработанным планом.

Исходя из сказанного, под *обеспечением ИПБ мы будем понимать деятельность государственных и общественных институтов по выработке и реализации системы правовых, организационных, информационных и иных мер, направленных на обеспечение защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.*

При этом будем отталкиваться от расширительного толкования понятия «состояние защищенности», обоснованного выше. Поэтому наряду с противодействием информационным угрозам в содержание обеспечения ИПБ включим меры по повышению устойчивости человека, социальных групп и общества к воздействию таких угроз.[250] Последнее направление имеет важное значение в силу невозможности полного экранирования социальных субъектов от негативного психологического влияния[251] и недостаточной эффективностью систем фильтрации информации.

Третий содержательный блок обеспечения ИПБ составляют меры по влиянию на саму информационную среду, в которой осуществляется деструктивное ИПВ на личность и социальные группы. Активизируя положительные факторы и нейтрализуя негативные элементы цифровой среды, можно повышать уровень защищенности объектов.[252] Представляется, что данное направление как раз укладывается в концепцию «информационной экологии», предполагающей создание определенного состояния информационной среды, безопасного для физического и психического здоровья человека, индивидуальной, групповой и общественной психологии.[253]

---

[250] Такой подход во многом соответствует выделенным Н. Н. Рыбалкиным двум стратегиям обеспечения безопасности. Защитная стратегия предполагает борьбу с конкретными угрозами, а стратегия утверждения – повышение жизнестойкости объекта воздействия. См.: *Рыбалкин Н. Н.* Философия безопасности. М.: Московский психолого-социальный институт, 2006. С. 195.

[251] Видный российский специалист по информационной безопасности А. А. Стрельцов в своей статье обоснованно отмечал, что в отношении значительного числа угроз безопасности объектов информационной сферы постановка цели их ликвидации не всегда представляется возможной. См.: *Стрельцов А. А.* Цель, структура и методы правового обеспечения информационной безопасности Российской Федерации // Научные и методологические проблемы информационной безопасности (сборник статей) / Под ред. В. П. Шерстюка. М.: МЦНМО, 2004. С. 49.

[252] *Сулакшин С. С.* Категория «безопасность»: от категориального смысла до государственного управления // Национальная безопасность: научное и государственное управленческое содержание: материалы Всеросс. науч. конф., 4 дек. 2009 г., Москва (текст + электронный ресурс). Центр пробл. анал. и гос.-упр. проект. М.: Научный эксперт, 2010. С. 15.

[253] *Степанов А. М., Бухтояров А. А., Бутенко Д. В.* Проблемы правовой политики обеспечения информационно-психологической безопасности. С. 30–35;

Таким образом, деятельность по обеспечению ИПБ включает в себя четыре основных элемента: 1) противодействие источникам угроз ИПБ; 2) исключение или уменьшение деструктивного влияния угроз на объекты ИПБ; 3) увеличение устойчивости объектов деструктивного ИПВ; 4) оказание влияния на элементы цифровой среды.

Также весьма ценной видится предложенная И. А. Самуйловой классификация основных групп мер по обеспечению ИПБ, включающая: 1) регулирование, в частности, ограничение информационных потоков; 2) организация информационных потоков (в том числе инициирование распространения определенной информации); 3) распространение способов и средств обработки и оценки информации; 4–5) формирование групповой и индивидуальной психологической защиты.[254]

Важнейшую роль в механизме обеспечения ИПБ играет *правовое обеспечение*, поскольку именно право устанавливает цели, задачи и направления такого обеспечения, а также регламентирует формы, средства и методы деятельности уполномоченных субъектов по противодействию угрозам ИПБ. Рассмотрим более подробно содержание правового обеспечения.

Авторы научной статьи определяют правовое обеспечение национальной безопасности как взаимосвязанную и упорядоченную совокупность нормативных правовых актов, которые закрепляют юридические принципы и нормы правового регулирования общественных отношений в области обеспечения национальной безопасности.[255] Такое определение, по нашему мнению, не вполне правильное. Во-первых, правовое обеспечение, как и любое обеспечение, представляет собой определенную деятельность на основе реализации системы мер. Во-вторых, неверно сводить всю систему правовых средств только к нормативным правовым актам.

Основательный анализ понятия правового обеспечения провел А. Н. Арзамаскин.[256] Ученый сопоставляет его с более разработанными в теории права категориями «правовое регулирование» и «правовое воздействие». В итоге он пришел к выводу о том, что правовое обеспечение включает в себя не только правовое регулирование, но и элементы правового воздействия. К числу последних он относит правосознание, правовую культуру, правовые принципы.[257] Мы разделяем данную точку

Телешина Н. Н. Информационная экология в России: сущность и проблемы правового обеспечения // Информационное право. 2014. № 1. С. 11–17.

[254] Информационно-психологическая и когнитивная безопасность: коллективная монография / Под ред. И. Ф. Кефели, Р. М. Юсупова. СПб.: ИД «Петрополис», 2017. С. 273.

[255] *Сексте Я. А., Ляпин И. Л.* Правовое обеспечение национальной безопасности РФ: основные направления, состояние и тенденции развития // Ленинградский юридический журнал. 2019. № 2. С. 73.

[256] *Арзамаскин А. Н.* Определение понятия «Правовое обеспечение»: постановка проблемы // Наука и школа. 2016. № 6. С. 47–51.

[257] Там же. С. 48.

зрения. Однако не поддерживаем мнение А. Н. Арзамаскина о включении в содержание правового обеспечения обеспечительных мер, включая «меры материально-технического, организационно-управленческого, кадрового, идеологического характера».[258]

В науке информационного права сформировался подход к пониманию правового обеспечения информационной безопасности прежде всего как правового регулирования. По мнению А. А. Стрельцова, правовое регулирование отношений в сфере обеспечения информационной безопасности предполагает установление определенных правовых норм, их применение и охрану от нарушения с использованием государственного принуждения.[259] А. А. Чеботарева справедливо отмечает, что правовое обеспечение информационной безопасности помимо правового регулирования отношений включает и правоприменительную деятельность.[260]

Разделяя в целом данную позицию, мы считаем, что правовое обеспечение безопасности включает в себя не только нормотворчество и правоприменение, но и иные формы реализации права.[261] А их, как известно, в теории права всего четыре: соблюдение, исполнение, использование, применение.[262] Поэтому автор считает целесообразным определение правового обеспечения ИПБ через понятие «правовых средств», лежащих в основе механизма правового регулирования.[263] С. С. Алексеев определял правовые средства как «субстанциональные, институциональные явления правовой действительности, воплощающие регулятивную силу права, его энергию».[264] А. В. Малько рассматривает правовые средства как «правовые явления, выражающиеся в инструментах (установлениях) и деяниях (технологии), с помощью которых удовлетворяются интересы субъектов права, обеспечивается достижение социальных целей».[265] Г. С. Беляева,

---

[258] Там же. С. 50.

[259] *Стрельцов А. А.* Теоретические и методологические основы правового обеспечения информационной безопасности России: дис. … д-ра юрид. наук. М., 2004. С. 90–91.

[260] *Чеботарева А. А.* Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: дис. … д-ра юрид. наук. М., 2017. С. 15.

[261] На это справедливо обратил внимание А. Н. Арзамаскин. См.: *Арзамаскин А. Н.* Определение понятия «Правовое обеспечение»: постановка проблемы // Наука и школа. 2016. № 6. С. 48.

[262] Теория государства и права: курс лекций / Под ред. Н. И. Матузова и А. В. Малько. 2-е изд., перераб. и доп. М.: Юрист, 2003. С. 453–454.

[263] Подход к определению правового обеспечения информационной безопасности через категорию правовых средств также использован авторами коллективной монографии. См.: Парадигма правового регулирования обеспечения международной информационной безопасности на примере опыта СНГ и ОДКБ: монография / И. Л. Бачило (и др.); под общ. ред. д-ра юрид. наук, доцента О. С. Макарова. Минск: Ин-т нац. безопасности Респ. Беларусь, 2016. С. 49.

[264] *Алексеев С. С.* Правовые средства: постановка проблемы, понятие, классификация // Советское государство и право. 1987. № 6. С. 14.

[265] *Малько А. В.* Правовые средства: вопросы теории и практики // Журнал российского права. 1998. № 8. С. 66–77.

характеризуя правовые средства, выступающие элементами механизма правового регулирования, указывает в их числе: нормы права, юридические факты, правоотношения, акты реализации права и правоприменительные акты.[266]

С учетом изложенного автор предлагает рассматривать *правовое обеспечение информационно-психологической безопасности как деятельность по разработке и реализации системы правовых средств, направленных на обеспечение защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.*

В науке и документах стратегического планирования в области национальной безопасности перед постановкой целей и задач обеспечения безопасности принято определять национальные интересы. В Стратегии НБ 2021 они определены как «объективно значимые потребности личности, общества и государства в безопасном и устойчивом развитии» (пп. 2 п. 5). Применительно к информационной сфере национальные интересы «определяются прежде всего той ролью, которую играет информация, информационная инфраструктура в обеспечении устойчивого развития нации в конкретных исторических условиях».[267]

Стратегия НБ 2021 закрепляет такие национальные интересы России на современном этапе, как защита конституционного строя, суверенитета, независимости, государственной и территориальной целостности России, укрепление обороны страны; поддержание гражданского мира и согласия в стране; развитие безопасного информационного пространства, защита российского общества от деструктивного ИПВ; укрепление традиционных российских духовно-нравственных ценностей, сохранение культурного и исторического наследия народа России (п. 25). Особо обращает на себя внимание, что защита от деструктивного ИПВ впервые выделена в качестве одного из национальных интересов в базовом документе стратегического планирования.

В этом плане требуется модернизация действующей Доктрины ИБ 2016 (п. 8), в которой защита от деструктивного ИПВ в перечне национальных интересов напрямую не отражена. Это, на наш взгляд, является большим недостатком. Вместе с тем отдельные сущностные элементы таких потребностей просматриваются в формулировках более общих национальных интересов, связанных с защитой основных прав и свобод в информационной сфере, обеспечения безопасности в области культуры и др.

По мнению автора, среди национальных интересов в информационно-психологической сфере, помимо базовых потребностей поддержания

---

[266] *Беляева Г. С.* К вопросу о сущности и системе правовых средств // Административное и муниципальное право. 2015. № 3. С. 310.

[267] *Стрельцов А. А.* Теоретические и методологические основы правового обеспечения информационной безопасности России: дис. … д-ра юрид. наук. М., 2004. С. 58.

психического здоровья граждан и общества, обеспечения суверенитета страны, укрепления национального согласия, политической и социальной стабильности, следует рассматривать сохранение традиционных ценностей и национальной идентичности. Данные интересы приобрели особое значение в условиях глобализации и формирования информационного общества.

С учетом проведенного анализа считаем возможным сформулировать *авторский перечень национальных интересов Российской Федерации в информационной сфере, касающихся обеспечения ИПБ*:

1) обеспечение и защита конституционных прав и свобод человека и гражданина, включая право на свободу, неприкосновенность частной жизни, защиту своей чести и доброго имени, свободу мысли и слова, право на информацию и свободу массовой информации;

2) формирование среды доверия в цифровой среде;

3) обеспечение доступа к информации, способствующей развитию личности и общества;

4) защита личности, социальных групп и общества от деструктивного информационно-психологического воздействия;

5) гарантирование психического здоровья и благополучия граждан;

6) сохранение традиционных духовно-нравственных ценностей и национальной идентичности российского общества, повышение культурного потенциала страны;

7) укрепление национального согласия, политической и социальной стабильности;

8) обеспечение информационного суверенитета России;

9) улучшение имиджа России и повышение ее авторитета на международной арене, усиление политического и культурного влияния России в мире;

10) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам деструктивного ИПВ на личность, социальные группы и общество.

Далее необходимо определить цель, задачи и направления обеспечения ИПБ. В Стратегии НБ 2021 целью обеспечения информационной безопасности названо укрепление суверенитета РФ в информационном пространстве (п. 56). В Доктрине ИБ 2016 общая стратегическая цель обеспечения информационной безопасности не определена, хотя в разделе IV зафиксированы такие цели применительно к отдельным областям государственного управления (обороны страны, государственной и общественной безопасности, экономики и др.).

По мнению автора, *стратегической целью обеспечения ИПБ* выступает поддержание состояния защищенности личности, социальных групп и общества в целом от деструктивного информационно-психологического воздействия, обеспечивающего гарантированную реализацию национальных интересов России.

На следующем уровне целеполагания необходимо дать характеристику задач и функций (направлений) обеспечения ИПБ. И здесь мы сталкиваемся с проблемой отсутствия общепринятого представления о задачах и функциях обеспечения безопасности в целом. Анализ Закона о безопасности, документов стратегического планирования в области обеспечения национальной безопасности обнаруживает не только значительные отличия в их перечне, но и даже использование разных терминов для их обозначения. Так, в ст. 9 Закона РФ «О безопасности» закреплялись пять «функций системы безопасности», тогда как в ст. 4 действующего Закона о безопасности схожий перечень функций вообще никак не обозначен, а лишь сопровождается предложением: «Деятельность по обеспечению безопасности включает в себя…». В законопроекте об ИПБ были разграничены задачи (ст. 6) и функции (ст. 7) обеспечения ИПБ. Однако в результате их анализа обнаружено частичное дублирование.

В Доктрине ИБ 2016 задачи обеспечения информационной безопасности не выделены, а его основные направления определены только применительно к отдельным сферам государственного управления. Положительно отличается в этом плане Стратегия НБ 2021. В ней четко обозначены основные задачи обеспечения информационной безопасности. К области ИПБ относятся следующие из них: 1) формирование безопасной среды оборота достоверной информации; 2) развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности РФ, определения их источников, оперативной ликвидации последствий реализации таких угроз; 3) создание условий для эффективного предупреждения, выявления и пресечения правонарушений, совершаемых с использованием ИКТ; 4) противодействие использованию информационной инфраструктуры РФ экстремистскими и террористическими организациями, специальными службами и пропагандистскими структурами иностранных государств для осуществления деструктивного информационного воздействия на граждан и общество и др.

Помимо основного тематического подраздела Стратегии НБ 2021, положения об обеспечении ИПБ присутствуют и в других разделах документа, посвященных обороне страны, государственной и общественной безопасности, защите традиционных российских духовно-нравственных ценностей, культуры и исторической памяти, стратегической стабильности и взаимовыгодному международному сотрудничеству. Их анализ позволяет выделить следующие дополнительные задачи обеспечения ИПБ: 1) поддержание морально-политического и психологического состояния личного состава Вооруженных сил и других воинских формирований, военно-патриотическое воспитание; 2) недопущение вмешательства во внутренние дела РФ, пресечение разведывательной и иной деятельности иностранных государств и отдельных лиц против национальных интересов РФ; 3) профилактика радикализма

и экстремизма, прежде всего среди детей и молодежи, недопущение распространения экстремистской продукции, пропаганды насилия и нетерпимости, межнациональной розни; 4) предупреждение и нейтрализация социальных, межконфессиональных и межнациональных конфликтов, сепаратизма, радикализма, деструктивных религиозных течений; 5) защита исторической правды, сохранение исторической памяти, противодействие фальсификации истории; 6) реализация государственной информационной политики по укреплению восприятия обществом традиционных российских духовно-нравственных и культурно-исторических ценностей, неприятию гражданами навязываемых извне деструктивных идей, стереотипов и моделей поведения; 7) укрепление культурного суверенитета РФ и сохранение ее единого культурного пространства, защита общества от внешней идейно-ценностной экспансии и внешнего деструктивного информационно-психологического воздействия; 8) духовно-нравственное и патриотическое воспитание граждан; 9) укрепление позиции российских средств массовой информации и коммуникации в глобальном информационном пространстве.

Как видно из изложенного перечня, новая Стратегия НБ 2021 очень четко и детально определяет задачи по обеспечению ИПБ. Причем большая их часть закреплена в рамках обеспечения не информационной безопасности, а и иных стратегических национальных приоритетов.

Представим авторское видение задач и функций обеспечения ИПБ. Первые рассматриваются как частные цели (подцели), которые нужно решить, чтобы достичь основной цели в заданных условиях.[268]

При определении задач обеспечения ИПБ важно избегать ряда методологических ошибок, присущих законодательным актам и документам стратегического планирования в области безопасности, на которые обратили внимание авторы коллективной монографии.[269] Они состоят в смешении основных и обеспечивающих, общих и частных задач обеспечения безопасности. Ученые альтернативно предлагают рассматривать в качестве основных задач обеспечения безопасности выявление угроз безопасности и противодействие им, а к вспомогательным задачам относят: управление процессом обеспечения безопасности; подбор, подготовку и расстановку сил и средств обеспечения безопасности; материально-техническое и финансовое обеспечение деятельности по обеспечению безопасности.[270]

Автор в целом разделяет данный подход и полагает возможным его использовать при определении задач ИПБ с учетом нескольких оговорок:

---

[268] *Новиков А. М., Новиков Д. А.* Методология. М.: СИНТЕГ, 2007. С. 323.

[269] Правовая основа обеспечения национальной безопасности Российской Федерации: монография / Под ред. А. В. Опалева. М.: ЮНИТИ-ДАНА, 2004. С. 76–82.

[270] Там же.

– во-первых, поддерживая разграничение основных и вспомогательных задач обеспечения безопасности, все же полагаем целесообразным их изложение в едином перечне;

– во-вторых, сам термин «вспомогательные задачи» представляется не вполне удачным, так как решение многих из них (постановка целей, правовое регулирование, определение сил и средств) предшествует деятельности по непосредственному обеспечению безопасности;

– в-третьих, считаем необходимым трактовать противодействие угрозам с учетом подходов, применяющихся в действующем российском законодательстве,[271] как деятельность, включающую три компонента: профилактику угроз; борьбу с угрозами (выявление, предупреждение, пресечение, правовое преследование); минимизацию и (или) ликвидацию последствий воздействия угроз;

– в-четвертых, предлагаем расширить число основных задач обеспечения безопасности применительно к сфере ИПБ, дополнив их повышением жизнестойкости объектов ИПБ.

Обобщая вышеизложенное, к *задачам обеспечения ИПБ* следует отнести:

1) прогнозирование, выявление, анализ и оценку угроз ИПБ;

2) анализ и оценку уязвимости личности, социальных групп и общества от деструктивного ИПВ;

3) стратегическое планирование в области обеспечения ИПБ;

4) правовое регулирование в области обеспечения ИПБ;

5) применение комплекса оперативных и долговременных мер по профилактике, предупреждению, пресечению и устранению угроз ИПБ, минимизации и (или) ликвидации последствий их воздействия;

6) применение комплекса оперативных и долговременных мер по повышению способности личности, социальных групп и общества противостоять деструктивному ИПВ;

7) организацию деятельности системы обеспечения ИПБ;

8) кадровое, информационное, материально-техническое и финансовое обеспечение деятельности субъектов обеспечения ИПБ;

9) международное сотрудничество в области обеспечения ИПБ.

Далее рассмотрим функции (направления) обеспечения ИПБ. По мнению Т. А. Поляковой, в условиях развития глобального информационного общества значимой теоретической проблемой информационного права становится обособление функций государства по обеспечению информационной безопасности.[272] Выделение направлений обеспечения

[271] См.: Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»; Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»; Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции».

[272] Актуальные проблемы информационного права: учебник / Коллектив авторов; под ред. И. Л. Бачило, М. А. Лапиной. М.: Юстиция, 2016. С. 370.

ИПБ важно не только для четкого определения предметного содержания деятельности уполномоченных субъектов, но и для указания основных векторов формирования и развития российского законодательства в данной сфере.

В теории управления функции рассматриваются как направления (виды) управленческой деятельности, обеспечивающие достижение целей управления и осуществляемые специальными приемами и способами.[273] Функция управления представляет собой устойчивую совокупность задач (операций, действий) по реализации процесса управления (его части) для достижения частных целей управления, основанную на разделении управленческого труда в органах управления.[274] Исходя из данной трактовки, в теории управления, начиная с классика А. Файоля,[275] принято выделять такие функции управления, как планирование, организация, координация, контроль.

Однако применительно к области обеспечения безопасности такая трактовка функций не подходит, так как она обозначает стадии управленческого процесса, а не ориентирует на направления деятельности субъектов обеспечения безопасности. Выйти из данной ситуации нам поможет обоснованная Г. А. Тумановым классификация функций управления на два класса: функции-операции, являющиеся функциями процесса управления, и функции-задачи, выступающие функциями системы управления.[276] Именно о последних, на наш взгляд, должна идти речь применительно к обеспечению безопасности.

Необходимо также учитывать важную мысль И. Л. Бачило о том, что «в конкретной системе понятие „функция" ставится в зависимость от сущности и сферы управления. Функция управления вообще приобретает плоть и кровь данного конкретного исторического социального организма – его системы, отдельных частей».[277] Это обязывает нас принимать во внимание специфику изучаемого вида безопасности и деятельности по ее обеспечению.

С учетом проведенного нами анализа Закона о безопасности, документов стратегического планирования в области национальной

---

[273] Теория управления: учебник / Под общ. ред. А. Л. Гапоненко, А. П. Панкрухина. 3-е изд., доп. и перераб. М.: РАГС, 2008. С. 87; Теория управления: учебник / Под ред. Ю. В. Васильева, В. Н. Парахиной, Л. И. Ушвицкого. 2-е изд., доп. М.: Финансы и статистика, 2005. С. 265.

[274] Основы теории управления в системах специального назначения / Под общ. ред. Ю. В. Бородакия, В. В. Масановца. М.: Управление делами Президента Российской Федерации, 2008. С. 26.

[275] *Вергилес Э. В.* Анализ принципов управления Анри Файоля. Моск. гос. ун-т экономики, статистики и информатики. М., 2001. С. 9.

[276] *Туманов Г. А.* Организация управления в сфере охраны общественного порядка. М.: Юридическая литература, 1971. С. 138.

[277] *Бачило И. Л.* Функции органов управления (правовые проблемы оформления и реализации). М.: Юрид. лит., 1976. С. 27.

и информационной безопасности, проекта Концепции Стратегии кибербезопасности России,[278] а также профильной научной литературы автор разработал собственную концепцию основных направлений (функций) обеспечения ИПБ. Однако предварим ее методологическим пояснением.

По мнению автора, при выделении направлений обеспечения безопасности нецелесообразно смешивать деятельность в рамках решения основных и обеспечительных задач. Для определения основных задач направления деятельности государственных органов отталкиваются от угроз безопасности и сфер их проявления (например, противодействие пропаганде терроризма или деятельности иностранных спецслужб по оказанию деструктивного ИПВ). При этом в рамках каждого из таких направлений деятельности необходимо решение однотипных обеспечительных задач в рамках выработки и реализации государственной политики обеспечения ИПБ (стратегическое планирование, правовое регулирование, материально-техническое обеспечение, подготовка кадров).

Поэтому мы изложим два перечня: основных направлений обеспечения ИПБ и основных направлений деятельности по выработке и реализации государственной политики обеспечения ИПБ.

Основные направления обеспечения ИПБ:

1) прогнозирование, выявление, анализ и оценка угроз ИПБ;

2) противодействие распространению негативной информации в средствах массовой информации и сети Интернет;

3) противодействие террористической и экстремистской пропаганде и вербовочной деятельности, разжиганию национальной, расовой, религиозной или социальной ненависти и вражды;

4) противодействие деструктивному ИПВ со стороны государственных органов и специальных служб иностранных государств, иностранных и международных организаций;

5) обеспечение информационно-психологической безопасности детей;

6) защита чести, достоинства и деловой репутации гражданина, деловой репутации юридического лица;

7) защита органов публичной власти, должностных лиц от деструктивного ИПВ;

8) противодействие фальсификации отечественной и мировой истории в ущерб интересам России;

9) противодействие распространению деструктивных субкультур и иных форм негативного ИПВ в духовной сфере;

10) противодействие преступлениям и административным правонарушениям, связанным с оказанием деструктивного ИПВ;

[278] Концепция Стратегии кибербезопасности России (проект) // Совет Федерации Российской Федерации. URL: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 12.10.2020).

11) информирование российской и зарубежной общественности о внутренней и внешней политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни;

12) ведение контрпропаганды в России и за рубежом;

13) формирование цифровой грамотности граждан и культуры информационной безопасности.

Основные направления деятельности по выработке и реализации государственной политики обеспечения ИПБ:

1) стратегическое планирование в сфере обеспечения ИПБ;

2) правовое регулирование в сфере обеспечения ИПБ;

3) осуществление государственного контроля (надзора) в сфере обеспечения ИПБ;

4) оказание государственных услуг в сфере обеспечения ИПБ;

5) координация деятельности субъектов обеспечения ИПБ;

6) организация материально-технического, финансового и информационного обеспечения деятельности субъектов обеспечения ИПБ;

7) проведение научных исследований в области обеспечения ИПБ;

8) подготовка кадров в области обеспечения ИПБ;

9) осуществление международного сотрудничества в области ИПБ.

В Доктрине ИБ 2016 закреплено, что обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами (п. 30). Эта деятельность осуществляется как в обычных, так и в особых условиях специальных правовых режимов.[279] В Доктрине ИБ 2000 был специально выделен ряд направлений обеспечения информационной безопасности в чрезвычайных ситуациях, не нашедший отражения в новой Доктрине.

В число базовых принципов обеспечения безопасности, согласно ст. 2 Закона о безопасности, входит *системность и комплексность* применения органами публичной власти «политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности». Реализация данного принципа в сфере государственного управления предполагает наличие системы обеспечения национальной безопасности Российской Федерации и соответствующих подсистем обеспечения отдельных видов безопасности.

К сожалению, в действующем Законе о безопасности понятие системы обеспечения безопасности вообще не используется, тогда как в утратившем силу аналогичном законе оно присутствовало, правда, ошибочно называлось «система безопасности». Согласно ст. 8 Закона РФ

[279] *Пчелинцев С. В.* Проблемы ограничения прав и свобод граждан в условиях особых правовых режимов: монография. М.: Норма, 2006.

«О безопасности» ее образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации и объединения, граждане, принимающие участие в обеспечении безопасности в соответствии с законом, а также законодательство, регламентирующее отношения в сфере безопасности. Как видно, законодатели выделяли в системе обеспечения безопасности два основных элемента: *институциональный* (субъекты обеспечения безопасности) и *нормативный* (законодательство в сфере обеспечения безопасности).

Вместе с тем в последние годы в документах стратегического планирования стал применяться несколько иной подход к определению системы обеспечения безопасности, выделяющий такие ее элементы, как *силы* и *средства* обеспечения безопасности. Он нашел отражение в утратившей силу Стратегии НБ 2009 и действующей Доктрине ИБ 2016. Согласно последней под силами обеспечения информационной безопасности понимаются «государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством РФ задач по обеспечению информационной безопасности», а под средствами – «правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности» (пп. «д» и «е» п. 2). Схожий подход нашел отражение и в новой Стратегии НБ 2021, в которой составными частями системы обеспечения национальной безопасности определены совокупность органов публичной власти и находящихся в их распоряжении инструментов (пп. 6 п. 5).

Автор в целом разделяет официальный подход, однако выступает против выделения инструментального элемента *вместо* нормативного, поскольку это противоречит значимости правовой регламентации общественных отношений в сфере обеспечения безопасности. Поэтому при дальнейшем рассмотрении мы будем исходить из триединой структуры системы обеспечения ИПБ, включающей (1) силы, (2) средства и методы, (3) правовое регулирование.

В Доктрине ИБ 2016 сказано, что система обеспечения информационной безопасности РФ является частью системы обеспечения национальной безопасности страны (п. 30). Соответственно, исходя из рассмотрения ИПБ как элемента ИБ, мы должны сделать вывод о том, что *система обеспечения ИПБ является частью системы (подсистемой) обеспечения ИБ*. Вместе с тем данному тезису присуща некоторая доля условности, поскольку выделение различных систем обеспечения отдельных видов безопасности является в большей мере мыслительным конструктом, «вписывающим» в нее определенные государственные органы и иные субъекты обеспечения безопасности. В реальности большинство из таких субъектов полифункциональны, что обуславливает их одновременное «членство» во многих системах обеспечения безопасности.

Таким образом, *система обеспечения ИПБ* представляет собой подсистему обеспечения ИБ, включающую в себя совокупность сил обеспечения ИПБ, используемых ими средств и методов, а также правового регулирования отношений в сфере обеспечения ИПБ. В ее структуре нами выделяются институциональная (силы), инструментальная (средства и методы) и нормативная (правовое регулирование) подсистемы.

Нормативная подсистема – система правового обеспечения ИПБ – играет особую роль, поскольку именно правовыми нормами регламентируется весь процесс обеспечения безопасности, включая определение его субъектов, их задач и функций, применяемых ими средств и методов деятельности.

Т. А. Полякова с соавторами отмечает иерархичность структуры системы правового регулирования обеспечения информационной безопасности в России. Элементами данной системы выступают правовые нормы, субъекты правоотношений, правовые средства, методы и принципы регулирования.[280] Этот вывод полностью применим к системе обеспечения ИПБ.

С учетом изложенного *систему правового обеспечения информационно-психологической безопасности можно определить как упорядоченный комплекс правовых средств, используемых для поддержания состояния защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.*

§ 2. Институционализация информационно-психологической безопасности в системе информационного права

Процессы широкого проникновения цифровых технологий во все сферы общественной жизни и вызванные ими социальные изменения обуславливают необходимость модернизации всей системы российского права. Как отмечает С. В. Поленина, «научно обоснованная система права тем важнее с точки зрения общественных интересов, чем точнее она отражает объективные закономерности».[281] Поэтому, как подчеркивает Т. А. Полякова, система информационного права должна достичь именно такого максимального соответствия в происходящих сегодня процессах цифровизации и развития информационного общества.[282] Ею отмечается усиление процесса институционализации в связи с развитием прорывных,

[280] Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. д. ю. н., профессора Т. А. Поляковой. Саратов: Амирит, 2020. С. 22–23.

[281] Теория государства и права: учебник / Под ред. В. К. Бабаева. М.: Юристъ, 2003. С. 406.

[282] *Полякова Т. А.* Влияние цифровой трансформации на развитие информационного права: тенденции, проблемы, перспективы // Мониторинг правоприменения. 2020. № 5. С. 54.

конвергентных информационных технологий, включая развитие институтов, имеющих междисциплинарный характер.[283] Мы полагаем, что таким новым правовым институтом информационного права является правовое обеспечение информационно-психологической безопасности.

Процесс институционализации в праве тесно связан с общими тенденциями развития правовой системы страны. «В проблематике правовой институционализации преломляются многие правовые явления и процессы – от правовой политики и правового регулирования отношений до реализации права и воспроизводства правопорядка».[284]

Как отмечает В. Б. Наумов, «в юридической науке доминирует понимание институционализации на основании институциональной теории как процесса создания институтов, а институт права традиционно рассматривается как система норм права, объединенных по признаку однородности их предмета».[285] Так, в юридическом словаре институты права определены как «относительно обособленные группы взаимосвязанных между собой юридических норм, регулирующих определенные разновидности общественных отношений».[286] Институт в правовом аспекте, по мнению Р. Г. Валиева, олицетворяет «интегрированную форму существования норм права».[287]

Институт, как и отрасль права, по мнению М. И. Байтина, характеризуют общие системные признаки функциональности и субстанциональности в их сочетании.[288] Базовыми признаками института права выступают предмет и метод правового регулирования. Предмет характеризует то, что регулирует право, а метод – определенные приемы, способы, средства воздействия права на общественные отношения.[289]

И. Л. Бачило определяет институты информационного права как «такие блоки правовых актов и норм, которые, будучи сгруппированы по единой цели, обеспечивают регулирование отношений» в сфере использования ИКТ.[290] И. М. Рассолов трактует институт информационного права как «относительно устойчивую и признанную группу информационно-правовых

---

[283] Там же. С. 55.

[284] *Валиев Р. Г.* Правовая институционализация и институты права: концептуальная модель // Lex russica. 2020. Т. 73. № 4. С. 104.

[285] *Наумов В. Б.* Институт идентификации в информационном праве: дис. … д-ра юрид. наук. М., 2020. С. 108.

[286] Институты права // Юридический энциклопедический словарь / М. О. Буянова и др.; отв. ред. М. Н. Марченко. М.: Проспект, 2009. С. 250.

[287] *Валиев Р. Г.* Правовая институционализация и институты права: концептуальная модель // Lex russica. 2020. Т. 73. № 4. С. 107.

[288] *Байтин М. И.* Сущность права (Современное нормативное правопонимание на грани двух веков). 2-е изд., доп. М.: ООО ИД «Право и государство», 2005. С. 288–289.

[289] Теория государства и права: курс лекций / Под ред. Н. И. Матузова и А. В. Малько. С. 399.

[290] *Бачило И. Л.* Информационное право: учебник для магистров. М.: Юрайт, 2015. С. 129.

норм, регулирующую определенные виды информационных правоотношений».[291]

В российской науке информационного права устоялось представление о рассмотрении правового регулирования обеспечения информационной безопасности в качестве института информационного права,[292] хотя ряд исследователей идентифицируют его как подотрасль информационного права.[293] Юридическим признанием данного факта можно считать принятие на уровне СНГ в 2014 г. модельного закона «Об информации, информатизации и обеспечении информационной безопасности», где в ч. 4 ст. 18 прямо закреплено, что «организационно-правовое регулирование обеспечения информационной безопасности рассматривается как важнейший институт информационного права и законодательства».

И. М. Рассолов выделил ряд признаков правового института информационной безопасности, включая наличие упорядоченной системы информационно-правовых норм, их целевую ориентированность на обеспечение жизненно важных интересов, выделение личностного, корпоративного и государственного уровней информационной безопасности.[294]

Учитывая современное состояние правового обеспечения информационной безопасности, автор солидарен с точкой зрения Т. А. Поляковой и иных ученых, определяющих его в качестве подотрасли информационного права, имеющей при этом межотраслевой характер.[295] Соответственно, мы предлагаем рассматривать совокупность правовых норм, регулирующих общественные отношения в сфере ИПБ, в качестве правового института «правовое обеспечение информационно-психологической безопасности» в составе названной подотрасли. Однако данное утверждение требует доказательства на основе изложенных выше критериев.

---

[291] *Рассолов И. М.* Информационное право: учебник. М.: Юрайт, 2011. С. 65.

[292] См.: *Бачило И. Л.* Информационное право: учебник для магистров. М.: Юрайт, 2015. С. 483–485; *Рассолов И. М.* Информационное право: учебник. М.: Юрайт, 2011. С. 353–359; Концепция Информационного кодекса Российской Федерации / Под ред. И. Л. Бачило. М.: ИГП РАН, 2014. С. 88–89; *Макаров О. С.* Правовое обеспечение информационной безопасности на примере защиты государственных секретов государств – участников Содружества Независимых Государств: автореф. дис. … д-ра юрид. наук. М., 2013. С. 23.

[293] *Лопатин В. Н.* Информационная безопасность России: дис. … д-ра юрид. наук. СПб., 2000. С. 136; *Полякова Т. А.* Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … д-ра юрид. наук. М., 2008. С. 13; *Андреев П. Г.* Институциональное развитие правового обеспечения информационной безопасности в российском информационном праве: автореф. дис. … канд. юрид. наук. Екатеринбург. 2012. С. 9–10; *Чеботарева А. А.* Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: дис. … д-ра юрид. наук. М., 2017. С. 146.

[294] *Рассолов И. М.* Информационное право: учебник. М.: Юрайт, 2011. С. 356.

[295] Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. д. ю. н., профессора Т. А. Поляковой. Саратов: Амирит, 2020. С. 23.

У выделенного института есть самостоятельный предмет правового регулирования – комплекс общественных отношений, связанных с защитой личности, социальных групп и общества от деструктивного ИПВ. Данная сфера отношений имеет достаточную четкую грань, отделяющую ее от другого большого блока отношений в рамках информационной безопасности – защиты информации. Названный предмет правового регулирования обладает достаточной однородностью, поскольку в его основе лежит общий механизм оказания деструктивного ИПВ на индивидуальную психику и общественное сознание, а также защиты от него.

Имеется характерный метод правового регулирования, охватывающий совокупность способов и средств воздействия права на общественные отношения. В сфере обеспечения ИПБ доминирует императивный метод правового регулирования, активно применяются правовые средства запретов и обязываний. Например, законодательством РФ установлены правовые запреты на распространение определенной негативной информации, дополняемые введением юридической ответственности за их нарушение и наделением государственных органов и информационных посредников обязанностями по ограничению распространения такого контента в определенных информационных средах.

Критерии единства правовых норм, нормативной обособленности и полноты регулируемых отношений выполняются лишь частично, что свидетельствует о том, что институт правового обеспечения ИПБ находится в стадии формирования. Вместе с тем уже сейчас отчетливо просматривается межотраслевая природа данного правового института, свойственная и его «материнской» подотрасли. «Институт права как системное правовое образование отличается высоким уровнем интеграции, выходящим за рамки отдельных отраслей права, приобретая межотраслевой или общеправовой статус», – отмечал Р. Г. Валиев.[296] Этот тезис справедлив в отношении изучаемого нами института правового обеспечения ИПБ.

Нормы информационного права играют ключевую роль в правовом регулировании целей, задач, принципов и направлений обеспечения ИПБ.[297] Прерогативой информационного права является регламентация вопросов противодействия распространению негативной информации в СМИ и сети Интернет.

---

[296] *Валиев Р. Г.* Правовая институционализация и институты права: концептуальная модель // Lex russica. 2020. Т. 73. № 4. С. 109.

[297] В статье ведущих российских ученых по информационному праву отмечалось, что «предметная и целевая основа отрасли определяется интересами человека, общества, государства как субъектов информационных отношений при использовании новых возможностей расширить базу своих знаний и использовать современные средства информационных коммуникаций, с одной стороны, и защитить этих участников информационного развития социума от возможного разрушительного или вредного для общества влияния – с другой». См.: *Бачило И. Л., Полякова Т. А., Антопольский А. А. и др.* Об основных направлениях развития информационного права за 2000–2015 гг. // Государство и право. 2017. № 1. С. 72.

Вместе с тем информационно-правовое регулирование не исчерпывает всей предметной области обеспечения ИПБ. Поэтому правовую основу ИПБ составляют также нормы иных отраслей права, включая конституционное, административное, уголовное, гражданское. Конституционное право устанавливает базовые принципы государственного и общественного устройства, правового статуса личности, а также систему органов публичной власти в Российской Федерации, имеющие отправное значение для всех сфер обеспечения безопасности. Кроме того, нормы конституционного законодательства в отдельных областях касаются вопросов противодействия деструктивному ИПВ (например, манипуляции общественным сознанием в ходе предвыборной агитации). Роль административного права проявляется прежде всего в регламентации правового статуса органов исполнительной власти, являющихся основными субъектами обеспечения ИПБ. Также административное право, равно как и уголовное право, устанавливает юридическую ответственность за правонарушения, связанные с оказанием деструктивного ИПВ на личность и социальные группы. Нормы гражданского права регламентируют вопросы защиты чести, достоинства и деловой репутации как нематериальных благ физических и юридических лиц, а также основания и виды гражданской ответственности в изучаемой нами области. Поэтому *правовой институт обеспечения ИПБ носит межотраслевой характер*.

Продемонстрируем этот тезис на основе анализа действующего российского законодательства, регламентирующего вопросы обеспечения ИПБ. В рассматриваемой сфере существует один специализированный федеральный закон, посвященный исключительно ИПБ. Речь идет о Законе о защите детей от информации. Согласно ч. 1 ст. 1 данного закона предмет его регулирования составляют отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции. В то же время в ч. 2 данной статьи содержатся оговорки, выводящие из сферы регламентации закона оборот некоторых видов информации, в частности информационной продукции, содержащей научную, научно-техническую, статистическую информацию либо имеющей значительную историческую, художественную или иную культурную ценность для общества, а также рекламы.

Принятие Закона о защите детей от информации в 2010 г. стало прорывным событием для развития системы правового обеспечения в нашей стране. Он установил важные правовые механизмы обеспечения ИПБ наиболее уязвимого объекта деструктивного ИПВ – детей. Вместе с тем, хотя нормы закона регламентируют большинство наиболее значимых форм распространения информации – зрелищные мероприятия, печатные издания, продукцию СМИ, они практически не распространяют свое

действие на интернет-ресурсы. Однако именно сеть Интернет в настоящее время выступает главным источником угроз ИПБ.

Для закрытия этой важнейшей области проявления угроз ИПБ были внесены многочисленные поправки в Закон об информации – базовый источник информационного права России. Именно его законодатель рассматривает в качестве основного правового источника противодействия интернет-угрозам различного рода, включая угрозы психологического характера.

Закон об информации регламентирует следующие основные аспекты обеспечения ИПБ:

– закрепление общего правового запрета на распространение противоправной информации (ч. 6 ст. 10);

– установление обязанностей отдельных субъектов по обеспечению ИПБ (ст. 6, 10.1, 10.3–10.6);

– регламентация порядка ограничения доступа к определенным видам негативной информации (ст. 15.1–15.1.2, 15.3, 15.3.1) и информационным ресурсам (15.4, 15.8, 15.9).

Со времени введения в 2012 г. в Закон об информации ст. 15.1, впервые закрепившей правовой механизм ограничения доступа к вредной информации в сети Интернет, блок правовых норм, направленных на закрепление различных правовых средств и механизмов обеспечения ИПБ, существенно вырос и продолжает постоянно расширяться. В этой связи А. А. Чеботаревой совершенно обоснованно указывалось на несоответствие названия закона сфере его регулирования и предлагалось заменить в нем слова «и о защите информации» словами «и обеспечении информационной безопасности».[298] При этом данный ученый ссылается на опыт модельного законодательства СНГ, а именно принятый в 2014 г. Модельный закон «Об информации, информатизации и обеспечении информационной безопасности».

Автор разделяет данное мнение. Реализация указанной инициативы повлечет необходимость закрепления базового понятийного аппарата в области информационной безопасности, включая ИПБ и дополнение Закона об информации статьями, посвященными организационно-правовым основам обеспечения информационной безопасности, а также ИПБ как ее составной части наряду с защитой информации.

Отметим еще один важный аспект. Признавая ключевую роль Закона об информации в противодействии интернет-угрозам ИПБ, следует признать, что в основном он предусматривает правовые механизмы борьбы с противоправным контентом, тогда как коммуникационные угрозы в сети Интернет нормы закона практически не затрагивают.

[298] *Чеботарева А. А.* Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: дис. … д-ра юрид. наук. М., 2017. С. 122.

Сфера СМИ в силу своей особой значимости является предметом регулирования отдельного законодательного акта – Закона РФ от 27 декабря 1991 г. № 2124–1 «О средствах массовой информации»[299] (далее – Закон о СМИ), одного из старейших источников информационного права России. К числу СМИ с 2011 г. относятся и сетевые издания – большой класс интернет-ресурсов.

Важнейшее значение для обеспечения ИПБ в деятельности СМИ имеет ст. 4 Закона о СМИ, регламентирующая недопустимость злоупотребления свободой массовой информации. Под этим понятием скрывается большое число различных форм распространения противоправного контента и иных общественно опасных действий в сфере массовой информации. Правовой запрет на злоупотребление свободой массовой информации в Законе о СМИ подкреплен широким спектром статей КоАП и УК РФ, устанавливающих ответственность за его нарушение.

Таким образом, российское информационное законодательство содержит большой комплекс правовых норм, регламентирующих вопросы обеспечения ИПБ в СМИ и сети Интернет – двух ключевых источниках ИПБ.

Сквозной характер имеет такой вид информации, как реклама, поскольку он охватывает как традиционные и новые медиа, так и офлайновые форматы (наружная, печатная, сувенирная реклама). В связи с повсеместным присутствием рекламы и широким применением в ней методов ИПВ она также требует внимания в контексте обеспечения ИПБ.

Отношения в сфере рекламы являются предметом регулирования Федерального закона от 13 марта 2006 г. № 38-ФЗ «О рекламе»[300] (далее – Закон о рекламе). Согласно п. 1 ст. 3 данного закона под *рекламой* понимается «информация, …адресованная неопределенному кругу лиц и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке».

Закон о рекламе регламентирует следующие правовые аспекты обеспечения ИПБ:

– общие требования к рекламе, включая критерии недобросовестной и недостоверной рекламы (ст. 5);

– правовые гарантии защиты детей в рекламе (ст. 6);

– закрепление перечня запрещенных объектов рекламирования (ст. 7);

– ограничения для отдельных способов распространения рекламы (ст. 14–20) и рекламы отдельных видов товаров (ст. 21–30.2).

Таким образом, рассмотренные законодательные акты, относящиеся к источникам информационного права, регламентируют отдельные аспекты обеспечения ИПБ в информационных офлайн- и онлайн средах,

[299] Российская газета. 1992. 8 февраля.
[300] СЗ РФ. 2006. № 12. Ст. 1232.

таких как СМИ, информационно-телекоммуникационные сети, включая сеть Интернет, зрелищные мероприятия и иные офлайн-формы распространения информации. Особое внимание заслуженно уделено правовым гарантиям защиты детей от негативной информации. Также обособленно установлены требования по предотвращению деструктивного ИПВ в рекламе.

Оценка состояния адекватности и полноты установленных данными законами правовых механизмов обеспечения ИПБ будет дана ниже. Однако уже на данном этапе очевидно, что при наличии достаточно многообразных правовых методов и средств противодействия угрозам ИПБ информационное законодательство не содержит отправных норм, характеризующих базовые аспекты обеспечения ИПБ, включая понятийный аппарат, угрозы ИПБ, правовые принципы и направления ее обеспечения. Следствием этого выступает отсутствие системности в правовом регулировании обеспечения ИПБ. Данный правовой пробел требует устранения.

Как отмечалось выше, информационно-правовое регулирование занимает ключевое место в системе правового обеспечения ИПБ, однако не исчерпывает его содержания. Конституционное законодательство, помимо основополагающих норм Основного закона, имеющих фундаментальную значимость для всей национальной правовой системы России, включает в себя федеральное законодательство, регламентирующее отдельные вопросы обеспечения ИПБ. В частности, в сфере избирательного процесса. Как известно, к стадиям избирательного процесса относится информационное обеспечение выборов и референдумов, включающее в себя информирование избирателей и участников референдума, предвыборную агитацию и агитацию по вопросам референдума. В рамках этой стадии широко применяются технологии манипуляции сознанием электората как самими кандидатами и избирательными объединениями, так и иными заинтересованными сторонами.[301] В связи с этим базовый Федеральный закон от 12 июня 2002 г. № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»,[302] а также основанные на его нормах законы о выборах отдельных органов публичной власти и должностных лиц содержат целый комплекс правовых мер, направленных на блокирование методов деструктивного ИПВ в отношении избирателей и гарантирование принципа их свободного волеизъявления[303] (ст. 3 названного закона).

---

[301] См.: *Егорова-Гантман Е. В., Плешаков К. В., Байбакова В. Б.* Политическая реклама. 2-е изд. М.: Никколо-Медиа, 2002.

[302] СЗ РФ. 2002. № 24. Ст. 2253.

[303] См.: *Смирнов А. А., Москвитина О. С.* Правовые основы противодействия манипуляции сознанием в избирательном процессе // Информатизация и информационная безопасность правоохранительных органов: XXI Всероссийская научная конференция (30–31 мая 2012 г.): сборник трудов. М.: Академия управления МВД России, 2012. С. 327–332.

Административное законодательство в рассматриваемой сфере регулирует множество аспектов обеспечения ИПБ:

- правовой статус субъектов обеспечения ИПБ;[304]

- правовые механизмы противодействия проявлениям терроризма и экстремизма в информационной среде, прежде всего противодействия экстремистской идеологии;[305]

- правовые меры, направленные на противодействие оказания деструктивного ИПВ со стороны государственных органов и специальных служб иностранных государств, иностранных и международных организаций;[306]

- правовые меры, направленные на противодействие деструктивным религиозным организациям;[307]

- правовые механизмы противодействия правонарушениям, связанным с оказанием деструктивного ИПВ;[308]

- административная ответственность за правонарушения в сфере ИПБ.[309]

Уголовное законодательство Российской Федерации закрепляет составы преступлений, связанных с оказанием деструктивного ИПВ, и предусматривает за них уголовные наказания. В последние годы в связи с появлением все новых контентных и коммуникационных угроз ИПБ число таких составов в УК РФ расширяется. Сама деятельность по выявлению, раскрытию, расследованию таких преступлений и рассмотрению уголовных дел в судах регламентируется Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[310] и Уголовно-процессуальным кодексом Российской Федерации от 18 декабря 2001 г. № 174-ФЗ.[311]

Гражданское право гарантирует защиту нематериальных благ, включая достоинство личности, честь и доброе имя, деловую репутацию (ст. 150

---

[304] Федеральные законы: от 17 января 1992 г. № 2202–1 «О прокуратуре Российской Федерации», от 3 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности, от 28 декабря 2010 г. № 403-ФЗ «О Следственном комитете Российской Федерации», от 7 февраля 2011 г. № 3-ФЗ «О полиции» и др.

[305] Федеральные законы: от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму», от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности».

[306] Федеральные законы: от 10 января 1996 г. № 5-ФЗ «О внешней разведке», от 12 января 1996 г. № 7-ФЗ «О некоммерческих организациях», от 28 декабря 2012 г. № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации».

[307] Федеральный закон от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях».

[308] Федеральные законы: от 24 июня 1999 г. № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних», от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» и др.

[309] Кодекс Российской Федерации об административных правонарушениях.

[310] СЗ РФ. 1995. № 33. Ст. 3349.

[311] СЗ РФ. 2001. № 52. Ст. 4921.

Гражданского кодекса Российской Федерации,[312] далее – ГК РФ). На них распространяются основные способы защиты гражданских прав. Также ГК РФ регламентирует механизмы компенсации морального вреда и защиты чести, достоинства и деловой репутации (ст. 151–152). Среди правовых способов защиты последних нормами ст. 152 ГК РФ предусмотрены опровержение порочащих его честь, достоинство или деловую репутацию сведений, удаление соответствующей информации, пресечение или запрещение ее дальнейшего распространения, возмещение убытков, компенсация морального вреда.

Проведенный анализ российского законодательства подтвердил тезис о *межотраслевом характере правового института обеспечения ИПБ и продемонстрировал наличие достаточно развитого механизма правового регулирования в данной сфере. Доминирующую роль в его структуре играют нормы информационного права, однако большое значение в правовом регулировании обеспечения ИПБ также имеют нормы конституционного, административного, уголовного и гражданского права.*

Вместе с тем действующий механизм правового регулирования обеспечения ИПБ имеет и ряд существенных недостатков. Важнейшим из них является отсутствие правового закрепления отправных начал и принципов обеспечения ИПБ, не позволяющих обрести данному механизму полноценной системности правового регулирования.

Кроме того, мы установили наличие больших пробелов в правовой регламентации целого ряда выделенных нами направлений обеспечения ИПБ, включая: защиту государственных и муниципальных органов, должностных лиц от деструктивного ИПВ; противодействие фальсификации отечественной и мировой истории в ущерб интересам России; противодействие распространению деструктивных субкультур и иных форм негативного ИПВ в духовной сфере; информационное обеспечение деятельности вооруженных сил, правоохранительных и иных государственных органов; информирование российской и зарубежной общественности о внутренней и внешней политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни.

В этой связи институт правового обеспечения ИПБ нуждается в дальнейшем системном развитии в целях реализации положений Стратегии НБ 2021.

§ 3. Правовые принципы обеспечения информационно-психологической безопасности

В механизме правового регулирования обеспечения ИПБ большое значение имеют правовые принципы, то есть закрепленные правовыми

[312] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ // СЗ РФ. 1994. № 32. Ст. 3301.

нормами основополагающие начала, исходные положения. Как отмечает Т. А. Полякова, «научные исследования базовых принципов обеспечения информационной безопасности носят фундаментальный характер, так как по сути направлены на развитие правовой системы государства, то есть его правовой политики в данной сфере».[313]

Принципы права в наиболее общем виде определяются как «исходные, определяющие идеи, положения, установки, которые составляют нравственную и организационную основу возникновения, развития и функционирования права».[314] По мнению В. М. Сырых, правовые принципы отражают основополагающие идеи и начала права, правового регулирования.[315] М. И. Байтин подчеркивает, что принципы права выражают главное, основное в праве, цели и тенденции его развития. И в сравнении с правовыми нормами, соответствующими определенному историческому периоду, принципы права отличаются большей устойчивостью и неизменностью в течение длительного времени.[316]

Признавая значение правовых принципов как отправных, исходных начал, нельзя упускать из виду их юридическую способность наряду с правовыми нормами выступать непосредственными регуляторами поведения и деятельности людей, то есть оказывать прямое регулирующее воздействие на поведение людей.[317] Таким образом, правовые принципы проявляют себя двояко: непосредственно и опосредованно (через конкретные нормативные предписания, выражающие сущность этих принципов).

В информационном праве принципы трактуются как «зафиксированные в правовых нормах, регулирующих информационные отношения, положения и идеи, определяющие сущность и содержание данной отрасли права, придающие системный характер ее нормам и институтам и позволяющие говорить о целостности механизма правового регулирования информационных отношений в обществе».[318] И. Л. Бачило провела обзорный анализ принципов информационного права и пришла к выводу о том, что в этой отрасли используется целая система принципов, включающая научные (системный подход, принцип гуманизации отношений, принцип учета диалектических зависимостей и связей и др.), конституционные (суверенитет РФ, принцип демократизма, законность и др.), общеправовые (законность, научность, системность и др.), специальные отраслевые

---

[313] *Полякова Т. А.* Базовые принципы правового обеспечения информационной безопасности // Труды Института государства и права РАН. 2016. № 3. С. 18.

[314] *Байтин М. И.* Сущность права (Современное нормативное правопонимание на грани двух веков). 2-е изд., доп. М.: ООО ИД «Право и государство», 2005. С. 148.

[315] *Сырых В. М.* Логические основания общей теории права. В 2 т. Т. 1: Элементный состав. М.: Юридический дом «Юстицинформ», 2000. С. 63.

[316] *Байтин М. И.* Сущность права (Современное нормативное правопонимание на грани двух веков). 2-е изд., доп. М.: ООО ИД «Право и государство», 2005. С. 149.

[317] *Червонюк В. И.* Теория государства и права: учебник. М.: ИНФРА-М, 2006. С. 269.

[318] *Рассолов И. М.* Информационное право: учебник. М.: Юрайт, 2011. С. 104.

принципы (свобода информации, установление ограничения доступа к информации только законом, достоверность информации и др.).[319]

Отправное значение для правового регулирования обеспечения ИПБ имеют положения Конституции Российской Федерации. Отметим ее наиболее значимые нормы,[320] являющиеся основополагающими началами для всей системы правового регулирования ИПБ:

– базовые национальные ценности и идентичность России (преамбула, ст. 67.1);

– признание идеологического многообразия, запрет установления государственной или обязательной идеологии (ч. 1 и 2 ст. 13);

– светский характер государства, запрет установления государственной или обязательной религии (ч. 1 ст. 14);

– запрет создания и деятельности общественных объединений, цели или действия которых направлены на насильственное изменение основ конституционного строя и нарушение целостности РФ, подрыв безопасности государства, создание вооруженных формирований, разжигание социальной, расовой, национальной и религиозной розни (ч. 5 ст. 13);

– признание и гарантирование свободы мысли и слова, свободы поиска, получения, использования и распространения информации (ч. 1 и 4 ст. 29);

– запрет пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду, пропаганды социального, расового, национального, религиозного или языкового превосходства (ч. 2 ст. 29);

– гарантирование свободы массовой информации и запрет цензуры (ч. 5 ст. 29);

– гарантирование свободы литературного, художественного, научного, технического и других видов творчества, преподавания (ч. 1 ст. 44);

– 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 (ч. 3 ст. 55);

– почитание памяти защитников Отечества, защита исторической правды, недопущение умаления значения подвига народа при защите Отечества (ч. 3 ст. 67.1);

– определение детей в качестве приоритета государственной политики России, создание государством условий, способствующих всестороннему духовному, нравственному, интеллектуальному и физическому развитию

[319] *Бачило И. Л.* Информационное право: учебник для магистров. М.: Юрайт, 2015. С. 99–109.

[320] Используется действующая редакция Конституции РФ с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.

детей, воспитанию в них патриотизма, гражданственности и уважения к старшим (ч. 4 ст. 67.1);

– отнесение обеспечения безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных к предмету ведения РФ (п. «м» ст. 71).

Закон об информации закрепляет комплекс принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации (ст. 3). Данные принципы естественным образом базируются на положениях Конституции РФ. К интересующей нас сфере ИПБ относятся следующие закрепленные в законе принципы:

– свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

– установление ограничений доступа к информации только федеральными законами;

– 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.

Свой свод принципов содержит Закон о безопасности. Статья 2 данного правового акта закрепляет следующие принципы обеспечения безопасности: законности; соблюдения прав и свобод человека и гражданина; системности и комплексности применения политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности; приоритета предупредительных мер; взаимодействия государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности (ст. 2). В Стратегии НБ 2021 и Доктрине ИБ 2016 такие принципы не выделены.

В законопроекте об ИПБ были сформулированы следующие принципы обеспечения ИПБ: государственная монополия на разработку и производство специальных средств ИПВ; гласность и гражданский контроль за обеспечением ИПБ; обязательность участия общественных организаций в деятельности по обеспечению ИПБ. Изложенный перечень весьма узок и недостаточно четко отражает основные конституционные принципы. Вместе с тем выделен интересный принцип государственной монополии на разработку и производство специальных средств ИПВ. Согласно ст. 2 законопроекта об ИПБ под такими средствами понимались «технические и программные средства, используемые для негативного информационно-психологического воздействия на человека или группу лиц». В ст. 15 данного законопроекта регламентировался перечень исключительных случаев применения специальных средств и методов

ИПВ. Идея установления монополии государственных структур на производство программно-технических спецсредств ИПВ и их применение в установленных законом случаях не лишена смысла, однако требует дополнительной проработки с участием профильных ведомств и структур.

Анализ правовых принципов обеспечения информационной безопасности приведен в трудах представителей науки информационного права.[321] Так, в подготовленной авторским коллективом ИГП РАН концепции Информационного кодекса РФ выделен комплекс таких принципов, включая «сдерживание распространения информации террористического, экстремистского и сепаратистского характера, а также подрывающей политическую, экономическую и социальную стабильность государства, культурный и духовный уклад общества».[322] Данный принцип посвящен противодействию оборота негативной информации, что заслуживает поддержки.

В условиях формирования глобального информационного общества большое значение для правового регулирования обеспечения ИПБ имеют принципы международного права. Основополагающие принципы международного права закреплены в Уставе Организации Объединенных Наций,[323] Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН, от 24 октября 1970 г.,[324] и Заключительном акте Совещания по безопасности и сотрудничеству в Европе от 1 августа 1975 г.[325]

К ним относятся 10 принципов: 1) суверенного равенства государств; 2) воздержания от угрозы силой или ее применения в международных отношениях; 3) разрешения международных споров мирными средствами; 4) невмешательства в дела, входящие в компетенцию государств; 5) обязанности государств сотрудничать во внешней сфере; 6) равноправия и самоопределения народов; 7) нерушимости государственных границ; 8) территориальной целостности; 9) уважения прав человека и основных свобод; 10) добросовестного выполнения международных обязательств.[326]

Сфера международной информационной безопасности (далее – МИБ) пока не стала предметом регулирования универсальных международных

[321] *Полякова Т. А.* Базовые принципы правового обеспечения информационной безопасности // Труды Института государства и права РАН. 2016. № 3. С. 17–40; Правовое регулирование обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. Т. А. Поляковой. Саратов: Амирит, 2019. С. 44–77.

[322] Концепция Информационного кодекса Российской Федерации / Под ред. И. Л. Бачило. М.: ИГП РАН, 2014. С. 93.

[323] Действующее международное право. Т. 1. М.: Московский независимый институт международного права, 1996. С. 7–33.

[324] Там же. С. 65–73.

[325] Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. XXXI. М., 1977. С. 544–589.

[326] Международное право: учебник / отв. ред. А. Н. Вылегжанин. М.: Высшее образование, Юрайт-Издат, 2009. С. 106–107.

договоров. Вместе с тем в 2011 г. на международной встрече Россией представлена концепция Конвенции об обеспечении международной информационной безопасности[327] (далее – концепция Конвенции МИБ). В данном документе изложен перечень принципов, соблюдение которых государствами-участниками необходимо «в целях создания и поддержания атмосферы доверия в информационном пространстве» (ст. 5). Приведем данный перечень с некоторыми изъятиями и обобщениями.

Основные принципы обеспечения международной информационной безопасности согласно концепции Конвенции МИБ:

– совместимость с задачами поддержания международного мира и безопасности, стратегической стабильности;

– соответствие общепризнанным принципам и нормам международного права;

– неделимость безопасности;

– достаточность потенциала любого государства по обеспечению безопасности национального информационного пространства;

– суверенное равенство всех государств-участников в информационном пространстве, включая право определять свои национальные интересы в данной области, выбирать способы их реализации;

– мирное урегулирование конфликтов;

– применимость права на самооборону в ответ на агрессию в информационном пространстве при условии идентификации ее источника и пропорциональности ответных мер;

– недопустимость бездоказательных и необоснованных обвинений других государств в совершении противоправных деяний с использованием информационно-коммуникационных технологий;

– соблюдение основных прав и свобод граждан, включая защиту от несанкционированного вмешательства в частную жизнь граждан, и соблюдение при этом баланса между этими правами и задачами противодействия использованию информационного пространства в террористических и иных преступных целях;

– недопустимость ограничений или нарушений доступа к информационному пространству, кроме как в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;

– добровольность и взаимность в деятельности по предупреждению, выявлению, пресечению, раскрытию и расследованию противоправных деяний в сфере использования информационно-коммуникационных

[327] Текст концепции Конвенции первоначально опубликован на сайте МИД России. URL: https://www.mid.ru/ru/foreign_policy/official_documents/1698725/ (дата обращения: 07.07.2021). Однако мы использовали новую редакцию данного документа 2021 г., размещенную на сайте Совета Безопасности РФ. См.: Совет Безопасности РФ. URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения: 09.01.2022).

технологий, в том числе в террористических и иных преступных целях, и ликвидации последствий таких деяний.

В первичной редакции концепции Конвенции МИБ 2011 г. также содержались такие принципы, как: ответственность государств за собственное информационное пространство, в том числе за его безопасность и содержание размещаемой в нем информации; гарантирование свободы слова и выражения мнения в информационном пространстве; обязанность государств поддерживать и стимулировать образовательно-просветительскую деятельность, направленную на формирование глобальной культуры кибербезопасности, и др., которые имеют прямое отношение к сфере ИПБ.

Как видно, концепция Конвенции МИБ закрепляет очень внушительный перечень правовых принципов обеспечения МИБ. Все они преследуют стратегическую цель создания и поддержания атмосферы доверия в информационном пространстве, предполагающую его использование в целях развития и сотрудничества стран, избегания конфронтации между ними и ведения «информационных войн». Большая часть принципов касается именно международных отношений (суверенного равенства, невмешательства во внутренние дела и др.), хотя другая часть относится к сфере внутренней политики государств (самостоятельность в целеполагании и выборе инструментария обеспечения информационной безопасности, соблюдение основных прав и свобод, недопустимость необоснованных ограничений или нарушений доступа к информационному пространству и др.). «Сквозное» значение имеет важнейший принцип государственного суверенитета в информационном пространстве, которому в проекте документа уделено большое внимание.

Также представляет интерес система основных принципов обеспечения информационной безопасности, закрепленная в Стратегии обеспечения информационной безопасности государств – участников Содружества Независимых Государств.[328] Среди них выделены: а) правовое равенство участников информационного взаимодействия; б) добровольность выполнения обязательств; в) проведение совместных мероприятий; д) последовательность действий государств; д) приоритетность предупредительных мер; е) совместная ответственность личности, общества и государства; ж) информирование общества.

С учетом проведенного исследования сущности и системы правовых принципов представим *авторское видение основных принципов обеспечения ИПБ:*

1) соблюдение прав и свобод человека и гражданина;

2) гарантирование свободы массовой информации и запрет цензуры;

3) законность;

[328] Утверждена решением Совета глав правительств СНГ от 25 октября 2019 г. // СПС «КонсультантПлюс».

4) 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;

5) суверенитет России в информационном пространстве;

6) создание условий, способствующих всестороннему духовному, нравственному, интеллектуальному и физическому развитию детей, воспитанию в них патриотизма, гражданственности и уважения к старшим;

7) охрана исторической памяти и защита исторической правды;

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

9) приоритет предупредительных мер обеспечения ИПБ;

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

Данные принципы имеют основополагающее значение для системы правового обеспечения ИПБ, правовой регламентации оснований и порядка применения мер обеспечения ИПБ. Они требуют правового закрепления в Законе об информации.

§ 4. Правовые средства и механизмы обеспечения информационно-психологической безопасности

Исследование механизма правового обеспечения ИПБ предполагает изучение правового инструментария, используемого информационным и иными отраслями российского права для защиты личности и общества от деструктивного психологического воздействия.

С. С. Алексеев определял механизм правового регулирования как взятую в единстве систему правовых средств, при помощи которой обеспечивается результативное правовое воздействие на общественные отношения.[329] Л. А. Морозова подчеркивала важность исследования данного механизма в целях определения правовых средств и способов упорядочения регулируемых отношений.[330]

Начнем рассмотрение с *методов правового регулирования* отношений в сфере обеспечения ИПБ. В теории права методы правового регулирования определяются как «совокупность приемов, способов правового воздействия на общественные отношения».[331]

Традиционно выделяют два основных метода правового регулирования: императивный, основанный на обязательных властных предписаниях и соподчинении одних участников другим, и диспозитивный,

---

[329] *Алексеев С. С.* Теория права. М.: Издательство БЕК, 1995. С. 215.

[330] *Морозова Л. А.* Теория государства и права: учебник. 4-е изд., перераб. и доп. М.: Эксмо, 2010. С. 293.

[331] Там же. С. 297; Теория государства и права: курс лекций / Под ред. Н. И. Матузова и А. В. Малько. 2-е изд., перераб. и доп. М.: Юрист, 2003. С. 399.

характеризующийся автономией и равноправием сторон, предоставлением субъектам возможности выбора вариантов поведения.[332]

С. С. Алексеев отмечал, что в отраслях права данные первичные методы правового регулирования выступают в различных вариациях и сочетаниях в зависимости от характера регулируемых отношений и иных социальных факторов.[333] Информационное право относится к отраслям публичного права, что предопределяет доминирование императивного метода правового регулирования. И. Л. Бачило называла его «государственно-правовым», подчеркивая при этом, что «здесь реализуются свойства властности и первенства государственной воли, которые свойственны административно-правовым отношениям».[334] Это особенно характерно для отношений в сфере обеспечения информационной безопасности, где государство преимущественно действует через установление жестких правил, обязанностей и запретов, подкрепленных мерами юридической ответственности.

Большинство норм информационного законодательства содержит властные предписания, связанные с осуществлением государственными органами определенных мер обеспечения ИПБ, а также соблюдением запретов и исполнением обязанностей физическими и юридическими лицами, некоммерческими организациями. Так, Законом об информации установлены алгоритмы ограничения доступа к интернет-ресурсам, содержащим противоправный контент (ст. 15.1–15.9). При этом четко регламентируются правила действий государственных и иных структур, вовлеченных на каждом этапе процедуры.

Вместе с тем в информационном праве в целом и правовом регулировании ИПБ в частности есть место и методам диспозитивного регулирования. Так, ч. 2 ст. 14 Закона о защите детей от информации закрепляет диспозитивную норму, согласно которой не являющийся сетевым изданием интернет-ресурс может содержать возрастную маркировку информационной продукции, которая присваивается ими самостоятельно.

Метод правового регулирования как более общая правовая категория включает в себя комплекс элементов, коими выступают способы правового регулирования. Основными способами правового регулирования являются: «а) дозволение – предоставление лицам права на свои собственные действия; б) запрещение – возложение на лиц обязанности воздерживаться от совершения действий определенного рода; в) позитивное связывание (обязывание) – возложение на лиц обязанности

---

[332] Теория государства и права: курс лекций / Под ред. Н. И. Матузова и А. В. Малько. 2-е изд., перераб. и доп. М.: Юрист, 2003. С. 401; *Червонюк В. И.* Теория государства и права: учебник. М.: ИНФРА-М, 2006. С. 314.

[333] *Алексеев С. С.* Теория права. М.: Издательство БЕК, 1995. С. 224.

[334] Актуальные проблемы информационного права: учебник / Коллектив авторов; под ред. И. Л. Бачило, М. А. Лапиной. М.: Юстиция, 2016. С. 40.

к активному поведению».[335] В. И. Червонюк в качестве дополнительных способов называет поощрение и рекомендации – своеобразные стимулы к правомерному поведению.[336]

В механизме правового обеспечения ИПБ весьма распространено использование *правовых запретов*. Примерами таких запретов выступают:

– запрет злоупотребления свободой массовой информации (ст. 4 Закона о СМИ);

– запрет распространения противоправной информации (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 (ч. 7 ст. 10 Закона об информации);

– запрет недобросовестной и недостоверной рекламы (ч. 1 ст. 5 Закона о рекламе);

– запрет оборота информационной продукции, содержащей информацию, запрещенную для распространения среди детей (ч. 1 ст. 11 Закона о защите детей от информации), и др.

Фундаментальное значение в механизме правового обеспечения ИПБ имеет закрепленный Законом об информации *запрет распространения противоправной информации*. В нем проявляется межотраслевая природа рассматриваемого правового института и прослеживаются отраслевые взаимосвязи информационного, административного и уголовного права. Данный правовой запрет сформулирован двояко: сначала через перечисление нескольких конкретных видов негативного контента (информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды), распространение которого запрещается, а затем через указание «иной информации, за распространение которой предусмотрена уголовная или административная ответственность». Таким образом, законодатель пошел по пути закрепления открытого перечня противоправной информации, который постоянно корректируется путем внесения изменений в УК и КоАП РФ.

В Модельном законе СНГ «Об информации, информатизации и обеспечении информационной безопасности» 2014 г. использован несколько иной подход к формулированию рассматриваемого запрета. В нем имеется отдельная ст. 25 «Защита от распространения вредной и использования деструктивной информации». В ч. 1 данной статьи установлен правовой запрет на распространение двух категорий вредной (деструктивной) информации: 1) информации, нарушающей права и законные интересы

[335] *Алексеев С. С.* Теория права. М.: Издательство БЕК, 1995. С. 225.

[336] *Червонюк В. И.* Теория государства и права: учебник. М.: ИНФРА-М, 2006. С. 315.

граждан и организаций; 2) информации, оказывающей деструктивное воздействие на индивидуальное, групповое или общественное сознание, подрывающей национальную безопасность. Авторами модельного закона предпринята попытка построить исчерпывающий перечень такой информации.

К информации, нарушающей права и законные интересы граждан и организаций, отнесены: заведомо ложная, позорящая, унижающая честь и достоинство личности информация; сведения, дискредитирующие деловую репутацию хозяйствующего субъекта; ложные сведения о товарах и услугах; заведомо ложное сообщение, в том числе об опасности; информация, содержащая угрозы причинения вреда правам и интересам лица, в том числе угрозу убийства или причинения другого вреда здоровью, угрозу уничтожения имущества; иная информация при отсутствии возможности отказаться от ее получения (ч. 1.1 ст. 25).

В качестве информации, оказывающей деструктивное воздействие на индивидуальное, групповое или общественное сознание, подрывающей национальную безопасность, идентифицированы: информация экстремистского, порнографического характера; информация, пропагандирующая культ насилия и жестокости, содержащая призывы к насильственному свержению конституционного строя, организации или проведению массовых беспорядков; информация, пропагандирующая войны, социальную, национальную, религиозную и расовую вражду или рознь; информация, включающая угрозу совершения акта терроризма; сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов, а также взрывчатых веществ и огнестрельного оружия (ч. 1.2 ст. 25).

Сами виды вредной (деструктивной) информации, перечисленные в нормах модельного закона, нами поддерживаются. Они во многом совпадают с выделенным нами выше перечнем основных контентных угроз ИПБ. Однако у автора имеются два методологических замечания.

Во-первых, в основе всех указанных в модельном законе видов вредной (деструктивной) информации лежит механизм оказания деструктивного ИПВ, но его типы различаются (введение в заблуждение, запугивание, устрашение, разжигание розни и т. д.). Поэтому разделение его на две предложенные категории, хотя и имеет определенную логику, но в целом представляется нам неверным.

Во-вторых, формирование закрытого (исчерпывающего) перечня вредной информации также видится нам нецелесообразным. Если для модельного закона такое решение отчасти может быть оправдано, то в национальном законодательстве лучше следовать формуле, использованной в российском Законе об информации. Она, напомним, предполагает указание конкретных видов запрещенного негативного

контента (прямой способ изложения), а также запрет распространения любой иной информации, за которую установлена уголовная или административная ответственность (бланкетный способ изложения). Это позволяет обеспечить определенную стабильность правовой нормы, иначе в нее пришлось бы постоянно вносить изменения и дополнения. Вместе с тем в российском законе стоило бы изложить более полный перечень вредной информации, взяв за основу нормы Модельного закона об информации и Закона о СМИ.

Любой вариант правовой регламентации перечня негативной информации, запрещенной к распространению, требует последующей синхронизации с механизмами ограничения доступа к такой информации. В России с момента введения Реестра запрещенных интернет-ресурсов использована достаточно интересная схема. Законодатель устанавливает процедуры блокировки таких ресурсов, содержащих определенные виды запрещенной информации (ст. 15.1, 15.1–1, 15.3 Закона об информации), во внесудебном порядке. Перечень видов такой информации постоянно пополняется. При этом для всех остальных видов противоправного контента предусмотрена процедура ограничения доступа на основании судебного решения (п. 2 ч. 5 ст. 15.1 Закона об информации). Такой алгоритм работы правового механизма блокировки в целом можно признать приемлемым. Однако налицо отсутствие системности и четких методологических принципов его функционирования.

Еще одним правовым способом обеспечения ИПБ в рамках императивного метода регулирования выступает *обязывание*. Чаще всего оно выражается в закреплении обязанностей определенных субъектов информационной сферы в рамках регламентации их правового статуса. Такие обязанности Законом об информации установлены, 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). Их содержание весьма разноплановое и варьируется от обязанности хранить переписку и метаданные для ОРИ (ч. 3 ст. 10.1) до обязанности прекратить выдачу сведений об указателе страницы сайта в сети Интернет, позволяющих получить доступ к информации о заявителе, распространяемой с нарушением закона, являющейся недостоверной или неактуальной, для оператора поисковой системы (ч. 1 ст. 10.3).

Наиболее значимыми в контексте обеспечения ИПБ выступают следующие юридические обязанности: а) не допускать использования сервиса в целях совершения уголовно наказуемых деяний, распространения пропаганды терроризма и иных экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости; б) проверять достоверность распространяемых общественно значимых сведений до их распространения; в) не допускать использование сервиса

в целях сокрытия или фальсификации общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений; г) не допускать распространение новостной информации с целью опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями и ряд иных. Они установлены для новостных агрегаторов и владельцев аудиовизуальных сервисов (ст. 10.4–10.5). Хотя часть из них сформулирована по типу пассивных обязанностей, то есть обязанности не допустить чего-то, их реализация предполагает активную деятельность по предварительному изучению, проверке и оценке распространяемого контента, а также принятию мер по прекращению оборота недостоверного контента в определенных случаях.

Обращает на себя внимание, что первая из содержащихся в списке обязанностей («не допускать использование сервиса в целях совершения…») текстуально совпадает с формулировкой ч. 1 ст. 4 Закона о СМИ, описывающей формы злоупотребления свободой массовой информации. Однако другие многочисленные формы такого злоупотребления (ч. 2–9 ст. 4 Закона о СМИ) в статьи о правовом статусе новостных агрегаторов и владельцев аудиовизуальных сервисов не попали. Это может быть объяснимо разницей между СМИ и интернет-сервисами, но только отчасти. Например, обязанность не допускать распространения сведений, содержащих инструкции по самодельному изготовлению взрывчатых веществ и взрывных устройств, является вполне универсальной. Даже в Законе о СМИ правовой запрет на распространение такой информации установлен не только для СМИ, но и применительно к «информационно-телекоммуникационным сетям». С другой стороны, непонятно, почему использование СМИ в целях распространения фейковой информации не нашло отражение в числе форм злоупотребления свободой СМИ в ст. 4 Закона о СМИ? Видимо, о данной норме забыли, когда принимали пакетные изменения в законодательство, касающиеся борьбы с фейками.

Ранее также комплекс обязанностей был установлен для блогеров, однако в 2017 г. содержащая его ст. 10.2 была признана утратившей силу якобы в связи с ее «неэффективностью».[337] Нам такой аргумент представляется весьма сомнительным. Популярные блогеры имеют большие зрительские аудитории и по своему влиянию сопоставимы с некоторыми СМИ, а потому выступают мощными потенциальными источниками деструктивного ИПВ. Упраздненная статья закрепляла обязанность блогеров соблюдать предписания законов, в частности: не допускать

[337] Власти решили отменить «Закон о блогерах»: в нем нет смысла // CNews. 09 июня 2017 г. URL: https://www.cnews.ru/news/top/2017–06–09_vlasti_reshili_otmenit_zakon_o_blogerah_v (дата обращения: 12.07.2021).

злоупотребления свободой массовой информации; проверять достоверность размещаемой общедоступной информации до ее размещения и незамедлительно удалять размещенную недостоверную информацию; не допускать публикацию сведений о частной жизни гражданина и др. Конечно же, признание упомянутой статьи Закона об информации не означает признания за блогерами права нарушать требования российского законодательства. Однако ряд конкретных обязанностей, в частности проверка достоверности публикуемой информации и незамедлительное удаление фейков, нигде больше не закреплены. Поэтому мы считаем решение об исключении ст. 10.2 из Закона об информации ошибкой, требующей исправления. Автор вовсе не настаивает на «реставрации» данной статьи в прежнем виде, однако считает необходимым правовую регламентацию статуса такой важной категории участников информационной сферы, как блогеры.

Третьим правовым способом регулирования обеспечения ИПБ выступает *дозволение*, олицетворяющее диспозитивный метод регулирования. Дозволение преимущественно используется в информационном праве при регламентации правового статуса физических лиц. Так, введенная в 2021 г. 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 обращение о принятии мер по удалению указанной информации или блокировке распространяющих их интернет-ресурсов.

Однако дозволения могут касаться и иных субъектов информационных правоотношений. Например, ст. 21 Закона о защите детей от информации наделяет правом осуществлять общественный контроль за соблюдением требований данного закона не только граждан, но и некоммерческие организации, в том числе посредством формирования горячих линий.

По нашему мнению, дозволение является важным методом правового обеспечения ИПБ, и его применение должно расширяться. Вектором такого расширения должна стать правовая регламентация прав физических и юридических лиц по участию в обеспечении ИПБ. Так, весьма перспективным представляется завершение реализации правовой инициативы о принятии федерального закона о кибердружинах, который должен регламентировать права и обязанности участников таких кибердружин в сфере обеспечения информационной безопасности.

Что касается дополнительных способов правового регулирования, к которым относятся *поощрение* и *рекомендации*, то они находят необоснованно малое применение в механизме правового обеспечения ИПБ. Особенно это касается законодательного уровня, где такие нормы практически отсутствуют. Между тем А. В. Минбалеев называл развитие таких способов регулирования, как льготы и стимулы, одним из направлений

трансформации метода информационного права.[338] Это подтверждается и зарубежной практикой. Проведенный нами анализ зарубежного опыта, в частности Европейского союза, показал активное применение поощрительных и рекомендательных норм в тексте правовых актов, посвященных обеспечению информационной безопасности.[339]

Опыт участия автора в ежегодном Форуме безопасного Интернета и иных подобных конференциях, где присутствовали представители ведущих СМИ и компаний интернет-отрасли, показал, что со стороны указанных субъектов в добровольном порядке реализовано множество позитивных инициатив, направленных на противодействие инфоугрозам и защиту своих пользователей. Собственно, сам названный Форум безопасного Интернета как главная площадка по теме кибербезопасности в части защиты от контентных и коммуникационных угроз был учрежден в 2009 г. по инициативе общественных и коммерческих организаций, включая Координационный центр домена.RU и Региональный общественный центр интернет-технологий (РОЦИТ).[340] Минкомсвязь России неизменно поддерживало проведение Форума. Однако в целом государство недостаточно четко, на наш взгляд, сформулировало заинтересованность в реализации такого рода инициатив гражданского общества и интернет-отрасли. Сделать это можно было с помощью поощрительных и рекомендательных правовых норм.

Положительным в этом плане является принятие Плана мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 годы.[341] В Плане закреплен комплекс поощрительных и рекомендательных норм, направленных на стимулирование участия институтов гражданского общества в обеспечении ИПБ детей и распространение имеющегося положительного опыта в данной сфере. В частности, План предусматривает: оказание государственной поддержки социально значимым проектам в области печатных и электронных массмедиа для детей и молодежи (п. 3), аккумулирование лучших практик субъектов РФ по поддержке региональных производителей информационной продукции для детей с последующей выработкой рекомендаций для субъектов РФ (п. 12); организацию и проведение Всероссийского конкурса социальной рекламы антинаркотической направленности и пропаганды здорового образа жизни «Спасем жизнь

[338] Цифровая трансформация: вызовы праву и векторы научных исследований: монография / Под общ. ред. А. Н. Савенкова; отв. ред. Т. А. Полякова, А. В. Минбалеев. М.: РГ-Пресс, 2021. С. 64.

[339] *Смирнов А. А.* Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского союза: монография. М.: ЮНИТИ-ДАНА, 2012.

[340] В Москве прошел Форум безопасного Интернета // Координационный центр домена.RU/.РФ. 12 февраля 2010 г. URL: https://cctld.ru/media/news/kc/18577/ (дата обращения: 12.08.2021).

[341] Утвержден приказом Минцифры России от 1 декабря 2020 г. № 644 // Вестник образования России. 2021. № 1.

вместе», направленного на формирование у подростков и молодежи негативного отношения к незаконному потреблению наркотиков (п. 24) и др. Принятие такого Плана можно только приветствовать.

Далее рассмотрим специальные правовые механизмы, используемые для обеспечения ИПБ. Такие механизмы включают определенные правовые средства и методы или их комплекс. Проведенный анализ информационного законодательства позволил отнести к ним следующие:

1. *Установление правовых запретов и иных ограничений на распространение определенных видов негативной информации* – означает правовое закрепление запретов на распространение негативного контента, а также ограничений иных видов. Правовые ограничения могут выражаться «в уменьшении количества возможных форм осуществления права или свободы, в фиксации или сужении пространственных и временных границ реализации права или свободы, круга лиц, имеющих возможность пользоваться правом (свободой), в исключении юридической возможности осуществления права или свободы в определенных случаях, в усложнении порядка осуществления права или свободы, а также в уничтожении, изъятии либо умалении блага, лежащего в основе конституционного права или свободы».[342]

Примеры основных правовых запретов такого рода были рассмотрены нами выше. Основополагающее значение имеет норма ч. 6 ст. 10 Закона об информации, устанавливающая запрет распространения противоправной информации. Отметим также, что нормами уголовного и административно-деликтного права может устанавливаться запрет не только на распространение, но и на изготовление (производство) определенных видов негативного контента, например детской порнографии (ст. 242.1 УК РФ).

Более сложный механизм регламентирован Законом о защите детей от информации. Согласно п. 7 ст. 2 данного закона под информацией, причиняющей вред их здоровью и развитию, понимается «информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом». Статья 5 закона детализирует это определение и выделяет две основные категории такой информации: 1) запрещенная для распространения среди детей; 2) информация, распространение которой среди детей определенных возрастных категорий ограничено. При этом нужно учитывать, что речь идет именно о детях. Поэтому даже информация первой категории не запрещена для распространения среди взрослых. Весь сложный правовой механизм действия закона направлен на то, чтобы оградить всех

[342] *Смирнов А. А.* Ограничение прав и свобод человека и гражданина Российской Федерации при обеспечении обороны страны и безопасности государства: автореф. дис. … канд. юрид. наук. М., 2007. С. 8.

детей от доступа к запрещенной для них наиболее опасной информации и при этом разграничить доступ детей разных возрастных категорий к соответствующим видам информации, сохранив при этом возможность доступа и потребления такого контента со стороны взрослых.

Закон о СМИ, помимо базового запрета на злоупотребление свободой массовой информации, устанавливает более гибкие ограничения на оборот определенного негативного контента. Например, такие ограничения установлены для эротического контента (ст. 37 Закона о СМИ).

2. *Закрепление специальных правил оборота информационной продукции определенных видов* – означает установление правовыми нормами специальных условий производства и распространения негативной информации. Такие условия могут включать пространственные и временные ограничения распространения контента, дополнительные требования к обороту информационной продукции. Все они нашли отражение в Законе о защите детей от информации.

Метод «временного водораздела» закреплен в ст. 13 данного закона, касающейся теле- и радиовещания. Согласно ей информационная продукция категории (18+) не подлежит распространению посредством теле- и радиовещания с 4 до 23 часов по местному времени, за определенными исключениями. Для части сведений категории «16+» допустимый временной интервал показа определен с 7 до 21 часа.

Законом о защите детей от информации также установлены пространственные ограничения для распространения информационной продукции, содержащей запрещенную для детей информацию. В частности, ее запрещено распространять в детских учреждениях и организациях или на расстоянии менее чем сто метров от них (ч. 3 и 4 ст. 15).

В рассматриваемом законе установлено множество дополнительных требований для распространения определенных видов информационной продукции. Например, они касаются содержания и художественного оформления информационной продукции, предназначенной для обучения детей в дошкольных образовательных организациях и используемой в образовательном процессе (ч. 2 и 3 ст. 15); содержания обложки и упаковки полиграфической продукции, содержащей информацию категории 18+ (ч. 1 и 2 ст. 16); наличия звукового оповещения о недопустимости или об ограничении присутствия детей соответствующих возрастных категорий на зрелищном мероприятии (ч. 7 ст. 11), и т. д.

3. *Закрепление обязанностей субъектов информационных правоотношений по обеспечению ИПБ* – означает установление правовыми нормами обязательств участников правоотношений по обеспечению ИПБ. Именно такой правовой механизм использовал законодатель применительно к ключевым информационным посредникам в сети Интернет. Начиная с 2014 г. в Закон об информации постепенно вводились новые

статьи, регламентирующие обязанности: 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). Значительная часть этих обязанностей касается обеспечения ИПБ, о чем было сказано выше.

Особую значимость имело дополнение Закона об информации в конце 2020 г. статьей 10.6 «Особенности распространения информации в социальных сетях». Данной статьей на владельцев социальных сетей был возложен комплекс обязанностей по соблюдению правовых запретов и ограничений в части распространения негативной информации, соблюдению прав и свобод граждан и организаций, размещению в социальной сети правил ее использования, адреса электронной почты для направления ему юридически значимых сообщений, своих данных, а также электронной формы для направления обращений о распространяемой с нарушением закона информации и ряд других. Однако наиболее важным стало закрепление обязанностей владельцев социальных сетей осуществлять мониторинг в целях выявления противоправного контента и принимать меры по ограничению доступа к нему.

4. *Возрастная классификация и маркировка информационной продукции* – предполагает проведение классификации информационной продукции на предмет приемлемости содержащейся в ней информации для людей определенных возрастных категорий с последующим нанесением на такую продукции присвоенного знака возрастной категории. Такой правовой механизм установлен Законом о защите детей от информации, которым выделены следующие возрастные категории информационной продукции: информационная продукция 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+). Требования к маркировке информационной продукции регламентированы ст. 12 данного Закона.

Сам правовой механизм возрастной классификации и маркировки используется двояким образом. С одной стороны, она выступает основой для установления правовых режимов оборота информационной продукции определенных возрастных категорий, а с другой – имеет самостоятельную значимость как способ оповещения родителей и педагогов о возрастных ограничениях информационной продукции для принятия ими решения о целесообразности и допустимости показа ее детям.

5. *Экспертиза информационной продукции* – означает производство исследований информационной продукции с использованием

специальных познаний. Основным нормативным правовым актом, регламентирующим экспертную деятельность в РФ, выступает Федеральный закон от 31 мая 2021 г. № 73-ФЗ «О государственной судебно-экспертной деятельности»[343] (далее – Закон об экспертизе). 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.[344] 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.[345]

Основным видом экспертиз в сфере ИПБ выступает лингвистическая экспертиза текста. Однако могут проводиться и другие виды экспертиз, например психофизиологическая, компьютерно-техническая и иные, в целях исследования наличия скрытых вставок, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье, при производстве по делу об административном правонарушении, предусмотренном ч. 1 ст. 13.15 КоАП РФ.

6. *Идентификация личности абонентов, пользователей сети Интернет и цифровых сервисов* – означает систему мер, направленную на установление и проверку подлинности личности пользователей информационных сервисов и услуг. Один из ведущих исследователей данной темы В. Б. Наумов определяет идентификацию как «информационный процесс, направленный на установление субъектного и объектного состава правоотношений на основе идентификаторов или их совокупности».[346]

Значимость идентификации в механизме обеспечения ИПБ обуславливается тем, что она направлена на устранение анонимности как одного из важнейших угрозообразующих факторов в цифровой

[343] СЗ РФ. 2001. № 23. Ст. 2291.

[344] *Бельчиков Ю. А., Горбаневский М. В., Жарков И. В.* Методические рекомендации по вопросам лингвистической экспертизы спорных текстов СМИ: сборник материалов. М.: ИПК «Информкнига», 2010. С. 29–30.

[345] Приказ Минкомсвязи России от 29 августа 2012 г. № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей» // Российская газета. 2012. 24 октября.

[346] *Наумов И. Б.* Институт идентификации в информационном праве: дис. … д-ра юрид. наук. М., 2020. С. 58.

среде. А. К. Жарова вполне обоснованно оценивает анонимные сети как источник информационных конфликтов.[347] Анонимностью пользуются как иностранные спецслужбы, так и экстремисты и иные преступники для осуществления вредоносной деятельности в цифровой среде, связанной с оказанием негативного ИПВ на отдельных индивидов или социальные группы. Фактор анонимности наиболее активно проявляет себя при использовании мобильной связи и информационно-телекоммуникационных сетей.

В этой связи в последние годы законодатель внес в действующее информационное законодательство ряд норм, направленных на устранение или снижение влияния анонимности в цифровых коммуникациях. В частности, были нормативно закреплены обязанности по осуществлению идентификации пользователей для оператора связи (ст. 44 Закона о связи) и организатора сервиса обмена мгновенными сообщениями (ч. 4.2 ст. 10.1 Закона об информации). Таким образом были существенно сокращены возможности для анонимного пользования мобильной связью, мессенджерами и услугами доступа к сети Интернет. Помимо пользователей, Закон об информации предусматривает идентификацию ряда важных информационных посредников, в частности владельцев новостных агрегаторов (ст. 10.4), аудиовизуальных сервисов (ст. 10.5) и социальных сетей (ст. 10.6).

Как справедливо отмечает В. Б. Наумов, реализация различных методов идентификации в условиях цифровой трансформации способствует решению важной задачи обеспечения доверия к цифровым коммуникациям.[348]

7. *Удаление или ограничение доступа к противоправному контенту* – включает правовые методы и средства ограничения доступа к запрещенной информации или ее удаления. Основные правовые механизмы ограничения доступа к противоправному контенту регламентированы Законом об информации (ст. 10.6, 15.1, 15.1–1, 15.3). Ключевую роль здесь играет Роскомнадзор, который реализует свои функции в данной области через взаимодействие с уполномоченными правоохранительными и иными государственными органами, а также информационными посредниками в лице провайдеров хостинга и операторов связи. Владелец социальной сети ограничивает доступ к противоправному контенту самостоятельно или через взаимодействие с Роскомнадзором.

Следует отметить, что применительно к социальным сетям Закон об информации регулирует лишь процедуру ограничения доступа

[347] *Жарова А. К.* Право и информационные конфликты в информационно-телекоммуникационной сфере. М.: Янус-К, 2016. С. 166–172.

[348] *Наумов И. Б.* Институт идентификации в информационном праве: дис. … д-ра юрид. наук. М., 2020. С. 216–217.

к перечисленным в нем категориям информации, и то только в общих чертах (сам алгоритм ограничения доступа владельцем социальной сети в законе не прописан). К тому же данная норма введена совсем недавно, опыт ее практического применения крайне мал. Однако социальные сети и иные интернет-платформы имеют длительный опыт самостоятельной модерации размещаемого пользователями контента и реагирования на нарушение установленных внутренних правил.

8. *Установление юридической ответственности за правонарушения, посягающие на ИПБ,* – означает правовое закрепление составов правонарушений и мер ответственности за их совершение. Ключевое значение здесь имеют нормы уголовного и административно-деликтного законодательства. Выше при анализе контентных и коммуникационных угроз ИПБ нами было показано большое количество составов преступлений и административных правонарушений, в основе которых лежит оказание деструктивного ИПВ, содержащихся в УК РФ и КоАП РФ. Причем непрерывное расширение спектра таких угроз диктует потребность постоянного дополнения составов правонарушений. Также формой юридической ответственности за правонарушения, посягающие на ИПБ, выступает гражданско-правовая ответственность, регламентируемая ГК РФ.

9. *Правовое регулирование мер контрпропаганды* – означает правовую регламентацию мер контрпропаганды, содержанием которой выступает оказание встречного ИПВ в целях нейтрализации деструктивной информационной активности противника (источника угрозы). В российском информационном законодательстве отсутствуют нормы, комплексно регулирующие данное направление деятельности. Фрагментарное правовое регулирование по данному вопросу имеется в Федеральном законе «О противодействии терроризму» и ряде иных законодательных актов, относящихся к сфере административного права. Этот вопрос будет подробно рассмотрен нами ниже.

10. *Правовое стимулирование развития цифровой грамотности и формирования культуры информационной безопасности* – включает правовые средства, направленные на стимулирование повышения осведомленности граждан о существующих угрозах ИПБ, их источниках и формах проявления, а также правилах безопасного поведения в информационной среде. Концепция информационной безопасности детей 2016 г.[349] в числе приоритетных задач обеспечения информационной безопасности детей закрепила формирование у детей навыков самостоятельного и ответственного потребления информационной продукции и повышение их уровня медиаграмотности. Поскольку

[349] Утв. распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р // Правительство РФ. URL: http://static.government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf (дата обращения: 21.07.2021).

основная роль в повышении цифровой грамотности и формировании культуры информационной безопасности отводится системе образования и институтам гражданского общества, главными задачами государства являются стимулирование и поддержка таких инициатив. Отрадно отметить, что мероприятия по формированию культуры информационной безопасности нашли отражение в Плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 годы.[350]

[350] Приказ Минцифры России от 1 декабря 2020 г. № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 годы» // Вестник образования России. 2021. № 1.

ГЛАВА III. СОСТОЯНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

§ 1. Международно-правовые стандарты в сфере обеспечения информационно-психологической безопасности

Глобальный характер информационных угроз детерминирует необходимость сближения подходов государств и мирового сообщества в целом по противостоянию им. Несмотря на наличие тенденций эрозии и даже кризиса международного права,[351] его нормы и принципы продолжают играть важную роль в регулировании международных отношений и закреплении правовых стандартов для национальных правовых систем.

Международно-правовое регулирование обеспечения ИПБ осуществляется нормами целого ряда отраслей международного права, включая право международной безопасности, международное гуманитарное право, право прав человека, международное уголовное право и др. При этом в международно-правовых актах само понятие ИПБ не используется. Вместо этого говорится об отдельных ее составляющих: защите детей от опасной информации, недопущении разжигания ненависти и вражды, борьбе с распространением детской порнографии и др.

Помимо международных актов, касающихся борьбы с отдельными угрозами ИПБ, мы считаем необходимым уделить внимание анализу норм международных договоров в области прав человека. Это обусловлено самой спецификой ИПБ и деятельности по ее обеспечению, которая непосредственно затрагивает вопросы целого ряда основных прав и свобод человека, включая свободу доступа к информации, свободу массовой информации и ряд иных.

В этой связи ниже проведем исследование релевантных международно-правовых норм, касающихся обеспечения ИПБ, в рамках следующих тематических групп международных актов в сферах: 1) прав человека; 2) СМИ и сети Интернет; 3) борьбы с преступностью и терроризмом в информационном пространстве; 4) международной информационной безопасности.

[351] *Мусаелян Л. А.* Кризис международного права: цивилизационный и геополитические факторы // Вестник Пермского университета. Юридические науки. 2014. Вып. 4. С. 211–225.

Международно-правовые акты в сфере прав человека

Всеобщая декларация прав человека от 10 декабря 1948 г.[352] (далее – Всеобщая декларация) и Международный пакт о гражданских и политических правах от 16 декабря 1966 г.[353] (далее – Международный пакт) в числе основных прав человека закрепляют право на свободу мысли, совести и религии (ст. 18 Всеобщей декларации и Международного пакта), право на свободу убеждений и их свободное выражение (ст. 19 Всеобщей декларации и Международного пакта).

При этом названные международные акты предусматривают допустимость ограничения указанных прав. В качестве правомерных целей ограничения указаны: «обеспечение должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе» (ч. 2 ст. 29 Всеобщей декларации), «охрана общественной безопасности, порядка, здоровья и морали, равно как и основных прав и свобод других лиц» (ч. 3 ст. 18 Международного пакта); «уважение прав и репутации других лиц; охрана государственной безопасности, общественного порядка, здоровья или нравственности населения» (ч. 3 ст. 19 Международного пакта).

Кроме того, в ст. 4 Международного пакта закреплено право государств отступать от своих обязательств во время «чрезвычайного положения в государстве, при котором жизнь нации находится под угрозой» (институт дерогации).[354] Для России это означает возможность введения дополнительных правовых ограничений в условиях особых правовых режимов чрезвычайного и военного положения.[355] Ограничение основных прав допускается «в такой степени, в какой это требуется остротой положения, при условии, что такие меры не являются несовместимыми с их другими обязательствами по международному праву и не влекут за собой дискриминации…».

Международный пакт содержит ряд ограничений свободы выражения мнения. Согласно ст. 20 данного акта «всякая пропаганда войны», а также «всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию» должны быть запрещены законом. Схожие правовые запреты закреплены и в других международно-правовых актах, в частности

---

[352] Международное право в документах: учебное пособие / Сост. Н. Т. Блатова, Г. М. Мелков. 4-е изд., перераб. и доп. М., 2003. С. 101–107.

[353] Сборник действующих договоров, соглашений и конвенций, заключенных с иностранными государствами. М., 1978. Вып. XXXII. С. 44.

[354] *Султанов А. Р.* Ограничение прав человека в международном праве (право на дерогацию) // Евразийский юридический журнал. 2008. № 3 (5). URL: http://www.eurasialaw.ru/index.php?option=com_content&view=article&id=3660:2012–12–18–05–49–02&catid=316:2012–12–18–05–36–05 (дата обращения: 27.03.2013).

[355] См.: *Пчелинцев С. В.* Проблемы ограничения прав и свобод граждан в условиях особых правовых режимов: монография. М.: Норма, 2006.

в отношении «прямого и публичного подстрекательства к совершению геноцида» (п. «с» ст. III Конвенции о предупреждении преступления геноцида и наказании за него от 9 декабря 1948 г.),[356] «поощрения преступления апартеида» (п. «б» ст. III Международной конвенции о пресечении преступления апартеида и наказании за него от 30 ноября 1973 г.),[357] «поощрения расовой дискриминации» (ст. 4 Международной конвенции о ликвидации всех форм расовой дискриминации от 30 ноября 1973 г.).[358]

Схожие международные стандарты содержатся в региональных международно-правовых актах о правах человека, в частности в Конвенции СНГ о правах и основных свободах человека от 26 мая 1995 г.[359] и Европейской конвенции о защите прав человека и основных свобод от 4 ноября 1950 г. (далее – ЕКПЧ).

Конвенция СНГ о правах и основных свободах человека во многом воспроизводит подходы Международного пакта в части правового регулирования оснований и порядка ограничения прав на свободу мысли, совести и религии (ст. 10), на свободное выражение своего мнения (ст. 11), на свободу ассоциаций с другими (ст. 12).

Нормы ЕКПЧ также гарантируют свободу мысли, совести и религии, свободу выражения мнения, но допускают возможность их ограничения. При этом несколько расширен перечень правомерных целей такого ограничения.

В Рекомендации Комитета министров Совета Европы (далее – КМСЕ) № 5 (2016) от 13 апреля 2016 г. «О свободе в Интернете»[360] прямо указано на применимость норм ЕКПЧ к онлайну и закреплена обязанность государств-членов «соблюдать, охранять и обеспечивать права человека и основные свободы в Интернете». Интернет-свобода определяется в Рекомендациях как осуществление в Интернете прав человека и основных свобод, а также их защита в соответствии с ЕКПЧ и Международным пактом. В приложении к Рекомендациям подтверждено действие критериев допустимости ограничений основных прав, предусмотренных ст. 10 ЕКПЧ, в отношении мер по блокированию или ограничению доступа к интернет-платформам или информационным и коммуникационным технологическим средствам, блокировке, установлению фильтров или изъятию интернет-контента.

Допустимость ограничения свободы выражения мнения в соответствии с ч. 2 ст. 10 ЕКПЧ многократно была подтверждена в судебной практике Европейского суда по правам человека (далее – ЕСПЧ). Предметом контроля ЕСПЧ является выполнение базовых критериев

[356] Международная защита прав и свобод человека: сборник документов. М., 1990. С. 103–109.
[357] Там же. С. 98–103.
[358] Там же. С. 125–139.
[359] Бюллетень международных договоров. 1999. № 6.
[360] СПС «КонсультантПлюс».

допустимости ее ограничения, включая: законность цели, закрепленность нормами закона, необходимость в демократическом обществе и пропорциональность.[361]

ЕСПЧ рассмотрел большое количество жалоб о злоупотреблении свободой самовыражения путем распространения непристойных сведений. При этом суд признал правомерным введение государством ограничений на распространение информации и идей для защиты нравственности, благополучия других лиц и в иных легитимных целях. Особенно подчеркивалась обоснованность принятия мер по охране уязвимых групп населения, прежде всего детей, в интересах «защиты нравственности».[362] То есть Европейский суд признал правомерность реализации странами мер по защите несовершеннолетних и иных уязвимых категорий лиц от негативной информации. Парламентская ассамблея Совета Европы (далее – ПАСЕ) в своей рекомендации указала на признание данного правила «в новом технологическом измерении информационного и коммуникационного обмена», включая сеть Интернет.[363]

Права детей регламентируются специальными конвенциями и иными международно-правовыми актами. Главным международным договором в данной сфере выступает Конвенция о правах ребенка от 20 ноября 1989 г.[364] (далее – Конвенция о правах ребенка). Конвенция исходит из принципа наилучшего обеспечения интересов ребенка и обязанности государств обеспечить ребенку необходимую защиту и заботу (ч. 1 и 2 ст. 3), закрепляет правовые гарантии и особенности правоспособности и дееспособности ребенка в части права на свободу выражения мнения, свободы мысли, совести и религии, а также устанавливает возможность их ограничения (ст. 12–14).

Отдельное внимание в Конвенции о правах ребенка уделено взаимодействию детей со СМИ. Согласно Конвенции государства обязаны предоставить ребенку доступ к информации из различных источников, прежде всего к материалам, содействующим благополучию и развитию ребенка, одновременно защитив детей от «информации и материалов, наносящих вред его благополучию» (п. «е» ст. 17).

---

[361] Свобода выражения мнения в Интернете. Отчет представителя по вопросам СМИ ОБСЕ Д. Миятовича. ОБСЕ, 2011. С. 14.

[362] Постановления ЕСПЧ: Даджен (Dudgeon) против Соединенного Королевства; Институт Отто-Премингер (Otto-Preminger-Institut) против Австрии; Уингроу (Wingrove) против Соединенного Королевства и др. См.: *Косевич Н. Р.* Защита прав детей в практике Европейского суда по правам человека // СПС «КонсультантПлюс».

[363] Рекомендация Парламентской ассамблеи Совета Европы № 1882 (2009) от 28 сентября 2009 г. «Продвижение интернет- и онлайновых ресурсов, безопасных для несовершеннолетних» // Парламентская ассамблея Совета Европы. URL: https://www.coe.int/T/r/Parliamentary_Assembly/[Russian_documents]/[2009]/[SepOct2009]/Rec1882_rus.asp (дата обращения: 03.03.2021).

[364] Сборник международных договоров СССР. Выпуск XLVI. 1993.

Кроме того, Конвенция о правах ребенка устанавливает обязанность государств по реализации комплекса необходимых мер «с целью защиты ребенка от всех форм физического или психологического насилия, оскорбления или злоупотребления…». Особое внимание в документе уделяется защите детей от сексуальной эксплуатации и сексуального совращения. В этих целях государства-участники принимают необходимые меры для предотвращения: а) склонения или принуждения ребенка к любой незаконной сексуальной деятельности; б) использования в целях эксплуатации детей в проституции или в другой незаконной сексуальной практике; в) использования в целях эксплуатации детей в порнографии и порнографических материалах (ст. 34).

Широкий комплекс правовых мер защиты прав детей в цифровой среде предусмотрен в Рекомендациях КМСЕ № 7 (2018) от 4 июля 2018 г. «О соблюдении, защите и осуществлении прав детей в цифровой среде».[365] В документе закреплено обязательство государств гарантировать и обеспечить реализацию полного объема прав ребенка в цифровой среде. В качестве мер правовой защиты таких прав и обеспечения безопасности детей в Рекомендациях установлены: а) регулярная оценка любых рисков причинения вреда, которые новые технологии могут представлять для здоровья детей; б) стимулирование внедрениями коммерческими предприятиями средств и методов обеспечения безопасности детей, включая системы родительского контроля и противодействия запугиванию и иным формам деструктивной коммуникации; в) использование эффективных систем подтверждения возраста; г) принятие мер по защите детей от коммерческой и сексуальной эксплуатации в цифровой среде; д) защита неприкосновенности частной жизни детей и их персональных данных; е) повышение осведомленности и цифровой грамотности детей, родителей и педагогов; ж) стимулирование создания высококачественного и полезного для детей контента и онлайн-услуг. Также Рекомендации предписывают государствам гарантировать использование эффективных мер защиты нарушенных прав детей.

Международные акты в области СМИ и сети Интернет

Международно-правовые акты данной группы регулируют технические и содержательные аспекты распространения массовой информации.[366] При этом в международном праве в области массовой информации до настоящего времени отсутствует базовый универсальный международный договор.

В плане регулирования контента СМИ первостепенное значение имеют нормы международных документов о правах человека,

[365] СПС «КонсультантПлюс».

[366] *Колосов Ю. М., Петров В. О.* Международное право массовой информации // Международное право: учебник / Отв. ред. А. Н. Вылегжанин. М.: Высшее образование, Юрайт-Издат, 2009. С. 779.

гарантирующие право на свободу убеждений и на свободное их выражение, включая свободу искать, получать и распространять информацию и идеи любыми способами и независимо от государственных границ. Свобода массовой информации оценивается как форма реализации свободы самовыражения. Соответственно, в отношении нее применимы нормы о допустимости правовых ограничений и правовые запреты пропаганды международных преступлений. Последние аспекты подробно освещены в отдельной Декларации, принятой Генеральной конференцией ЮНЕСКО.[367]

Ряд важных международно-правовых актов в сфере свободы массовой информации принят в рамках Совета Европы.[368] К их числу относятся Декларация о средствах массовой информации и правах человека от 23 января 1970 г.[369] и Декларация о свободе выражения мнения и информации от 29 апреля 1982 г.[370] Подтверждая гарантии свободы и независимости СМИ, включая запрет прямой или косвенной цензуры, данные документы устанавливают ряд требований к СМИ, включая выполнение своих задач с ощущением социальной ответственности. Для этой цели рекомендуется *принятие кодексов профессиональной этики для журналистов*, в которых должны содержаться принципы, связанные с распространением достоверной информации, разделением самой информации и комментариев, недопустимостью клеветы, а также соблюдением неприкосновенности частной жизни. Для контроля выполнения данных правил и рассмотрения возникающих споров предписано учреждение *советов по печати*.

Помимо деклараций, носящих рекомендательный характер, на уровне Совета Европы принята юридически обязательная Европейская конвенция о трансграничном телевидении от 5 мая 1989 г.[371] (далее – ЕКТТ). В ней содержится ряд важных норм, касающихся ИПБ. Так, согласно ст. 7 ЕКТТ, «программы в целом, их представление и содержание

---

[367] 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 // Права человека: сборник международных договоров. Т. 1 (часть первая): Универсальные договоры. Организация Объединенных Наций. Нью-Йорк и Женева, 1994.

[368] Freedom of Expression and the Media: Standard-setting by the Council of Europe. (I) Committee of Ministers. (II) Parliamentary Assembly. Susanne Nikoltchev & Tarlach McGonagle (Eds.), European Audiovisual Observatory. Strasbourg, 2011; Recommendations and Declarations of the Committee of Ministers of the Council of Europe in the field of media and information society. Strasbourg, July 2015.

[369] Собрание актов Президента и Правительства РФ. 1993. № 15. Ст. 1338.

[370] Совет Европы и Россия. Сборник документов. М.: Юридическая литература, 2004. С. 679–680.

[371] Текст Конвенции изменен в соответствии с положениями Протокола (СЕД № 171) с даты вступления его в силу 1 марта 2002 г. Совет Европы. URL: http://conventions.coe.int/Treaty/rus/Treaties/Html/132.htm (дата обращения: 24.10.2020).

должны обеспечивать уважение к достоинству человеческой личности и основным правам других людей. В частности, они не должны: а) быть непристойными и, в особенности, содержать порнографию; б) чрезмерно выделять насилие и способствовать расовой ненависти» (ч. 1 ст. 7). Отдельная норма ЕКТТ закрепляет принцип «временного водораздела» в интересах защиты детей: «Все программы, которые могут нанести вред физическому, умственному или нравственному развитию детей и подростков, не должны транслироваться в тот период времени, когда они могут их смотреть» (ч. 2 ст. 7). Также в конвенции содержится комплекс требований и ограничений применительно к рекламе в интересах защиты телезрителей (ст. 11–15). Рассматриваемая конвенция подписана Россией в 2006 г., но не ратифицирована до настоящего времени.

Важное значение в контексте исследуемой проблематики имеют рекомендации КМСЕ, касающиеся распространения негативной информации в СМИ: № 7 (89) от 27 апреля 1989 г. относительно принципов распространения видеозаписей, содержащих насилие, жестокость или имеющих порнографическое содержание,[372] и № 19 (97) от 20 октября 1997 г. о демонстрации насилия в электронных средствах массовой информации.[373] В них закреплены следующие правовые механизмы обеспечения ИПБ: а) принятие кодексов поведения и иных актов саморегулирования; б) применение механизмов классификации и маркировки контента; в) введение правовых запретов и ограничений на распространение негативной информации; г) контроль правил распространения контента и применение в случае нарушения мер юридической ответственности; д) информирование общества о возможной опасности информации.

В Рекомендациях о демонстрации насилия в электронных СМИ основная ответственность за контроль над содержанием информации в СМИ возлагается на их редакции. Также подчеркивается важное значение общественного контроля в данной сфере. На родителей и учителей возлагается ответственность за формирование у детей фильтров критического восприятия образов насилия путем медиаобучения, за применение инструментов и методов ограничений доступа детей к негативному контенту.

В связи с постоянно возрастающей ролью Интернета предпринимаются попытки международно-правового регулирования отношений, связанных с его использованием, включая вопросы безопасности. Однако такое регулирование до сих пор находится на достаточно низком уровне. До настоящего времени практически отсутствуют императивные международные договоры в данной сфере, что отчасти компенсируется принятием международно-правовых актов рекомендательного характера. К числу

[372] Совет Европы. URL: https://rm.coe.int/native/090000168077c477 (дата обращения: 12.03.2021).

[373] Совет Европы и Россия. Сборник документов. М.: Юридическая литература, 2004. С. 851–859.

последних относятся такие значимые документы, как Окинавская хартия глобального информационного общества от 22 июля 2000 г.,[374] Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» от 12 декабря 2003 г.[375] и ряд иных.

В данных политико-декларативных международных актах подчеркивается важность создания безопасного киберпространства. Для этого рекомендуется распространение этических принципов на поведение в киберпространстве и формирование глобальной культуры кибербезопасности.

Целый блок значимых международно-правовых актов, касающихся обеспечения безопасности в Интернете, принят в Совете Европы. Одним из них является Декларация о свободе обмена информацией в Интернете от 28 мая 2003 г. (далее – Декларация о свободе Интернета). В данном документе закреплена идея нахождения баланса между частными и публичными интересами, с одной стороны, и свободой оборота информации в сети, с другой. Декларация о свободе Интернета закрепляет либеральную модель регулирования обмена информацией в Интернете, что выражается в лимитировании государственного вмешательства в данные процессы, акценте на саморегулировании при признании роли государственного регулирования, а также в ограничении ответственности информационных посредников за содержание распространяемой в сети информации. Вместе с тем документ предусматривает право национальных властей принимать специальные меры по защите детей в онлайн-пространстве и блокировке противоправного контента.

В рекомендациях КМСЕ № 8 (2001) от 5 сентября 2001 г. о вопросах саморегулирования виртуального содержания[376] и № 5 (2009) от 8 июля 2009 г. о мерах по защите детей от пагубного влияния недопустимого интернет-контента и обеспечения их активного участия в новой информационной и коммуникационной среде,[377] а также в Рекомендации ПАСЕ № 1882 (2009) от 28 сентября 2009 г. «Продвижение интернет- и онлайновых ресурсов, безопасных для несовершеннолетних»[378] предусмотрены следующие правовые механизмы обеспечения ИПБ в сети Интернет: а) создание само-

[374] Дипломатический вестник. 2000. № 8. С. 51–56.

[375] Международный союз электросвязи. URL: http://www.itu.int/wsis/outcome/booklet/declaration_Bru.html (дата обращения: 11.01.2013).

[376] Совет Европы и Россия. Сборник документов. М.: Юридическая литература, 2004. С. 877–881.

[377] Council of Europe URL: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2009–5-of-the-committee-of-ministers-to-member-states-on-measures-to-protect-children-against-harmful-content-and-behaviour-and-?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/ (дата обращения: 27.07.2021).

[378] Парламентская ассамблея Совета Европы. URL: https://www.coe.int/T/r/Parliamentary_Assembly/%5BRussian_documents%5D/%5B2009%5D/%5BSepOct2009%5D/Rec1882_rus.asp (дата обращения: 24.06.2021).

регулируемых организаций, представляющих интернет-отрасль, которые должны вырабатывать собственные регулятивные механизмы (кодексы поведения и т. п.), а также активно вовлекаться в законотворческий процесс; б) поощрение государствами определения признаков вредного содержания новых информационных и коммуникационных услуг (в частности, насилие, порнография, поощрение потребления табака, алкоголя, азартных игр и др.); в) маркировка контента, позволяющая пользователям распознать и фильтровать вредный контент независимо от его происхождения[379]; г) содействие развитию систем фильтрации контента и иных инструментов безопасности пользователей, применению фильтров пользователями и провайдерами интернет-услуг[380]; д) поощрение применения инструментов ограничения доступа детей к вредному контенту, включая системы проверки возраста, личных идентификационных кодов, паролей, шифрования и декодирования, карт с электронным кодом; е) создание сетевых пространств и ресурсов, безопасных для детей; ж) учреждение провайдерами и государственными органами механизма приема и рассмотрения жалоб на вредный контент; з) информирование и повышение осведомленности интернет-пользователей, в том числе посредством целевых общественных кампаний и школьного обучения.

КМСЕ принял ряд рекомендаций, адресованных отдельным провайдерам интернет-услуг, в частности поисковым системам[381] и сервисам социальных сетей.[382] В них также подчеркивается значимость развития медиаграмотности и механизмов саморегулирования и сорегулирования в интересах безопасности пользователей, а также необходимость использования настроек и иных инструментов их защиты от цифровых угроз. В Рекомендации № 4 (2012) отдельное внимание уделяется защите детей от контентных и коммуникационных угроз, включая кибербуллинг и кибергруминг.

В 2018 г. КМСЕ принял Рекомендацию о роли и ответственности интернет-посредников.[383] В документе большое внимание уделено ограничению доступа к контенту. Установлено, что блокировка и удаление контента

[379] В Рекомендации № 1882 содержалась ссылка к системе рейтингов, установленных Ассоциацией оценки интернет-контента ICRA (Internet Content Rating Association). Однако, как отмечалось в обзоре РАЭК, система возрастной маркировки интернет-страниц была признана в Европе неэффективной, и от нее в итоге отказались. См.: Международный опыт охраны детей в Интернете. Аналитический отчет. РАЭК, 2011. С. 5–6.

[380] В отношении интернет-фильтров имеется специальная Рекомендация Комитета министров Совета Европы № 6 (2008) от 26 марта 2008 г. о мерах по развитию уважения к свободе выражения мнения и информации в связи с интернет-фильтрами.

[381] Рекомендация Комитета министров Советы Европы № 3 (2012) от 4 апреля 2012 г. к государствам-членам о защите прав человека применительно к поисковым системам // СПС «КонсультантПлюс».

[382] Рекомендация Комитета министров Советы Европы № 4 (2012) от 4 апреля 2012 г. «О защите прав человека применительно к сервисам социальных сетей» // СПС «КонсультантПлюс».

[383] Рекомендация Комитета министров Советы Европы № 2 (2018) от 7 марта 2018 г. «О роли и ответственности интернет-посредников» // СПС «КонсультантПлюс».

могут применяться интернет-посредниками на основании как предписаний государственных органов, так и своих внутренних правил. Рекомендация фактически запрещает государствам возлагать на интернет-посредников обязанность мониторинга стороннего контента («контента третьего лица»), к которому они обеспечивают доступ, передают или хранят, и ограничивает их ответственность за такой контент. Это, в свою очередь, не исключает ответственности посредников в отношении противоправного контента в случае, если они своевременно не приняли мер ограничения доступа к нему, в том числе при получении уведомления. В отношении мер модерации контента, применяемых самими интернет-посредниками, в Рекомендации закреплены требования транспарентности и соблюдения прав человека. Также в документе содержатся требования о прохождении специальной правовой подготовки персоналом, участвующим в модерации контента.

Международные акты в области борьбы с преступностью и терроризмом в информационном пространстве

Проблематика борьбы с киберпреступностью находится в фокусе внимания международного сообщества как одно из приоритетных направлений противодействия угрозам цифровой среды. Борьбе с киберпреступностью посвящены специальные резолюции Генеральной ассамблеи ООН A/55/63[384] и A/RES/56/121[385] «Борьба с преступным использованием информационных технологий», A/73/187[386] и A/74/247[387] «Противодействие использованию информационно-коммуникационных технологий в преступных целях».

До настоящего времени отсутствует универсальный международный договор, который регламентировал бы сферу борьбы с киберпреступностью. В 2017 г. Российская Федерация представила в ООН первый проект Конвенции о сотрудничестве в сфере противодействия информационной преступности.[388] В 2019 г. по инициативе нашей страны был

[384] Резолюция Генеральной ассамблеи ООН A/55/63 от 4 декабря 2000 г. «Борьба с преступным использованием информационных технологий» // Организация Объединенных Наций. URL: http://www.un.org/ru/documents/ods.asp?m=A/RES/55/63 (дата обращения: 23.04.2021).

[385] Резолюция Генеральной ассамблеи ООН A/56/121 от 19 декабря 2001 г. «Борьба с преступным использованием информационных технологий» // Организация Объединенных Наций. URL: http://www.un.org/ru/documents/ods.asp?m=A/RES/56/121 (дата обращения: 23.04.2021).

[386] Резолюция Генеральной ассамблеи ООН A/73/187 от 17 декабря 2018 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Организация Объединенных Наций. URL: https://undocs.org/ru/A/RES/73/187 (дата обращения: 23.04.2021).

[387] Резолюция Генеральной ассамблеи ООН A/74/247 от 27 декабря 2019 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Организация Объединенных Наций. URL: https://undocs.org/pdf?symbol=ru/A/Res/74/247 (дата обращения: 23.04.2021).

[388] Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности A/C.3/72/12 от 17 октября

учрежден специальный комитет ООН для разработки всеобъемлющей международной конвенции, и уже через два года Россия внесла в него проект Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях[389] (далее – Проект Конвенции ООН об информационной преступности). Работу над данным проектом планируется завершить в 2023 г.

Наиболее авторитетным региональным международным договором в области борьбы с киберпреступностью выступает Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г.[390] (далее – Конвенция о киберпреступности). По состоянию на февраль 2022 г. ее участниками являются 66 государств, причем среди них не только страны – члены Совета Европы, но и государства Северной и Латинской Америки, Африки и Азии.[391] Россия не ратифицировала данную конвенцию из-за неприемлемости норм о трансграничном доступе к компьютерным данным без уведомления и согласия государства.

Позже были приняты Дополнительный протокол в отношении криминализации деяний расистского и ксенофобского характера, совершаемых при помощи компьютерных систем, от 28 января 2003 г.[392] (далее – Дополнительный протокол к Конвенции о киберпреступности) и Второй протокол, касающийся расширения сотрудничества и раскрытия электронных доказательств, от 17 ноября 2021 г.[393] Данные акты определяют составы киберпреступлений, процессуальные аспекты борьбы с ними, регламентируют установление юрисдикции и международное сотрудничество в борьбе с киберпреступностью.

К сфере ИПБ относятся прежде всего *преступления, связанные с детской порнографией* (ст. 9 Конвенции о киберпреступности). Следует отметить, что детская порнография, производство и оборот которой является киберпреступлением, рассматривается в международных

2021 г. // Организация Объединенных Наций. URL: https://undocs.org/ru/A/C.3/72/12 (дата обращения: 05.04.2021).

[389] О внесении в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях // МИД России. 28.07.2021. URL: https://archive.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4831832 (дата обращения: 27.09.2021).

[390] Convention on Cybercrime. Budapest, 23.XI.2001 (ETS – No. 185) // Council of Europe. URL: https://rm.coe.int/1680081561 (дата обращения: 06.02.2022).

[391] Chart of signatures and ratifications of Treaty 185 // Council of Europe. Status as of 06/02/2022 URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (дата обращения: 06.02.2022).

[392] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Strasbourg, 28.I.2003 (ETS No. 189) // Council of Europe. URL: https://rm.coe.int/168008160f (дата обращения: 06.02.2022).

[393] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence Council of Europe. URL: https://rm.coe.int/1680a49dab (дата обращения: 06.02.2022).

актах и с другой позиции – как форма сексуальной эксплуатации детей. В таком качестве она нашла свое отражение в Факультативном протоколе к Конвенции о правах ребенка, касающемся торговли детьми, детской проституции и детской порнографии, от 25 мая 2000 г.[394] (далее – Факультативный договор) и Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений от 25 октября 2007 г.[395] (далее – Конвенция о защите детей).

Данными международными договорами закреплена обязанность государств осуществить криминализацию изготовления и оборота детской порнографии, кибергруминга («приставание к детям с сексуальными целями) и иных преступлений, связанных с использованием ИКТ в целях сексуальной эксплуатации, установить серьезные меры наказания за их совершение для физических лиц, а также ответственность юридических лиц. Кроме того, предусмотрено установление государствами запрета производства и распространения материалов, пропагандирующих такие преступления (ч. 5 ст. 9 Факультативного протокола, ч. 2 ст. 8 Конвенции о защите детей).

Основная часть указанных международных договоров посвящена уголовно-процессуальным вопросам, которые находятся за рамками предмета нашего исследования. Больший интерес представляют нормы, закрепляющие иные меры противодействия детской порнографии и сексуальной эксплуатации детей, включая: а) мероприятия, направленные на повышение осведомленности об угрозе, способах предотвращения и реагирования на нее (ч. 2 ст. 9 Факультативного протокола, ст. 5 и 6 Конвенции о защите детей); б) организацию линий помощи по телефону и через Интернет (ст. 13 Конвенции о защите детей); в) создание специальных механизмов мониторинга и координационных центров для сбора данных в целях наблюдения и оценки феномена сексуальной эксплуатации и сексуального насилия над детьми, включая детскую порнографию (п. «b» ч. 2 ст. 10 Конвенции о защите детей); г) защиту частной жизни и личности детей – жертв преступлений посредством принятия мер по запрету публичного распространения информации, которая могла бы привести к их идентификации (п. «e» ч. 1 ст. 8 Факультативного протокола, п. «e» ч. 1 ст. 31 Конвенции о защите детей).

Протокол к Конвенции о киберпреступности предусматривает криминализацию в законодательстве государств деяний, связанных с распространением расистских и ксенофобских материалов посредством компьютерных систем, угрозами и оскорблениями расистского характера, одобрением или оправданием геноцида и иных преступлений

[394] Организация Объединенных Наций: официальный сайт. URL: http://www.un.org/ru/documents/decl_conv/conventions/rightschild_protocol2.shtml (дата обращения: 14 июня 2021 г.).

[395] Бюллетень международных договоров. 2014. № 6.

против человечества. Как видно, перечисленные деяния охватывают и контентные, и коммуникационные угрозы ИПБ.

В российском проекте Конвенции ООН об информационной преступности 2021 г., помимо традиционного состава преступления, связанного с изготовлением и оборотом детской порнографии (ст. 15), закреплено и множество новых для международного права составов преступлений, в основе которых лежит оказание деструктивного ИПВ, включая: а) склонение к самоубийству или доведение до его совершения (ст. 16); б) преступления, связанные с вовлечением несовершеннолетних в совершение противоправных действий, опасных для их жизни и здоровья (ст. 17); в) создание и использование цифровой информации для введения пользователя в заблуждение (ст. 18); г) подстрекательство к подрывной или вооруженной деятельности (ст. 19) и др. Они отражают опыт развития российского уголовного законодательства последнего десятилетия.

Анализируя положения международных актов, касающихся терроризма в информационном пространстве, следует отметить, что они затрагивают аспекты использования возможностей СМИ и Интернета в деятельности террористических организаций. В контексте темы нашего исследования нас интересуют вопросы пропаганды идеологии терроризма и иные формы деструктивного ИПВ со стороны экстремистских элементов.

Один из комплексных универсальных международных актов в данной области – Глобальная контртеррористическая стратегия ООН, принятая резолюцией A/RES/60/288 Генеральной ассамблеи от 8 сентября 2006 г.,[396] – 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.

В региональных международных договорах по борьбе с терроризмом – Конвенции Совета Европы о предупреждении терроризма от 16 мая 2005 г.,[397] Договоре о сотрудничестве государств – участников СНГ в борьбе с терроризмом от 4 июня 1999 г.,[398] Шанхайской Конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом (г. Шанхай, 15 июня 2001 г.)[399] – преимущественно регулируется международное сотрудничество государств в борьбе с терроризмом, включая вопросы взаимодействия и информационного обмена при выявлении, раскрытии и расследовании преступлений террористического характера. Конвенция

[396] Организация Объединенных Наций. URL: https://undocs.org/ru/A/RES/60/288 (дата обращения: 03.04.2021).

[397] Бюллетень международных договоров. 2009. № 9.

[398] Там же.

[399] Бюллетень международных договоров. 2004. № 1.

Совета Европы также предусматривает национальные обязательства стран в данной сфере, включая принятие мер по предупреждению террористических преступлений (ст. 3), а также их криминализации в национальном законодательстве (ст. 5–7). В их числе – публичное подстрекательство к терроризму и вербовка (ст. 5 и 6).

Отдельно необходимо выделить Конвенцию ШОС по противодействию экстремизму от 9 июня 2017 г.[400] (далее – Конвенция ШОС). В документе большое внимание уделяется борьбе с проявлениями экстремизма в информационном пространстве. Так, в числе мер на национальном уровне в Конвенции названы: а) мониторинг СМИ и сети Интернет в целях своевременного выявления и пресечения распространения экстремистской идеологии; б) усиление пропагандистской деятельности по противодействию экстремизму и контрпропагандистской работы против распространения экстремистской идеологии; в) ограничение доступа к экстремистскому контенту в информационно-телекоммуникационных сетях.

Вопросам деятельности СМИ по освещению терроризма посвящены Рекомендация ПАСЕ № 1706 (2005) «СМИ и терроризм» и Декларация о свободе выражения мнений и информации в СМИ в контексте борьбы с терроризмом от 2 марта 2005 г., принятая КМСЕ. Основные положения данных документов подробно проанализированы нами в научной статье.[401] Ими предусматривается комплекс мер, касающихся обеспечения ИПБ, включая: а) выработку правил освещения террористических актов журналистами и закрепление их в кодексах поведения; б) соблюдение ограничений на распространение определенных видов информации, травмирующей психику, усиливающих социальную напряженность либо создающих угрозу для безопасности граждан; в) дополнение школьной программы курсами медийной грамотности.

В завершение данного подраздела отметим еще один документ рекомендательного характера – Всеобъемлющую международную рамочную стратегию противодействия распространению террористических идей.[402] В данном акте изложены основные рекомендации по борьбе с террористической пропагандой, в том числе в Интернете. Особое внимание при этом уделено контрпропаганде.

Международно-правовые акты в сфере международной информационной безопасности

---

[400] Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102574570&backlink=1&&nd=102632751 (дата обращения: 14.02.2021).

[401] *Смирнов А. А.* Европейские стандарты правового регулирования освещения терроризма в СМИ // Административное право и процесс. 2014. № 1. С. 71–74.

[402] Приложение к письму Председателя Комитета Совета безопасности, учрежденного резолюцией 1373 (2001) о борьбе с терроризмом, от 26 апреля 2017 г. на имя Председателя Совета безопасности S/2017/375.

Международная информационная безопасность (далее – МИБ) устойчиво вошла в повестку работы ведущих международных организаций как один из важных аспектов международной безопасности. Генеральной ассамблеей ООН начиная с 1998 г. был принят целый ряд резолюций под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности».[403] Россия сыграла ключевую роль в продвижении вопросов МИБ в повестку международных организаций.[404] При этом наша страна придерживается широкого подхода к пониманию информационной безопасности, включая в него как информационно-технические, так и социогуманитарные, политико-идеологические аспекты.[405]

В дальнейшем был принят ряд важных международных договоров глобального, регионального и двустороннего уровней, образующих отдельную составляющую системы правового регулирования обеспечения информационной безопасности.[406] К ним, в частности, относится Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г.[407] (далее – Соглашение ШОС в области МИБ). Ранее, в 2011 г., Россией представлена концепция Конвенции об обеспечении международной информационной безопасности (далее – концепция Конвенции МИБ), а в 2021 г. подготовлена ее новая редакция. В настоящее время действует уже второе поколение Основ государственной политики Российской Федерации в области международной информационной безопасности[408] (далее – Основы ГП в области МИБ).

Согласно Основам ГП в области МИБ международная информационная безопасность определяется как «состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного

---

[403] Резолюция Генеральной ассамблеи ООН A/RES/53/70 от 4 декабря 1998 г. и последующие резолюции. См.: Международная информационная безопасность: Теория и практика. В 3 т. Т. 2: Сборник документов (на русском языке) / Под общ. ред. А. В. Крутских. 2-е изд., доп. М.: Издательство «Аспект Пресс», 2021. С. 257–313.

[404] См.: Вступительное слово Секретаря Совета безопасности Российской Федерации Н. П. Патрушева // Международная информационная безопасность: Теория и практика. В 3 т. Т. 1: Учебник для вузов / Под общ. ред. А. В. Крутских. 2-е изд., доп. М.: Издательство «Аспект Пресс», 2021. С. 11.

[405] *Зиновьева Е. С.* Международная информационная безопасность: монография. М.: МГИМО-университет, 2013. С. 54–55.

[406] Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. д. ю. н., профессора Т. А. Поляковой. Саратов: Амирит, 2020. С. 39.

[407] Бюллетень международных договоров. 2012. № 2.

[408] Основы государственной политики Российской Федерации в области международной информационной безопасности (утв. Указом Президента РФ от 12 апреля 2021 г. № 21) // СЗ РФ. 2021. № 16. Ст. 274.

партнерства обеспечивается поддержание международного мира, безопасности и стабильности» (п. 6).

Угрозы ИПБ просматриваются в перечне основных угроз МИБ, закрепленных в указанных международных актах и Основах ГП в области МИБ. В Соглашении ШОС в области МИБ отдельно выделена угроза «распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств». Кроме того, психологическая компонента имплицитно присутствует и в таких обозначенных в данном Соглашении угрозах, как информационная война, информационный терроризм и информационная преступность. Схожий перечень угроз содержится в Основах ГП в области МИБ. В новой редакции концепции Конвенции МИБ среди угроз МИБ также выделены подрывная пропаганда и распространение фейковой информации, относящиеся к интересующей нас сфере ИПБ.

Соглашение ШОС в области МИБ определяет вполне традиционные для международных договоров направления межгосударственного сотрудничества в области МИБ, включая выработку и реализацию совместных мер, создание системы мониторинга и совместного реагирования на информационные угрозы, развитие норм международного права в области ограничения распространения и применения информационного оружия, обмен опытом и подготовку специалистов и др.

Концепция Конвенции МИБ в качестве своей стратегической цели называет содействие формированию системы МИБ. Для ее реализации в документе закреплены основные принципы обеспечения МИБ и ключевые направления ее обеспечения, в том числе: предотвращение конфликтов в информационном пространстве, противодействие использованию ИКТ в террористических и преступных целях, а также меры укрепления доверия в области МИБ. В рамках этих направлений закреплен ряд правовых мер обеспечения МИБ, касающихся сферы ИПБ, в частности запрет использования ИКТ для вмешательства во внутренние дела государств и противодействие распространению недостоверной или искаженной информации. В остальном в документе содержатся традиционные меры международного сотрудничества, включая совершенствование договорно-правовой базы и национального законодательства, реализацию совместных программ и планов, обмен информацией и координацию действий, обмен опытом и т. д.

В Основах ГП в области МИБ предусмотрен широкий перечень направлений реализации государственной политики по развитию сотрудничества России с иностранными государствами на глобальном, многостороннем и двустороннем уровнях. Он включает в себя: а) содействие принятию на универсальном уровне Конвенции МИБ; б) организацию под эгидой ООН регулярного институционального диалога; в) содействие выработке новых

принципов и норм международного права, регулирующих деятельность государств в глобальном информационном пространстве; г) развитие сотрудничества в области МИБ на двусторонней и многосторонней основе, а также в форматах СНГ, БРИКС, ОДКБ, АСЕАН, G-20 и другие направления.

Развитие правового регулирования обеспечения ИПБ в рамках правового поля МИБ представляется нам весьма значимым, поскольку трансграничный характер многих информационных угроз обуславливает необходимость тесного международного сотрудничества для эффективного противодействия им. При этом мы поддерживаем включение вопросов обеспечения ИПБ в общую предметную повестку МИБ и продвижение подходов Российской Федерации на международной арене, в том числе содействие принятию Конвенции МИБ. Полагаем, что ее принятие в рамках ООН заложило бы фундамент для международно-правового регулирования в сфере МИБ на глобальном уровне, который можно развивать на региональном уровне и (или) по отдельным направлениям обеспечения МИБ, включая психологические аспекты (ИПБ).

§ 2. Зарубежный опыт правового обеспечения информационно-психологической безопасности

Потребности формирования и развития эффективной системы правового обеспечения информационно-психологической безопасности в Российской Федерации обуславливают необходимость изучения и критического переосмысления зарубежного опыта в данной сфере. Важно выделить положительный опыт правового регулирования в зарубежных государствах и оценить его применимость в российских реалиях. Для этого нами будет использован инструментарий сравнительно-правового анализа.

Основное внимание автор уделяет анализу законодательного регулирования европейских стран и США, где оно имеет долгую историю и высокий уровень развития. Поскольку наиболее развитые страны Европы входят в настоящий момент в состав Евросоюза, то нами будет проанализировано законодательство ЕС в рассматриваемой области, которое освещается в его системной связи с правовыми актами стран-членов. Хотя такое регулирование имеет международно-правовые черты, некоторые акты ЕС носят характер наднациональных и обладают прямым действием на территории ЕС. По этой причине мы рассмотрим их в настоящем блоке.

Помимо европейского и североамериканского законодательства изучения требует и опыт иных зарубежных стран, содержащих альтернативные модели решения вопросов обеспечения ИПБ. Представляется целесообразным взять в качестве объектов исследования опыт стран Азиатско-Тихоокеанского региона.

Подчеркнем, что использование любого зарубежного опыта в нашей стране не должно иметь характер механического заимствования,

а, напротив, требует обязательной его адаптации к особенностям российского социокультурного контекста и национальной правовой системы. Основным критерием отбора и внедрения в России зарубежной практики правового регулирования обеспечения ИПБ, на наш взгляд, должна выступать ее реальная эффективность. Вместе с тем в нашей стране могут быть использованы лишь те зарубежные практики, которые совместимы с закрепленными Основным законом базовыми началами конституционного строя РФ и международными обязательствами России.

Сделав вводные пояснения, перейдем непосредственно к анализу зарубежного опыта правового обеспечения ИПБ. Материал традиционно изложим по тематическим группам по критерию предмета правового регулирования. В качестве основных тематических блоков будут выделены: 1) противодействие распространению негативного контента в массмедиа; 2) обеспечение безопасности пользователей в Интернете; 3) обеспечение безопасности пользователей компьютерных игр; 4) противодействие киберпреступности. Конечно, данные направления не исчерпывают всего поля правового регулирования обеспечения ИПБ. Например, в последние годы резко возросла актуальность противодействия распространению фейковой информации. Однако ограниченность объема исследования не позволяет рассмотреть все интересующие нас вопросы.

1. Противодействие распространению негативного контента в массмедиа

Западные и иные зарубежные государства, закрепляя правовые гарантии содействия развитию независимых и плюралистических СМИ,[409] включали в соответствующие правовые акты положения, направленные на предотвращение оборота негативной информации.

Зарубежный опыт правового регулирования СМИ в аспекте безопасности проанализирован в ряде отечественных научных исследований[410] и коллективном исследовании с участием автора.[411] Нами также проведен

---

[409] *Рихтер А. Г.* Международные стандарты и зарубежная практика регулирования журналистики. Издание ЮНЕСКО. М., 2011. С. 103.

[410] *Сулакшин С. С., Сазонова Е. С., Хвыля-Олинтер А. И.* Государственная политика защиты нравственности и СМИ. Рабочая книга для законодателя. М.: Наука и политика, 2014; *Ефимова Л. Л., Кочерга С. А.* Информационная безопасность детей: российский и зарубежный опыт: монография. М.: ЮНИТИ-ДАНА, 2013; *Иванов И. С.* Правовая защита детей от информации, причиняющей вред их здоровью и развитию. Расширенный научно-практический комментарий; подготовлен для СПС «КонсультантПлюс». 2012; *Кобзева С. В.* Сравнительно-правовой анализ регулирования оборота вредной информации в телерадиовещании и кинопрокате // Информационное право. 2010. № 2. С. 8–13; *Белицкая А.* Защита несовершеннолетних от вредного воздействия информационной среды в законодательстве постсоветских стран // Законодательство и практика масс-медиа. 2006. № 7–8.

[411] Концепция информационной безопасности детей. Раздел 10. Анализ международного и зарубежного опыта правового регулирования информационной безопасности детей и подростков // Роскомнадзор: официальный сайт. URL: https://rkn.gov.ru/docs/1_Razdel_10.pdf (дата обращения: 25.01.2022).

самостоятельный анализ законодательства иностранных государств и Европейского союза.[412]

В законодательных актах США и европейских стран, принятых преимущественно в период 1980–1990-х гг. (Закон Франции «О свободном вещании» 1986 г.,[413] Закон Великобритании «О видеозаписях» 1984 г.,[414] Закон США о телекоммуникациях 1996,[415] Законы Канады «О радиовещании» 1991 г.[416] и «О телекоммуникациях» 1993 г.,[417] Государственный договор Германии о службах массмедиа 1997 г.[418]), содержались запреты и ограничения на распространение негативной информации, включая порнографические и иные непристойные материалы, сцены насилия и преступлений, потребления наркотиков и т. п.

Иногда описание вредной информации дано в весьма размытых формулировках, как, например, использование «любых непристойных, неприличных либо грубых выражений в радиосвязи» (ст. 1464 титула 18 Свода законов США).[419] При введении ограничений часто используется метод ограничения показа негативного контента в дневное время («временной водораздел»).

Различается степень конкретности нормативных предписаний законов зарубежных государств. Например, в законодательстве Великобритании и Канады закреплены лишь нормы общего характера, которые детализированы на уровне подзаконного регулирования[420] или саморегулирования.[421]

---

[412] *Смирнов А. А.* Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография. М.: ЮНИТИ-ДАНА, Закон и право, 2012.

[413] Loi n 86–1067 du 30 septembre 1986 relative à la liberté de communication // Legifrance. URL: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068930/ (дата обращения: 12.03.2021).

[414] Video Recordins act 1984 // Legislation.GOV.UK. URL: https://www.legislation.gov.uk/ukpga/1984/39/contents (дата обращения: 12.03.2021).

[415] Telecommunications Act of 1996 // Federal Communications Commission. URL: https://www.fcc.gov/general/telecommunications-act-1996 (дата обращения: 12.03.2021).

[416] Canadian Broadcasting Act (S.C. 1991) // Justice Law Site. URL: https://laws-lois.justice.gc.ca/eng/acts/b-9.01/ (дата обращения: 12.03.2021).

[417] Telecommunications Act (S.C. 1993) // Justice Law Site. URL: https://laws.justice.gc.ca/eng/acts/T-3.4/index.html (дата обращения: 12.03.2021).

[418] Staatsvertrag uber Mediendienste (Mediendienstestaats-vertrag) // URL: http://www.presserecht.de/index.php?option=com_content&task=view&id=26 (дата обращения: 17.02.2021).

[419] 18 U. S. Code § 1464 – Broadcasting obscene language // Cornell University Law School. URL: https://www.law.cornell.edu/uscode/text/18/1464 (дата обращения: 12.03.2021).

[420] Например, в Великобритании регулятором Ofcom принимается Кодекс вещания (The Ofcom Broadcasting Code).

[421] В качестве примера можно привести Кодекс этики (Code of Ethics) и Кодекс о насилии в телевизионных программах (CAB Code Regarding Violence in Television Programming), принятые Канадской ассоциацией телерадиовещателей (Canadian Association of Broadcasters).

В Европейском союзе базовым правовым актом в области СМИ выступает Директива об аудиовизуальных медиауслугах 2010 г. (Audiovisual Media Services Directive). Сейчас действует ее кодифицированная версия в редакции от 14 ноября 2018 г.[422] Статья 6 Директивы закрепляет обязанность государств – членов ЕС обеспечить отсутствие в содержании предоставляемых аудиовизуальных медиауслуг (далее – АВМУ): а) подстрекательств к жестокости или ненависти, направленных против группы лиц или членов группы, основанных на признаках пола, расы, этнического и социального происхождения, взглядов и т. д.; б) публичных призывов к совершению террористических актов. Принимаемые странами меры должны быть необходимыми и пропорциональными, учитывать права и соблюдать принципы, установленные в Хартии.[423]

Статья 6а Директивы содержит ряд специальных правовых гарантий обеспечения ИПБ детей. Во-первых, она закрепляет обязанность государств – членов ЕС обеспечить с помощью надлежащих средств, чтобы АВМУ, которые могут нанести вред физическому, психическому или нравственному развитию несовершеннолетних, не были доступны для их просмотра или прослушивания. Данные меры могут включать выбор времени вещания, инструменты для проверки возраста или иные технические меры и должны быть пропорциональны потенциальному вреду программы. Особо оговаривается, что наиболее вредный контент, такой как немотивированная жестокость или порнография, должен быть предметом строжайших мер (ч. 1). Во-вторых, ст. 6а предусматривает предоставление провайдерами АВМУ достаточной информации зрителям о негативном контенте для детей. Для данной цели провайдеры медиауслуг должны использовать систему, описывающую потенциально вредный характер контента аудиовизуальной медиауслуги (ч. 3). В целях имплементации норм данной статьи государства должны поощрять использование совместного регулирования и содействовать саморегулированию посредством национальных кодексов поведения (ч. 3–4).

Важно отметить, что после внесенных в 2018 г. изменений в Директиву об аудиовизуальных медиауслугах ее действие стало распространяться не только на эфирное телевещание и телевизионные системы видео по запросу, но и некоторые интернет-сервисы, включая видеохостинг YouTube и социальную сеть Facebook, в части распространения аудиовизуального контента.[424]

---

[422] Directive 2010/13/eu of the European Parliament and of the Council of 10 march 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02010L0013–20181218&from=EN (дата обращения: 12.02.2021).

[423] Имеется в виду Хартия Европейского союза об основных правах от 12 декабря 2007 г. (2007/C303/01).

[424] Revision of the Audiovisual Media Services Directive (AVMSD) // European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/revision-avmsd (дата обращения: 20.01.2022).

Отметим, что законодательство о защите детей от вредной информации в СМИ в Европе имеет длительную историю. Специализированные законы в данной сфере были приняты еще в середине XX века (Закон ФРГ «О распространении произведений и медиаконтента, вредных для молодежи» 1953 г.[425] и Закон Великобритании «О детях и молодежи (вредные публикации)» 1955 г.[426]). В этих законах закреплены следующие правовые механизмы защиты детей от вредных сведений: а) запрет показа вредных для детей материалов в дневное время; б) возрастная классификация и маркировка информационной продукции; в) оповещение о наличии вредной информации для детей в радио- и телетрансляциях; г) запрет включения вредного контента в информационную продукцию для детей и распространения такого контента в доступных для детей местах. Как видим, весь указанный правовой инструментарий лег в основу российского закона о защите детей от информации.

Отдельно необходимо сказать о механизмах классификации контента. Они подробно описаны в научной литературе[427] и других источниках. В большинстве стран мира применяется принцип возрастной классификации. Однако системы классификации, включающие в себя перечень возрастных категорий (рейтингов), механизм их присвоения и маркировки, в разных странах различаются. Функционально задача возрастной классификации медиаконтента возложена на неправительственные организации, учрежденные самой медиаиндустрией (американский Комитет по классификации фильмов CARA, Британский совет классификации фильмов BBFC, германская Добровольная организация саморегулирования киноиндустрии FSK, Нидерландский институт классификации аудиовизуальных медиа NICAM и др.). Контроль за их работой осуществляют государственные надзорные органы в сфере медиакоммуникаций. Реже функции классификации выполняют государственные органы, например: австралийский Совет по классификации ACB, Центральный совет классификации фильмов CBFC Министерства информации и телерадиовещания Индии и др.[428]

---

[425] Gesetz über die Verbreitung jugendgefährdender Schriften 1953 // Bundesanzeiger Verlag. URL: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl153s0377.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl153s0377.pdf%27%5D__1644751594003 (дата обращения: 17.02.2021).

[426] Children and Young Persons (Harmful Publication) Act 1955 // Legislation.GOV.UK. URL: https://www.legislation.gov.uk/ukpga/Eliz2/3–4/28/contents (дата обращения: 12.03.2021).

[427] *Ефимова Л. Л., Кочерга С. А.* Информационная безопасность детей: российский и зарубежный опыт. М.: ЮНИТИ-ДАНА, 2013 С. 45–50, 55–192; *Сулакшин С. С., Сазонова Е. С., Хвыля-Олинтер А. И.* Государственная политика защиты нравственности и СМИ. Рабочая книга для законодателя. М.: Наука и политика, 2014. С. 229–241.

[428] Концепция информационной безопасности детей. Раздел 10. Анализ международного и зарубежного опыта правового регулирования информационной безопасности детей и подростков // Роскомнадзор: официальный сайт. URL: https://rkn.gov.ru/docs/1_Razdel_10.pdf (дата обращения: 25.01.2022).

Возрастная маркировка обычно обозначается цифровыми (например, 12, 15 и 18 в Республике Корея) или буквенными обозначениями (категория «PG» в США – рекомендуется присутствие родителей) либо их сочетанием (категория «R18+» в Японии – запрещенная для детей информация). Помимо возрастной маркировки применяется также контентная маркировка (Content Labels, Descriptors), обозначающая конкретный вид содержащейся вредной информации. Так, в американской системе классификации телепрограмм используются следующие контентные дескрипторы: D – непристойный диалог, L – грубый или оскорбительный язык, S – сексуальные ситуации, V – насилие, FV – фэнтези-насилие.[429] Контентная маркировка представляется нам весьма перспективным инструментом, поскольку она не только дает родителям информацию о возрастном ограничении для определенной продукции, но и поясняет, какой именно вредный контент в ней содержится.

Интересно отметить, что, помимо информационной функции возрастной и контентной маркировки медиапродукции, в США, Канаде и Бразилии предпринимались попытки придать им более жесткий характер фильтров посредством программно-технических мер. Речь идет о так называемом чипе насилия (V-chip) – устройстве, встраиваемом в телевизоры и позволяющем на основе автоматического считывания ТВ-маркировок блокировать определенные телепередачи, неприемлемые для детей, в соответствии с задаваемыми пользователем настройками. В США в начале 2000-х гг. действовало правило обязательного наличия таких чипов в телевизорах диагональю свыше 13 дюймов.[430] Однако регулятор в лице Федеральной комиссии связи по результатам анализа сделал вывод о низкой востребованности данного инструмента, прежде всего из-за сложной настройки V-чипов и пассивности самих родителей в их применении.[431] Вместе с тем, как показало проведенное в 2007 г. в США социологическое исследование, подавляющее большинство американских родителей признают систему классификации ТВ-контента вместе с V-чипами эффективными инструментами защиты детей от негативных сведений (63% разделяют это мнение, 27% не согласны с ним).[432]

2. Обеспечение безопасности пользователей Интернета

---

[429] Understanding the TV Ratings and Parental Controls // TV Parental Guidelines. URL: http://www.tvguidelines.org/resources/TV_Parental_Guidelines_Brochure.pdf (дата обращения: 14.07.2021).

[430] About the TV Ratings and V-chip // TV Parental Guidelines. URL: http://www.tvguidelines.org/index.htm (дата обращения: 14.07.2013).

[431] In the Matter of Violent Television Programming and Its Impact on Children. Report. Federal Communications Commission (April 25, 2007). P. 13–14. URL: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07–50A1.pdf (дата обращения: 21.04.2012).

[432] TV Watch Survey of Parents Topline. June 2007. Luntz, Maslansky Strategic Research & Hart Research. URL: http://www.televisionwatch.org/junepollresults.pdf (дата обращения: 14.07.2013).

В связи со стремительным развитием Интернета и ростом связанных с этим киберугроз в зарубежных странах (преимущественно западных) в конце 1990-х – начале 2000-х гг. начало формироваться законодательство в области обеспечения кибербезопасности. Первоначально оно складывалось фрагментарно, по отдельным направлениям (защита информации, защита информационной инфраструктуры, обеспечение безопасности детей в Интернете и т. д.), тогда как в настоящее время во многих странах приняты базовые стратегии кибербезопасности, на основе которых идет становление профильного законодательства. Нас будет интересовать законодательство в области обеспечения ИПБ пользователей Интернета.

Пионерами в рассматриваемой области выступали США и Европейский союз. В США – стране, где изобрели Интернет, – законодательство в области кибербезопасности имеет наиболее давнюю историю. Одним из первых законов в сфере Интернета стал Закон «О телекоммуникациях» 1996 г. (Telecommunications Act of 1996). В частности, он включал раздел 5 «Непристойность и насилие», именуемый также актом «О благопристойности коммуникаций» (Communications Decency Act of 1996), в котором впервые была предпринята попытка регулирования ограничения распространения порнографических материалов в Интернете. Им устанавливалась уголовная ответственность за распространение материала, который является «неприличным или непристойным», для лиц моложе 18 лет. Однако из-за размытости формулировок базовые нормы Закона «О благопристойности коммуникаций» были признаны неконституционными Верховным судом США в 1997 г.[433] Та же судьба постигла и его последователя – Закон о защите детей в онлайн 1998 г. (Child Online Protection Act, COPA), цель которого состояла в ограничении доступа несовершеннолетних к вредным для них материалам.[434] Более успешным оказался Закон о защите детей в Интернете 2000 г. (Children's Internet Protection Act, CIPA), который обязал школы и библиотеки в США применять интернет-фильтры и иные меры для обеспечения безопасности детей в сети.[435] Выполнение такого требования является одним из условий получения федерального финансирования. Также сохраняет свое действие Закон о защите частной жизни детей в онлайн 1998 г. (Children's Online Privacy Protection Act of 1998, COPPA) в редакции от 2013 г., предписывающий осуществление мер по реализации политики охраны частной жизни детей со стороны операторов интернет-услуг.[436] Им устанавливается

[433] *Ефимова Л. Л., Кочерга С. А.* Информационная безопасность детей: российский и зарубежный опыт. М.: ЮНИТИ-ДАНА, 2013. С. 81.

[434] *Singel R.* Net Censorship Law Struck Down Again // Wired.com. 22.07.2008. URL: http://www.wired.com/threatlevel/2008/07/net-censorship/ (дата обращения: 12.03.2019).

[435] Children's Internet Protection Act // Federal Communications Commission. URL: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act (дата обращения: 21.02.2021).

[436] Children's Online Privacy Protection Rule («COPPA») // Federal Communications Commission. URL: https://www.ftc.gov/enforcement/rules/rulemaking-

необходимость получения согласия родителей или опекунов для получения и обработки персональных данных детей в возрасте до 13 лет.

В последующий период в развитии законодательства США в области кибербезопасности был сделан акцент на технических аспектах защиты от угроз информационных систем и иных объектов. Возвращение к психологическим аспектам произошло во многом вследствие появления проблемы фейковых новостей и внешнего вмешательства в выборы. Что касается собственно закрепления правил противодействия негативному контенту и коммуникации, то основное бремя этой работы взяли на себя администрации социальных сетей. Это произошло под сильным давлением американских властей.

Практика комплексного и сбалансированного регулирования ИПБ интернет-пользователей имеется и в Европейском союзе. В рамках политики ЕС в сфере развития информационного общества (Information society) большое внимание уделялось вопросам безопасности сетевой коммуникации. В качестве примера можно привести программный документ 2010 г. – «Цифровая повестка дня для Европы»,[437] принятый в рамках развития одного из направлений политической стратегии развития Европейского союза до 2020 г. – Стратегии «Европа 2020». В рамках реализации «Цифровой повестки дня для Европы» в период 2010-х гг. была реализована система мер по обеспечению безопасности пользователей Интернета в ЕС, включая: а) усиление борьбы с киберпреступностью, в том числе учреждение Европейского центра по киберпреступности; б) развитие механизмов подачи жалоб на незаконный контент; в) проведение информационно-просветительских кампаний о правилах интернет-безопасности; г) поддержку корпоративного саморегулирования в сфере использования онлайн-услуг.

Европейский союз выступил пионером в плане правовой регламентации обеспечения безопасности детей в Интернете. Принятый в конце 1990-х гг. пакет правовых актов нормативного и программного характера обеспечил создание на пространстве ЕС одной из лучших в мире защит несовершеннолетних в онлайн-среде. Среди наиболее значимых юридических документов ЕС можно отметить: рекомендации по защите несовершеннолетних и человеческого достоинства 98/560/ЕС[438]

---

regulatory-reform-proceedings/childrens-online-privacy-protection-rule (дата обращения: 12.02.2021).

[437] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions «A Digital Agenda for Europe». Brussels, 26.8.2010. COM(2010) 245 final/2 // Eur-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245R%2801%29 (дата обращения: 14.07.2019).

[438] Council Recommendation 98/560/EC of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity // Eur-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31998H0560 (дата обращения: 14.07.2019).

и 2006/952 ЕС,[439] Директиву об аудиовизуальных медиауслугах, программы «Безопасный Интернет» (Safer Internet Programme) 1999–2013 гг. и пришедшую им на смену в 2014 г. программу «Лучший Интернет для детей» (Better Internet for Kids).[440] Указанные документы подробно проанализированы нами в монографии,[441] поэтому ограничимся их краткой характеристикой.

Рекомендации по защите несовершеннолетних и человеческого достоинства 1998 и 2006 гг. регламентировали действия, направленные на обеспечение онлайн-безопасности детей. Государствам – участникам ЕС предписывалось развивать профильное законодательство, противодействовать распространению негативного контента в сети (в том числе через механизм рассмотрения жалоб и реагирования на них), стимулировать компании интернет-отрасли разрабатывать и внедрять программно-технические, правовые и иные средства, включая принятие актов саморегулирования, а также проводить обучающие и иные программы повышения медиаграмотности детей, их родителей и педагогов. Производителей и провайдеров интернет-услуг призывали к разработке и принятию кодексов поведения, участию совместно с государственными органами в разработке национальных мер, предоставлению пользователям необходимых инструментов и опций для обеспечения безопасности и повышения их осведомленности, внедрению систем фильтрации и стимулированию использования систем маркировки интернет-контента. Европейская комиссия была призвана выявлять и распространять положительный опыт, а также принять меры на общеевропейском уровне.

Нормы Директивы об аудиовизуальных медиауслугах, частично распространяющиеся на контент в Интернете, мы рассмотрели выше. В плане нормативного регулирования необходимо выделить два исключительно важных акта, касающихся саморегулирования компаний интернет-отрасли, принятых на уровне ЕС и имеющих рамочный характер: Европейские правила безопасного использования мобильной связи детьми и подростками 2007 г.[442] и Принципы безопасного использования социальных сетей в ЕС

[439] Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry // EurLex. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006H0952 (дата обращения: 14.07.2019).

[440] Better Internet for Kids. URL: https://www.betterinternetforkids.eu/ (дата обращения: 14.07.2019).

[441] *Смирнов А. А.* Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского союза: монография. М.: ЮНИТИ-ДАНА, Закон и право, 2012.

[442] European Framework for Safer Mobile Use by Young Teenagers and Children // GSMA Europe. URL: https://www.gsma.com/gsmaeurope/safer-mobile-use/european-framework/#:~:text=The%20European%20Framework%20for%20Safer, content%20on%20their%20mobile%20phones. (дата обращения: 14.02.2021).

2009 г.[443] Они отличаются сферой регулирования, но закрепляют схожий набор мер обеспечения безопасности детей, включая: а) регулирование доступа детей к услугам и контенту; б) повышение осведомленности и обучение; в) классификация контента; г) выявление и удаление незаконного контента; д) обеспечение пользователей инструментами защиты; е) учреждение механизма жалоб.[444] Проведенный обзор правоприменения данных актов в области саморегулирования показал высокий уровень имплементации и работоспособность их положений на уровне стран – членов ЕС.[445]

Что касается программных документов ЕС по безопасному Интернету, то они во многом закрепляют сходные с описанными выше меры защиты детей в сети. Однако главная ценность данных программ обусловливается комплексом тематических проектов по исследованию интернет-рисков и способов противодействия им (проекты FIVES, EU KIDS, Online, ROBERT, POG и др.), а также проведение Дня безопасного Интернета и иных просветительских мероприятий.[446] Начиная с 2012 г. по настоящее время в рамках реализации Европейской стратегии создания лучшего Интернета для детей[447] в странах ЕС проведено большое количество мероприятий по созданию позитивного контента для детей, повышению цифровой грамотности и онлайн-безопасности в школах, внедрению систем родительского контроля и адекватных настроек конфиденциальности аккаунтов детей в социальных сетях, применению механизмов возрастной классификации и маркировки контента, а также по борьбе с материалами, содержащими сцены сексуальной эксплуатации или сексуального насилия над детьми.

Отдельно рассмотрим *вопрос ограничения доступа к интернет-контенту.* Выбор механизма его решения в разных странах во многом

---

[443] Safer Social Networking Principles for the EU // Rusla. URL: http://www.rusla.ru/rsba/technology/safety/sn_principles.pdf (дата обращения: 15.01.2020).

[444] См: *Смирнов А. А.* Корпоративное саморегулирование в сфере обеспечения безопасности детей в Интернете: опыт Европейского союза // Юридическая наука как основа правового обеспечения инновационного развития России (Кутафинские чтения): Материалы секции информационного права международной научно-практической конференции. Сборник докладов. Москва, 29 ноября 2011 г. / Под ред. проф. И. М. Рассолова, доц. С. Г. Чубуковой. Киров: Типография «Старая Вятка», 2012. С. 80–86.

[445] Third implementation review of the European Framework for Safer Mobile Use by Younger Teenagers and Children. GSMA Europe, June 2010; Donoso V. Assessment of the implementation of the Safer Social Networking Principles for the EU on 9 services: Summary Report. European Commission, Safer Internet Programme, Luxembourg, 2011.

[446] См.: *Смирнов А. А.* О программе Европейского союза «Безопасный Интернет» // Дети в информационном обществе. 2011. № 7. С. 64–69.

[447] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Strategy for a Better Internet for Children COM/2012/0196 final // Eur-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0196&from=EN (дата обращения: 15.01.2020).

обуславливается политической системой. Хотя содержание и характер применяемых ограничений на распространение информации в Интернете в демократических и иных странах заметно отличаются, в целом они свойственны не только авторитарным и тоталитарным политическим режимам.[448]

Авторы аналитического доклада «Фильтрация контента в Интернете. Анализ мировой практики» выделили две основные группы методов «цензуры контента» во Всемирной сети: 1) технические (блокирование сайтов по IP-адресу или URL, пакетная фильтрация, искажение DNS-записей, фильтрация результатов поиска и др.); 2) нетехнические (законодательные запреты распространения определенного контента, оказание давления на владельцев сайтов, интернет-посредников и пользователей, самоцензура).[449] Эксперты выделили пять культурно-страновых моделей фильтрации контента в Интернете:

1) азиатская модель – характеризуется широким усмотрением государственных органов относительно применения мер фильтрации негативного контента в целях защиты нравственности или по политическим мотивам (КНР,[450] Вьетнам, Южная Корея, Сингапур);

2) ближневосточная модель – предполагает ограничение доступа к информации, противоречащей нормам ислама, а также блокировку правозащитных ресурсов (Саудовская Аравия, Катар, Оман, ОАЭ);

3) рестрикционная модель – присуща странам с неустойчивой внутриполитической ситуацией, власти которых прибегают к ограничению доступа к сайтам крайней политической оппозиции, нередко разделяющей исламистские взгляды (Иран, Сирия, Эфиопия, Узбекистан);

4) континентальная модель – для нее свойственно применение фильтрации общественно опасной информации, категории которой определены законом, а также пиратских сайтов (Франция, Великобритания, Германия, Бельгия);

5) либеральная модель – характеризуется отсутствием систематической фильтрации контента, ограничительные меры принимаются только в отношении нарушающих закон ресурсов и их владельцев (США, Япония, Бразилия).

---

[448] Фильтрация контента в Интернете. Анализ мировой практики. Аналитический доклад. Фонд развития гражданского общества, 2013. С. 1.

[449] Там же. С. 2, 27–32.

[450] А. А. Тедеев, анализируя в своей статье применяемую в НКР систему социального рейтинга, высказывает интересную мысль о том, что подобные «цифровые социальные регуляторы делают в недалеком будущем потенциально ненужным контроль за оборотом информации, Интернетом и социальными платформами (фильтрацию и ограничения контента)». Автор не вполне согласен с данным тезисом, поскольку подобные системы цифрового контроля, в отличие от механизмов блокировки, не способны быстро пресечь само распространение социально опасной информации. См.: *Тедеев А. А.* Право, цифровая трансформация, цифровой посткапитализм (постановка проблемы) // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 12. С. 67.

Применяемые механизмы блокировки запрещенного интернет-контента также могут существенно различаться в разных странах. Они могут включать ограничение доступа к определенным интернет-ресурсам, разделегирование доменов, запрет или ограничение результатов поисковой выдачи по определенным запросам, удаление или блокировку доступа к конкретным аккаунтам в социальных сетях или размещенной информации и др.

Особое внимание в последние годы уделяется противодействию фейковым новостям и дезинформации. В связи с отсутствием каких-либо единых стандартов в различных государствах мира предприняты попытки самостоятельного решения данной проблемы.[451] В подготовленной экспертами РАПСИ сводной таблице выделены следующие способы борьбы с фейками за рубежом: 1) штрафы и иные санкции за распространение фейков (Германия, Малайзия); 2) защита государственных интересов в сети посредством запретов и быстрого удаления «подрывного» контента (Вьетнам); 3) блокировка зарубежных доменов (Украина); 4) блокировка аккаунтов в социальных сетях и привлечение к ответственности блогеров и журналистов (Египет); 5) запрет анонимных комментариев в социальных сетях и мессенджерах (Казахстан); 6) блокировка отдельных соцсетей и мессенджеров (Иран, Шри-Ланка); 7) раскрытие ключей шифрования (Австралия); 8) идентификация пользователей и вскрытие переписки (США); 9) блокировка анонимайзеров (Венесуэла, Белоруссия); 10) досмотр провайдеров (Китай); 11) привлечение гражданских волонтеров для мониторинга (Вьетнам); 12) закрепление ответственности пользователей за посещение определенных сайтов (Египет).[452] Как видно из этого перечня, для противодействия фейкам применяется универсальный инструментарий, используемый для сдерживания иных информационных угроз в сети.

Сквозным и весьма значимым аспектом противодействия распространению негативной информации в Интернете является вопрос *ответственности провайдеров интернет-услуг* (Internet Service Providers,

[451] В данном контексте стоит отметить Совместную декларацию о свободе выражения мнения, а также «фейковых» новостях, дезинформации и пропаганде, принятую 3 марта 2017 г. специальными представителями ООН, ОБСЕ, Организации американских государств и специальным докладчиком по вопросу о свободе выражения мнения и доступе к информации в Африке. В Декларации предпринята попытка зафиксировать базовые подходы к противодействию ложной информации. Однако данный документ не носит юридически обязывающего характера. Обзор имеющихся международных стандартов и национальных подходов противодействия дезинформации в контексте свободы СМИ проведен А. Рихтером. См.: International Standards and Comparative National Approaches to Countering Disinformation in the Context of Freedom of the Media (on the request of the Russian Federation) / Prepared by Dr. Andrey Rikhter, Senior Adviser, Office of the OSCE Representative on Freedom of the Media. Vienna, March 2019.

[452] Все способы борьбы с фейками в России и за рубежом // Российское агентство правовой и судебной информации. 21.12.2018. URL: http://rapsinews.ru/incident_publication/20181221/292876054.html (дата обращения: 21.02.2021).

ISP). Общий подход, которого долгое время придерживались европейские страны и США, состоял в ограничении ответственности провайдеров интернет-услуг за оборот незаконного и иного вредоносного контента. В частности, ст. 15 Директивы об электронной коммерции ЕС 2000 г.[453] четко фиксировала принцип отсутствия обязанности по контролю передаваемой информации у провайдеров.

Однако в последние годы в связи с изменившейся обстановкой наблюдается пересмотр данного подхода. Лучшей иллюстрацией этого является инициатива Европейской комиссии по принятию Закона о цифровых услугах,[454] запуск которой во многом связан с необходимостью усиления защиты интернет-пользователей от новых цифровых угроз, таких как дезинформация и манипулирование. Проект регламента Европарламента и Совета ЕС о едином рынке для цифровых услуг (Закона о цифровых услугах) и внесении изменений в Директиву об электронной коммерции внесен Еврокомиссией в декабре 2020 г.[455] По оценкам экспертов ICANN, переговоры по документу, вероятно, продлятся до 2023–2025 гг.,[456] однако его положения представляют интерес уже сейчас.

Проект Регламента устанавливает отсутствие у провайдеров интернет-услуг общих обязательств по мониторингу информации и выявлению фактов или обстоятельств, указывающих на незаконную деятельность (ст. 7). Но для них установлена обязанность оперативного реагирования на обращения национальных судебных или административных органов о принятии мер в отношении конкретного элемента незаконного контента (ст. 8).

В то же время проект предполагает возложение на крупные интернет-платформы[457] (very large online platforms) особой ответственности и дополнительных обязанностей в плане реагирования на незаконный контент. Так, для них закреплена обязанность проводить выявление и оценку системных рисков, в числе которых названы распространение негативного контента и преднамеренное манипулирование услугами платформ (ст. 26), а также принимать меры по снижению данных рисков (ст. 27). Такие меры могут включать: а) адаптацию систем модерации контента или

[453] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market // Eur-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031 (дата обращения: 27.04.2021).

[454] The Digital Services Act package // European Commision. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (дата обращения: 27.04.2021).

[455] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. Brussels, 15.12.2020 COM(2020) 825 final // Eur-Lex. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN (дата обращения: 21.11.2021).

[456] *Плексида Е.* Новости Евросоюза: Закон о цифровых услугах. ICANN. Июль 2020 г. С. 5.

[457] Критерием их выделения является месячная аудитория активных пользователей, превышающая 45 млн человек.

рекомендаций, процессов принятия решений, функционирования услуг, их условий и положений; б) усиление надзора за любой деятельностью, создающей риски; в) инициирование или корректировку сотрудничества с иными онлайновыми платформами на основе кодексов поведения и протоколов о кризисных ситуациях и др.

3. Обеспечение безопасности пользователей электронных игр

В зарубежных странах отдельное внимание уделяется такой специфической информационной среде, как электронные (компьютерные и видео) игры. Это связано с развитием индустрии компьютерных игр и активным увлечением ее продукцией молодежи и иных слоев населения. По мнению западных исследователей, компьютерные игры заменили музыку в качестве наиболее значимого компонента молодежной субкультуры.[458] Пандемия существенно усилила тенденцию роста востребованности компьютерных игр. При этом увеличивается не только время самой игры, но и просмотр игровых видео и стримов на YouTube или Twitch.[459]

В контексте нашей темы следует отметить, что большинство современных компьютерных игр имеют онлайн-формат. Он позволяет игрокам общаться и обмениваться информацией между собой. А потому компьютерные игры могут не только сами содержать негативный контент, но и выступать платформой для деструктивной коммуникации и распространения вредной информации, созданной пользователями.

Среди правовых механизмов обеспечения ИПБ в данной области применяется апробированный на аудиовизуальных СМИ метод возрастной классификации и маркировки. Причем, как правило, для электронных игр существуют свои отдельные системы рейтингов: американская ESRB, общеевропейская PEGI, германская USK, японская CERO и др. Хотя в некоторых странах они подпадают под действие общих систем возрастной классификации (Бразилия, Австралия, Сингапур и др.).[460]

В качестве примера кратко рассмотрим Общеевропейскую систему возрастной классификации игр PEGI (Pan-European Game Information age rating system). Она является успешным примером саморегулирования в сфере игровой индустрии на уровне ЕС. Правовой основой для ее создания стало Решение Совета ЕС 2002 г.[461] и последовавшие за этим

---

[458] *Monahan S.* Video games have replaced music as the most important aspect of youth culture // The Guardian. 11 Jan 2021. URL: https://www.theguardian.com/commentisfree/2021/jan/11/video-games-music-youth-culture?fbclid=IwAR0zH5C_eioD53G_aZcylOBIA7hdvUOfa01558HitbZo5A5XToD6S_Vp9wg (дата обращения: 08.04.2021).

[459] *Traeger P.* Gaming as a Cultural Force Just Stepped to the Forefront of Entertainment // ADWEEK. URL: https://www.adweek.com/sponsored/gaming-as-a-cultural-force-just-stepped-to-the-forefront-of-entertainment/ (дата обращения: 09.04.2021).

[460] *Ефимова Л. Л., Кочерга С. А.* Информационная безопасность детей: российский и зарубежный опыт: монография. М.: ЮНИТИ-ДАНА, 2013. С. 45–50, 55–192.

[461] Council Resolution 2002/C65/02 of 1 March 2002 on the protection of consumers, in particular young people, through the labelling of certain video games and computer games according to age group.

акты саморегулирования отрасли. Система PEGI была запущена осенью 2003 г. и по состоянию на 2021 г. используется в 38 странах Европы.[462]

Система функционирует на основе Кодекса поведения (PEGI Code of Conduct), внутри которого выделен свод правил, касающихся аспектов безопасности (PEGI Online Safety Code).[463] Он включает комплекс следующих мер: 1) обязательство компаний – производителей игр, владеющих лицензией «PEGI Online», запрещать на своих онлайн-сервисах неприемлемые материалы и поведение пользователей, которые являются незаконными, оскорбительными, расистскими, унижающими достоинство, развращающими, угрожающими, непристойными или которые могут постоянно препятствовать развитию молодежи; 2) соблюдение правил обработки персональных данных пользователей; 3) получение возрастного рейтинга; 4) наличие механизма подачи жалоб игроками; 5) удаление неуместного контента в онлайн-сервисах; 6) ответственную рекламную политику, в том числе соблюдение возрастных ограничений.

Возрастная классификация PEGI включает пять категорий (рис. 2), для каждой определены содержательные критерии. Возрастная маркировка размещается на упаковке игры или на стартовой странице ее интернет-сайта.

Система PEGI также предусматривает контентную маркировку (см. рис. 3). Соответствующие дескрипторы обозначают содержащийся в игре вид негативного контента (насилие, нецензурная брань, устрашение, наркотики, сексуальные сцены, дискриминация) или присущий игре иной риск (азартный характер игры, наличие платных опций).

Рис. 2. Знаки возрастной классификации PEGI (источник: URL: http://www.pegi.info)

Рис. 3. Знаки контентной маркировки PEGI (источник: URL: http://www.pegi.info)

Проведенное в 2008 г. компанией Nielsen Games социологическое исследование подтвердило высокую осведомленность (62%) людей о системе PEGI, понимание смысла возрастных (93%) и контентных (50%)

[462] Здесь и далее приведена информация с официального сайта Общеевропейской системы возрастной классификации игр PEGI. URL: http://www.pegi.info (дата обращения: 01.05.2021).

[463] PEGI Online Safety Code // PEGI. URL: https://pegi.info/page/pegi-online-safety-code (дата обращения: 01.05.2021).

маркировок. При этом почти половина родителей признала полезность системы при выборе компьютерных игр для детей.[464]

Кроме того, на уровне национального гражданского и уголовного законодательства стран – членов ЕС регламентируются правила их розничной продажи и ответственность за их нарушение. При этом законодательством ряда государств (Великобритания, ФРГ, Италия и др.) установлен прямой запрет на распространение некоторых видеоигр либо введены эквивалентные запрету меры, такие как конфискация, отказ в классификации либо введение заградительных торговых ограничений.[465]

Также на сайте PEGI говорится об обязательном оснащении всех игровых консолей, портативных устройств и операционных систем для компьютеров и ноутбуков системами родительского контроля, позволяющими взрослым защищать конфиденциальность и безопасность своих детей в Интернете по различным параметрам. С помощью этих инструментов управления родители могут: а) выбирать, в какие игры детям разрешено играть (на основе возрастных рейтингов PEGI); б) контролировать и отслеживать использование цифровых покупок; в) ограничивать доступ к просмотру веб-страниц с помощью фильтра; г) регулировать количество времени, которое дети могут проводить за играми; д) контролировать онлайн-контакты (чаты) и обмен данными (текстовые сообщения, пользовательский контент).[466]

4. Противодействие киберпреступности

Противодействие киберпреступности выступает одним из ключевых направлений обеспечения информационной безопасности. Важная роль здесь отводится правовому регулированию. Как отмечается в работе «Понимание киберпреступности», подготовленной под эгидой Международного союза электросвязи (далее – Руководство МСЭ), формирование адекватной правовой базы является ключевым элементом стратегии кибербезопасности.[467]

Большая часть киберпреступлений связана с воздействием на информационные системы и содержащуюся в них компьютерную информацию. К интересующей нас сфере ИПБ относится прежде всего группа киберпреступлений, связанных с контентом и негативной коммуникацией. Противодействие им осуществляется посредством криминализации наиболее опасных видов вредоносного контента и коммуникации и привлечения физических и юридических лиц к ответственности за их совершение.

---

[464] How is PEGI recognised by consumers? // PEGI. URL: http://www.pegi.info/en/index/id/37/ (дата обращения: 12.11.2011).

[465] *Ефимова Л. Л., Кочерга С. А.* Информационная безопасность детей: российский и зарубежный опыт: монография. М.: ЮНИТИ-ДАНА, 2013. С. 167–168.

[466] Parental control tools // PEGI. URL: https://pegi.info/parental-controls (дата обращения: 01.05.2021).

[467] Понимание киберпреступности: явление, задачи и законодательный ответ / М. Герке. Международный союз электросвязи, 2012. С. 3.

При этом криминализация несет также мощное профилактическое воздействие, предупреждая общественно опасную деятельность, связанную с оказанием деструктивного ИПВ (общая превенция).

В связи с отсутствием универсального международного договора в области борьбы с киберпреступностью не существует единый перечень киберпреступлений, признаваемый большинством государств мира. Это относится и к деяниям, связанным с распространением негативной информации. Как подчеркивается в Руководстве МСЭ, законодательное определение видов незаконного контента испытывает сильное влияние особенностей правовой и культурных систем стран, вследствие чего оно существенно различается в разных странах.[468] Единый консенсус достигнут только в отношении запрета и криминализации детской порнографии. В отношении признания противоправности других видов контента, таких как эротика или «обычная» порнография, расистские материалы или агрессивные выказывания, пропаганда насилия и жестокости, оскорбление религии, клевета и дезинформация, наблюдается значительная страновая дифференциация. Хотя в авторитетном тематическом исследовании Управления ООН по наркотикам и преступности компьютерные преступления, связанные с расизмом или ксенофобией, включены в состав универсального перечня деяний, признаваемых киберпреступлениями в большинстве стран мира.[469]

Дифференциация в плане криминализации негативного контента, равно как и деструктивной коммуникации, характерна не только для стран с разной политической культурой (например, западноевропейских и арабских государств в отношении антирелигиозной пропаганды), но и для государств с общими политическими ценностями (например, США и Франции в отношении разжигания ненависти). Учитывая трансграничную природу Интернета, это приводит к тому, что его пользователи легко могут получать доступ к информации, запрещенной в их собственной стране, но законно доступной за рубежом.[470] Кроме того, это затрудняет межгосударственное сотрудничество, поскольку взаимная правовая помощь оказывается на основе обоюдного признания деяния преступлением (принцип двойной криминализации). При наличии расхождений в законодательстве разных стран преследование киберпреступлений может быть существенно затруднено.[471] В отношении тех видов контента, которые полностью не запрещены

[468] Понимание киберпреступности: явление, задачи и законодательный ответ / М. Герке. Международный союз электросвязи, 2012. С. 22.

[469] Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора. UNODC, 2013.

[470] Понимание киберпреступности: явление, задачи и законодательный ответ / М. Герке. Международный союз электросвязи, 2012. С. 4, 22.

[471] Дефицит международного сотрудничества позволяет киберпреступности оставаться безнаказанной: Информационный бюллетень № 8. Двенадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию. Салвадор, Бразилия,

уголовным законом, но рассматриваются как потенциально опасные для детей (например, эротика или порнография), могут применяться специальные меры защиты, такие как системы «подтверждения взрослости».[472]

Следует отметить, что предметом правового регулирования в законодательстве зарубежных стран, помимо вопросов криминализации киберпреступлений (материальное уголовное право), выступают также уголовно-процессуальные аспекты расследования таких преступлений и сбора доказательств, международное сотрудничество в данной области. Большая часть перечисленного выходит за рамки предмета нашего исследования в силу избранной научной специальности. Однако важно отметить, что, как подчеркивается в Руководстве МСЭ, законодательное регулирование не должно ограничиваться только уголовно-правовой сферой и обязано включать в себя вопросы профилактики таких преступлений.[473] При принятии необходимых мер следует обсудить весь спектр методов, в частности *повышение осведомленности, доступность и бесплатное предоставление программ защиты, внедрение решений, позволяющих ограничить доступ к определенному контенту*.[474]

Кроме того, в Руководстве МСЭ настойчиво проводится мысль о том, что законодательные меры должны выступать частью целостной стратегии борьбы с киберпреступностью.[475] Та же идея звучит и в проекте типовой политики борьбы с киберпреступностью (Cybercrime/e-Crimes: Model Policy Guidelines), разработанном в рамках инициативы ICB4PAC: «Решение многоплановых проблем борьбы с киберпреступностью требует всестороннего подхода, включающего всеобъемлющую политику, законодательство, обучение, повышение осведомленности, создание потенциала, проведение исследований, а также технические подходы».[476]

§ 3. Модели правового регулирования обеспечения информационно-психологической безопасности

Задача модернизации правовой системы в условиях цифровой трансформации преопределяет необходимость выработки новых моделей правового регулирования общественных отношений, испытывающих на себе влияние новых ИКТ. Требуют переосмысления вопросы

12–19 апреля 2010 г. // Организация Объединенных Наций: официальный сайт. URL: http://www.un.org/ru/conf/crimecongress2010/factsheet8.pdf (дата обращения: 21.03.2019); Понимание киберпреступности: явление, задачи и законодательный ответ / М. Герке. Международный союз электросвязи, 2012. С. 22.

[472] Понимание киберпреступности: явление, задачи и законодательный ответ. С. 23.

[473] Там же. С. 101.

[474] Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts. HIPCAR. ITU, 2012. URL: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1–5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf (дата обращения: 10.05.2019).

[475] Понимание киберпреступности: явление, задачи и законодательный ответ. С. 98.

[476] Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts.

соотношения национального и международного права, правовых и иных источников социального регулирования отношений.

Поэтому изучение механизма правового обеспечения ИПБ предполагает анализ ряда методологических аспектов, касающихся оптимальных моделей правового регулирования отношений в рассматриваемой области.

Первым таким вопросом методологического значения является *вопрос об уровне правового регулирования обеспечения ИПБ*. С одной стороны, считается общепринятым, что регулирование отдельных направлений обеспечения национальной безопасности страны осуществляется преимущественно на государственном уровне. Роль же международного права сводится к регламентации вопросов международного сотрудничества в рассматриваемой области и закреплению соответствующих международных стандартов, на которые должны ориентироваться государства. Это, в свою очередь, не исключает того факта, что в отдельных сферах безопасности значение международно-правового регулирования весьма велико. Наиболее ярким примером является ядерная безопасность, где международный режим нераспространения ядерного оружия и правовые ограничения его применения в качестве акта агрессии и обороны играют ключевую роль.

Полагаем, что *приоритетным уровнем правового регулирования обеспечения ИПБ должен выступать национальный*. При этом мы исходим из признания государственного суверенитета России в информационной сфере. Как известно, государственный суверенитет означает «самостоятельность и свободу нации в определении своего политико-юридического статуса, выбора модели экономического, социального и политического развития».[477] Он закреплен Конституцией Российской Федерации в качестве основы конституционного строя (ч. 1 ст. 4).

Признание суверенитета применительно к информационной сфере означает самостоятельность России в выборе модели государственно-правового регулирования данной области, определении правового статуса действующих в ней субъектов и закреплении правил их поведения, включая вопросы юридической ответственности. А. А. Ефремов также включает в состав государственного суверенитета в информационном пространстве участие страны в международно-правовом регулировании глобального и региональных информационных пространств.[478]

Значимость его обеспечения в современных условиях очень четко обозначил директор СВР России С. Нарышкин, отметив, что «в мире постправды задача укрепления информационного суверенитета становится

---

[477] Государственный суверенитет // *Иванец Г. И., Калинский И. В., Червонюк В. И.* Конституционное право России: энциклопедический словарь / Под общ. ред. В. И. Червонюка. М.: Юрид. лит., 2002. С. 63.

[478] *Ефремов А. А.* Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации: дис. … д-ра юрид. наук. М., 2020. С. 15.

не менее актуальной, чем, скажем, наращивание оборонного потенциала или развитие национальной экономики».[479]

В контексте рассматриваемой проблематики вывод о приоритетности национального правового регулирования означает потребность в законодательной регламентации целей, задач и направлений обеспечения ИПБ, системы обеспечения ИПБ и правового статуса составляющих ее субъектов, форм, методов и средств обеспечения ИПБ в Российской Федерации.

Трансграничный характер многих угроз ИПБ обуславливает потребность в выработке и реализации общих международных стратегий противодействия им.[480] Исследователи А. В. Минбалеев и И. С. Бойченко также подчеркивают значительное влияние международного права на национальные правовые режимы в области информационной безопасности.[481]

Роль международного права в сфере обеспечения ИПБ видится в закреплении общих правовых стандартов в данной области, включая вопросы соблюдения прав человека при обеспечении ИПБ, форм, методов и процедур международного сотрудничества в борьбе с отдельными угрозами ИПБ. Проведенный нами анализ основных международно-правовых актов является наглядным тому подтверждением.

Сделанный нами общий вывод вполне справедлив для области социальной коммуникации и СМИ, однако требует оговорок относительно сети Интернет как главной информационной среды. Специфика Всемирной сети состоит в том, что это первый в истории человечества поистине глобальный социальный феномен. Географический фактор во многом утрачивает свое значение в глобальной сети, а границы государств становятся легко проницаемыми информационными потоками, что приводит к размыванию государственного суверенитета. Как точно заметил создатель Всемирной паутины (WWW) Тим Бернерс-Ли, «нигде и никогда глобальные системы не вступали в такое противоречие с локальной реальностью, как это происходит сегодня в Интернете».[482]

---

[479] Выступление директора Службы внешней разведки С. Нарышкина на VI Московской конференции по международной безопасности. 27.04.2017 // YouTube. URL: https://www.youtube.com/watch?v=CgUL5zbk5AU (дата обращения: 16.05.2021).

[480] Как справедливо отмечалось в Докладе о мировом развитии 2014 Всемирного банка, «международное сообщество может предложить консультационные услуги, оказать содействие в координации международной политики, а также предоставить общие ресурсы в тех случаях, когда риски превосходят потенциал отдельных стран либо носят трансграничный или межпоколенческий характер». См.: Риски и возможности. Управление рисками в интересах развития // Доклад о мировом развитии 2014. Всемирный банк. URL: http://siteresources.worldbank.org/EXTNWDR2013/Resources/8258024–1352909193861/8936935–1356011448215/8986901–1380730337640/RUS_MainMessages.pdf (дата обращения: 04.10.2015).

[481] Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. д. ю. н., профессора Т. А. Поляковой. Саратов: Амирит, 2020. С. 136.

[482] *Биргер П.* Люди будущего. Как отец WWW Тим Бернерс-Ли создает новый Интернет // Slon. URL: http://slon.ru/biz/1005395/ (дата обращения: 20.10.2013).

Интернет обеспечивает доступ к контенту вне зависимости от места его размещения. Коммуникация в сети между людьми также происходит в режиме реального времени независимо от того, находится ли ваш собеседник в соседнем подъезде или на другом континенте. Единственным барьером в таких условиях остается незнание языка, но и он преодолевается с помощью продвинутых систем машинного перевода. Еще одним важным фактором глобального интернет-пространства являются крупные технологические компании, опосредующие сетевую коммуникацию между людьми. Наиболее важными из них являются платформы социальных сетей, мессенджеров и электронной почты. Такие компании, как Google и Facebook, предоставляют веб-услуги в большинстве стран мира.

Все это обуславливает сложность борьбы с глобальными киберугрозами на национальном уровне. В качестве иллюстрации можно привести борьбу с киберпреступностью, зачастую имеющую транснациональный характер и включающую действия групп преступников, находящихся в разных странах. Поэтому их уголовное преследование просто невозможно без тесного сотрудничества государств.

Поэтому международно-правовое регулирование отношений в киберпространстве (включая вопросы обеспечения ИПБ) имеет не меньшее значение, чем национальная регламентация. Однако его развитие по ряду направлений многие годы стопорится вследствие противоречия позиций ведущих мировых держав в данной области. Этому явно не способствует и усиливающееся информационное противоборство государств в киберпространстве.[483] Отчасти сложившая ситуация компенсируется успешным опытом правового регулирования на региональном уровне, в частности в рамках СНГ, ШОС, ОДКБ. Но вне зависимости от развития международного права в рассматриваемой области правовая регламентация кибербезопасности на национальном уровне должна оставаться приоритетной. И принцип информационного суверенитета должен распространяться на киберсреду, какой бы сложной ни была его реализация. Именно такой подход заложен в проекте Конвенции об обеспечении международной информационной безопасности и в Основах государственной политики РФ в области МИБ.

Что касается внутригосударственного уровня, то Конституция РФ позволяет осуществлять правовое регулирование информационной сферы, включая вопросы обеспечения ИПБ, как на федеральном, так и на региональном уровне при безусловном приоритете федерального законодательства. Внесенными в 2020 г. поправками в Основной закон обеспечение безопасности личности, общества и государства при

[483] *Кларк М., Нейк Р.* Третья мировая война: какой она будет? СПб.: Питер, 2011; *Ларина Е., Овчинский В.* Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М.: Книжный мир, 2014; *Савин Л.* Стрелы кентавра. Кибервойна по-американски. М.: Издательство «Кислород», 2020.

применении информационных технологий, обороте цифровых данных отнесено к предметам ведения РФ.

Базовые механизмы обеспечения ИПБ в СМИ, сети Интернет, межличностной и групповой коммуникации, включая вопросы уголовной и административной ответственности, должны быть закреплены федеральными законами. Роль регионального законодательства нам видится преимущественно в возможном дополнении и (или) детализации положений федерального законодательства применительно к конкретному субъекту РФ с учетом его социокультурной специфики. Кроме того, именно на региональном уровне должен быть нормативно закреплен и реализован основной объем мероприятий профилактического характера, таких как повышение осведомленности граждан об угрозах ИПБ, обучение их методам защиты от таких угроз в Интернете и реальной жизни, внедрение программно-технических средств противодействия негативному контенту. Оптимальной формой правового закрепления таких мероприятий на региональном уровне выступают региональные целевые программы обеспечения информационной безопасности. Закон о защите детей от информации наделил региональные органы власти полномочиями по осуществлению комплекса мероприятий по обеспечению информационной безопасности детей.

Следующим важным вопросом методологического значения в рассматриваемой области является *вопрос о форме правового регулирования обеспечения ИПБ*. Речь идет о соотношении традиционного «жесткого права» (hard law) и «мягкого права» (soft law)[484] в нормативном регулировании отношений в рассматриваемой области. «Мягкое право» прежде всего проявляет себя здесь в актах саморегулирования в области СМИ (media self-regulation), в частности в кодексах этики (code of ethics).[485] Инициативы саморегулирования упомянуты в Окинавской хартии Глобального информационного общества от 21 июля 2000 г. как средство повышения доверия к электронным рынкам. Среди таких возможных инициатив упомянуты кодексы поведения, маркировка и другие программы подтверждения надежности.

Мы разделяем точку зрения исследователей ИГП РАН о том, что «борьба с распространением негативной информации и защита прав граждан от таких информационных угроз лежит во взаимодействии различных регуляторных механизмов, сочетания правового регулирования

[484] *Демин А. В.* «Мягкое право» в системе социального регулирования: постановка проблемы // Роль международных и внутригосударственных рекомендательных актов в правовой системе России: материалы круглого стола с международным участием (Иркутск, 26 апреля 2013 г.). Институт законодательства и правовой информации им. М. М. Сперанского. Иркутск, 2013. С. 26–34.

[485] The Media Self-Regulation Guidebook. All questions and answers. Organization for Security and Co-operation in Europe. Office of the Representative on Freedom of the Media. Vienna, 2008.

с организационным, этическим, техническим саморегулированием или сорегулированием».[486]

Согласно Федеральному закону от 1 декабря 2007 г. № 315-ФЗ «О саморегулируемых организациях»[487] формами саморегулирования являются стандарты и правила предпринимательской или профессиональной деятельности, обязательные для выполнения всеми членами саморегулируемой организации (ч. 3 ст. 3).

Понятие сорегулирования нормативно не определено. А. В. Минбалеев предлагает понимать под ним «комплексный механизм упорядочения общественных отношений, с помощью которого в результате взаимодействия государства и саморегулируемых организаций создается государственный или общественный орган, осуществляющий контроль за деятельностью тех или иных субъектов предпринимательской или профессиональной деятельности».[488]

В проанализированных нами международно-правовых актах, регламентирующих вопросы распространения информации в СМИ и Интернете, допускается как государственно-правовое, так и саморегулирование/сорегулирование, хотя в вопросах правового регулирования медиаконтента в документах Совета Европы и ОБСЕ делается акцент на саморегулировании. В зарубежных странах применяемые подходы значительно отличаются. В европейских государствах и США приоритет также отдан саморегулированию, а в странах Азии и Ближнего Востока первостепенным является государственно-правовое регулирование.

Данный вопрос неоднократно поднимался в нашей стране и приобрел особую остроту в связи с повышением роли Интернета. Автор неоднократно был свидетелем и участником подобных дискуссий, например в рамках ежегодного Форума безопасного Интернета, круглых столов в Государственной Думе.

Признавая высокую значимость саморегулирования медиаотрасли и интернет-сферы в системе противодействия вызовам и угрозам цифровой среды, мы считаем, что имеющиеся в нашей стране механизмы саморегулирования не способны в настоящий момент обеспечить надлежащую защиту гражданина и общества от таких угроз. Это обуславливается как декларативностью многих актов саморегулирования (Кодекса этических норм Общества профессиональных журналистов 1996 г., Хартии телерадиовещателей 1999 г., Хартии телерадиовещателей

---

[486] Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Под общ. ред. д. ю. н., профессора Т. А. Поляковой. Саратов: Амирит, 2020. С. 135.

[487] СЗ РФ. 2007. № 49. Ст. 6076.

[488] *Минбалеев А. В.* Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества: автореф. дис. … д-ра юрид. наук. Челябинск, 2012. С. 11.

«Против жестокости и насилия» 2005 г. и др.[489]), так и слабостью институциональных механизмов контроля саморегулируемых организаций медиаотрасли за их исполнением. К последним в разное время относились: Судебная палата по информационным спорам при Президенте России (1994–2000 гг.), Большое жюри Союза журналистов России (1998 г. – н. в.), Общественная комиссия по жалобам на прессу (2005 г. – н. в.).[490] Несмотря на их позитивный вклад в повышение качества работы СМИ и транслируемой информации, они не смогли выстроить мощную систему саморегулирования, которой государство могло бы делегировать часть функций по обеспечению ИПБ в СМИ. В этой связи принятие Закона о защите детей от информации было насущной необходимостью и средством устранения значительного пробела в праве.

Схожим образом обстоят дела и в российской интернет-отрасли. Хотя ее представителями (прежде всего крупнейшими интернет-компаниями – «Яндекс», Mail group, Microsoft, Google) в отсутствие государственной поддержки был добровольно предпринят ряд позитивных шагов по обеспечению безопасности интернет-отрасли, они так и не смогли выработать действенных актов саморегулирования в сфере Интернета.[491] А вносимые инициативы, такие как Хартия «Рунет против детской порнографии» 2007 г., Манифест РАЭК «Российский Интернет в XXI веке: безопасность детей» 2012 г. и др., оказались хорошо звучащими «декларациями о намерениях». Они явно уступают рассмотренным нами европейским аналогам – Европейским правилам безопасного использования мобильной связи детьми и подростками 2007 г. и Принципам безопасного использования социальных сетей в ЕС 2009 г., поскольку, в отличие от последних, не закрепляют конкретных обязательств интернет-индустрии и (или) механизма контроля за их соблюдением.

Такое положение дел в области саморегулирования Интернета в России вынудило государство пойти на принятие системы мер государственно-правового регулирования по обеспечению ИПБ в киберпространстве. Они включали учреждение нескольких организационно-правовых механизмов ограничения информации в сети Интернет,

---

[489] Общественная комиссия по жалобам на прессу. Раздел «Документы». URL: http://www.presscouncil.ru/index.php/teoriya-i-praktika/dokumenty (дата обращения: 12.08.2021).

[490] *Мамонтова О.* Организации саморегулирования СМИ в России // Общественная комиссия по жалобам на прессу. 14.07.2013. URL: https://www.presscouncil.ru/teoriya-i-praktika/knigi-i-stati/1905-organizatsii-samoregulirovaniya-smi-v-rossii (дата обращения: 21.11.2021).

[491] В 2003 г. В. Б. Наумов в своей диссертации констатировал низкий уровень механизмов саморегулирования Интернета в России. Хотя с тех пор ситуация в целом существенно изменилась, такие механизмы в интересующей нас области не получили должного развития. См.: *Наумов В. Б.* Правовое регулирование распространения информации в сети Интернет: автореф. дис. … канд. юрид. наук. Екатеринбург, 2003. С. 14.

закрепление правовых обязанностей ключевых информационных посредников и установление мер юридической ответственности за их невыполнение.

Важным шагом государства стало дополнение Закона об информации статьей 10.6, регламентирующей особенности распространения информации в социальных сетях. Нормы данной статьи впервые в российской правовой практике закрепили обязательства владельцев социальных сетей по осуществлению самостоятельного мониторинга публикуемой информации и удалению выявленного противоправного контента. Кроме того, ими были регламентированы требования по содержанию и публичному размещению правил пользования социальной сетью. Согласно ч. 2 ст. 10.6 Закона об информации правила использования социальной сети должны содержать: а) требования к распространению в социальной сети информации; б) права и обязанности владельца и пользователей социальной сети; в) порядок рассмотрения обращений пользователей; г) алгоритм мониторинга социальной сети в целях выявления противоправной информации, а также рассмотрения обращений о выявлении такой информации.

Вместе с тем перспективы саморегулирования в интернет-отрасли выглядят вполне оптимистичными, поскольку здесь имеется достаточно мощный и авторитетный институт представительства ее интересов – Российская ассоциация электронных коммуникаций (РАЭК).[492] Представляется возможной организация на ее основе некой платформы (например, комиссии) по саморегулированию Интернета.

Однако, исходя из реалий сегодняшнего дня, следует сделать вывод о том, что *приоритет в правовом регулировании обеспечения ИПБ в СМИ и сети Интернет должен быть за государством. Отраслевое саморегулирование в данных сферах должно дополнять законодательное регулирование, дабы предотвратить его избыточность и чрезмерное вмешательство государства в деятельность СМИ и субъектов интернет-индустрии. По мере укрепления механизмов отраслевого саморегулирования в России вполне возможен трансферт части регулятивных полномочий от государства к негосударственным корпоративным институтам.*

В заключение отметим еще один важный аспект. Часто дискуссии по данной проблеме напоминают «перетягивание каната» между сторонниками государственного регулирования и корпоративного саморегулирования. То есть ключевым ее вопросом становится, какую из двух моделей выбрать? Однако при этом зачастую упускается из виду, что речь идет лишь о выборе формы правовой регламентации, эффективность которой будет зависеть от ее содержательного наполнения. Поэтому вне зависимости от выбранного приоритета важным является объединение

[492] Российская ассоциация электронных коммуникаций. URL: http://raec.ru/.

усилий всех заинтересованных сторон (государства, медиаотрасли, институтов гражданского общества и науки) для совместной выработки и реализации правил поведения в интересах создания цифровой среды доверия. Проходящий красной нитью через все изученные нами документы Европейского союза многосторонний подход (multistakeholder approach) к обеспечению безопасности в информационной сфере должен быть воплощен в жизнь и в нашей стране.

Исследование моделей правового регулирования обеспечения ИПБ также предполагает *изучение роли иных социальных регуляторов в данной сфере*. Ведущие ученые в области информационного права указывают на возрастание роли таких регуляторов в условиях цифровой трансформации. Так, по мнению А. В. Минбалеева, в современных условиях цифровые технологии вынуждают право «трансформироваться и взаимодействовать с другими регуляторами».[493] Г. Г. Камалова также отмечает, что «развитие общественных отношений в информационной сфере показывает значимость этических норм и саморегулирования, связанных с прорывными цифровыми технологиями».[494]

В юридической науке все действующие в обществе нормы разделяют на две большие группы – социальные и технические. При этом группа социальных норм, в свою очередь, подразделяется на правовые, моральные, политические, эстетические, религиозные, семейные, корпоративные, нормы обычаев, традиций, привычек и т. д.[495]

В механизме обеспечения ИПБ наибольшую значимость имеют моральные, эстетические и другие социальные нормы, относящиеся к сфере культуры. Многие из них выступают защитными механизмами культуры,[496] обеспечивающими устойчивость и выживаемость общества. Именно в культуре содержатся те базовые ценности и мировоззренческие установки, выработанные в ходе многовекового развития российской нации, которые выступают самым надежным барьером на пути проникновения деструктивных идей, взглядов, установок. В ней же заложены и мощные инструменты защиты своего «культурно-цивилизационного ядра» и противодействия его эрозии и разрушения.

---

[493] Цифровое право: учебник / Под ред. В. В. Блажеева, М. А. Егоровой. М.: Проспект, 2020. С. 123.

[494] Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и роботехники: монография / Под общ. ред. к. ю. н. В. Б. Наумова. СПб.: НП-Принт, 2020. С. 73.

[495] Теория государства и права: Курс лекций / Под ред. Н. И. Матузова и А. В. Малько. С. 320–326.

[496] *Штроо В. А.* Защитные механизмы групповой динамики в организационном контексте // Психология. Журнал Высшей школы экономики. 2007. Т. 4. № 1. С. 151–157; *Давыдов А. И.* Защитные механизмы цивилизации // Гуманитарные исследования. 2016. № 4. С. 21–24; *Костина А. В., Макаревич Э. Ф., Карпухин О. И., Луков В. А.* Культура как фактор национальной безопасности современной России: значение и ролевая модель. М.: Ленанд, 2021.

Ключевую роль в механизме обеспечения ИПБ играет мораль. Она определяется как форма общественного сознания, которая «регулирует поведение человека во всех сферах общественной жизни, поддерживая и санкционируя определенные общественные устои, строй жизни, общение».[497] Мораль «обобщает тот срез человеческого опыта, разные стороны которого обозначаются словами „добро" и „зло", „добродетель" и „порок", „правильное" и „неправильное", „долг", „совесть", „справедливость" и т. д.»[498]

Мораль (нравственность) выступает весьма значимым источником нормативного регулирования ИПБ, поскольку содержит в себе целый свод правил и установок, сдерживающих оказание деструктивного ИПВ. Это касается как распространения непристойной информации (пошлости, жестокости, откровенной эротики и т. п.), так и обмана, унижения, запугивания и иных форм негативной коммуникации. Причем нормы морали, выработанные в ходе длительного исторического развития нашей страны, содержат гораздо более широкий перечень запретов и ограничений, чем правовые нормы. Поэтому поддержание и укрепление морали выступает императивом обеспечения ИПБ.

Вместе с тем в современном глобальном информационном обществе нормы морали, как и иные социальные нормы, подвержены мощной эрозии. Это обусловлено целым рядом факторов, включая глобализацию, свободный доступ к любой информации, ускорение социальной динамики и др. Поэтому в ряде случаев для обеспечения соблюдения важных нравственных норм используются механизмы юридической ответственности. В действующем УК РФ имеется глава 25 «Преступления против здоровья населения и общественной нравственности», хотя составы преступлений, нарушающих общественную нравственность, содержатся и в других главах уголовного закона. Более того, после целого ряда резонансных происшествий российский законодатель прибегнул к мерам уголовной ответственности за публичные действия, выражающие явное неуважение к обществу и совершенные в целях оскорбления религиозных чувств верующих (ч. 1 ст. 148 УК РФ), и за распространение выражающих явное неуважение к обществу сведений о днях воинской славы и памятных датах России, связанных с защитой Отечества, а равно осквернение символов воинской славы России, оскорбление памяти защитников Отечества либо унижение чести и достоинства ветерана Великой Отечественной войны, совершенные публично (ч. 3 ст. 354.1 УК РФ).

Однако в современных условиях, помимо морали как формы общественного сознания, источниками социального регулирования

[497] Мораль // Философский словарь / Под ред. И. Т. Фролова. С. 342.

[498] Мораль // Новая философская энциклопедия. В 4 т. Институт философии РАН; Национальный общественно-научный фонд; Председатель научно-редакционного совета В. С. Степин. М.: Мысль, 2000–2001. URL: https://iphlib.ru/library/collection/newphilenc/document/HASH0c180705923b860f63380c?p.s=TextQuery (дата обращения: 23.11.2021).

выступают и документально зафиксированные этические нормы. Речь идет об этическом регулировании, представляющем собой «установление правил поведения для определенного сообщества, соблюдение которых обеспечивается не государством, а соответствующим сообществом (социальным, профессиональным и др.)».[499] Средствами такого регулирования, по мнению М. А. Рожковой, становятся различные нормы, кроме действующих правовых, то есть это могут быть упомянутые корпоративные нормы, нормы морали, обычаи и т. д. Оно осуществляется в виде закрепления основополагающих принципов и общих правил и рассчитано на определенное сообщество граждан и (или) юридических лиц.[500]

Примером акта этического регулирования является принятый в конце 2021 г. *Кодекс этики в сфере искусственного интеллекта*.[501] Документ 26 октября 2021 г. подписали участники Альянса в сфере искусственного интеллекта: Сбербанк, «Газпром нефть», «Яндекс», VK, МТС, Российский фонд прямых инвестиций, представители Сколково, «Ростелекома», Росатома, InfoWatch и ЦИАН.[502] Кодекс устанавливает общие этические принципы и стандарты поведения в сфере использования искусственного интеллекта (далее – ИИ).

В тексте документа закреплены шесть основных принципов этики в сфере ИИ: 1) главный приоритет развития технологий ИИ в защите интересов и прав людей и отдельного человека; 2) необходимо осознавать ответственность при создании и использовании ИИ; 3) ответственность за последствия применения систем ИИ всегда несет человек; 4) технологии ИИ нужно применять по назначению и внедрять там, где это принесет пользу людям; 5) интересы развития технологий ИИ выше интересов конкуренции; 6) важна максимальная прозрачность и правдивость в информировании об уровне развития технологий ИИ, их возможностях и рисках. Изучение данных принципов и раскрывающих их содержание правил позволяет сделать вывод, что они касаются и перспективных аспектов ИПБ, в частности коммуникации человека с системами ИИ.

Следует отметить, что механизмы этического регулирования давно применяются в области СМИ и Интернета. Так, большинство упомянутых нами российских актов саморегулирования медиаотрасли (Кодекс этических норм Общества профессиональных журналистов 1996 г., Хартия телерадиовещателей 1999 г., Хартия телерадиовещателей «Против

[499] *Рожкова М. А.* О правовых аспектах использования технологий: RegTech и SupTech // Хозяйство и право. 2020. № 6. С. 7.

[500] Там же. С. 7–8.

[501] Текст Кодекса размещен на сетевом ресурсе проекта «Берза». URL: https://berza.ru/wp-content/uploads/2021/10/kodeks-etiki-v-sfere-iskusstvennogo-intellekta.pdf (дата обращения: 26.12.2021).

[502] Российские компании подписали кодекс этики искусственного интеллекта // Право.ру. 26 октября 2021 г. URL: https://pravo.ru/news/236149/ (дата обращения: 26.12.2021).

жестокости и насилия» 2005 г.) можно отнести к документам этического регулирования. Помимо этих документов, Общественной коллегией по жалобам на прессу (далее – Коллегия) приняты *Медиаэтический стандарт 2015 г.*[503] и *Новомедийный стандарт 2020 г.*[504]

В преамбуле Медиаэтического стандарта Коллегия выразила убеждение, что «следование выделяемым в „стандарт Коллегии"… принципам, нормам и правилам поведения конкретных журналистов и конкретных редакций существенно сокращает риск появления информационных споров, укрепляет свободу СМИ и доверие к ним, отвечает интересам российских граждан и российского общества в целом». В документе выделено восемь важных принципов, включая обеспечение права граждан на информацию, профессиональной и социальной ответственности журналиста, добросовестного освещения событий, уважения частной жизни и человеческого достоинства и др. В более позднем Новомедийном стандарте сформулирован ряд важных дополнительных правил и установок для журналистов, напрямую относящихся к сфере ИПБ. Среди них: быть правдивым, держаться в стороне от пропаганды, ссылаться на источники, отделять факты от мнений, исправлять ошибки и др.

Этическое регулирование имеет важное значение и для интернет-отрасли. Выше мы отмечали принятие хартии «Рунет против детской порнографии» 2007 г. и манифеста РАЭК «Российский Интернет в XXI веке: безопасность детей» 2012 г., которые правомерно отнести к источникам этических норм. 27 ноября 2021 г. состоялось важное событие: российские интернет-компании, медиахолдинги и телеком-операторы из недавно созданного Альянса по защите детей в цифровой среде подписали *хартию «Цифровая этика детства»*[505] (далее – Хартия). Среди подписантов документа такие крупные IT-компании, как Mail.ru Group, «Яндекс», «Лаборатория Касперского», Национальная Медиа Группа, «Газпром-Медиа Холдинг», «МегаФон», «Ростелеком», МТС, «Вымпелком».[506] При этом Хартия открыта для присоединения других потенциальных участников.

В Хартии выделены пять принципов цифровой этики детства: 1) уважение ребенка как личности; 2) совместная ответственность; 3) сохранение конфиденциальности; 4) инклюзивный подход; 5) сохранение ценностных ориентиров в онлайн-пространстве. Как видно, данные

[503] Общественная коллегия по жалобам на прессу URL: https://www.presscouncil.ru/teoriya-i-praktika/dokumenty/4756-mediaeticheskij-standart-2015 (дата обращения: 12.07.2021).

[504] Общественная коллегия по жалобам на прессу URL: https://www.presscouncil.ru/teoriya-i-praktika/dokumenty/6267-novomedijnyj-standart-kolllegii-po-zhalobam-na-pressu (дата обращения: 12.07.2021).

[505] Текст Хартии размещен на сайте Альянса по защите детей в цифровой среде. URL: https://internetforkids.ru/charter/ (дата обращения: 30.11.2021).

[506] Российские компании подписали хартию безопасности детей в интернете // Коммерсант. 29.11.2021. URL: https://www.kommersant.ru/doc/5099594 (дата обращения: 30.11.2021).

принципы носят достаточно общий характер. Более подробно они раскрыты в следующем разделе Хартии под названием «Основы цифровой этики детства». Такие основы сформулированы как система обязательств участников Хартии в рамках нескольких выделенных приоритетов.

В целом Хартия носит весьма позитивный характер и оценивается нами как значимый этический акт в сфере обеспечения ИПБ. Вместе с тем она явно не претендует на полноценный акт отраслевого саморегулирования, поскольку, как и предыдущие схожие документы, не содержит четких обязательств со стороны компаний IT-отрасли по мерам обеспечения безопасности детей в цифровом пространстве.

Другую большую группу регуляторов составляют *технические нормы*. К ним в широком смысле относят биологические, санитарно-гигиенические, санитарно-эпидемиологические, технологические, научно-технические, экологические и др.[507] При этом часть данных норм находит закрепление в правовых актах и именуется технико-юридическими. Именно в таком ключе определяет техническое регулирование профильный федеральный закон,[508] согласно которому под ним понимается «правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции или к продукции и связанным с требованиями к продукции процессам… и правовое регулирование отношений в области оценки соответствия».

В науке же применяется иной подход, основанный на разграничении правового и технического регулирования. Так, М. А. Рожкова трактует техническое (нормативное) регулирование как «установление технических требований и стандартов, которые предъявляются к продукции, а также к производственным, технологическим, логистическим и иным процессам».[509] При этом автор проводит разграничение между правовыми и техническими нормами, отмечая, что последние содержатся в технических стандартах, принимаемых государственными органами или неправительственными организациями.[510]

В. Б. Наумов в своей диссертации отмечал тенденцию проникновения технических норм в информационное право и увеличения значения актов технического регулирования, обусловленную «высокой взаимосвязью информационной сферы с цифровыми технологиями и зависимостью правового регулирования информационных отношений от особенностей технологий и архитектуры сетей и систем».[511]

---

[507] *Червонюк В. И.* Теория государства и права: учебник. М.: ИНФРА-М, 2006. С. 295.

[508] Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» // СЗ РФ. 2002. № 52. Ст. 5140.

[509] *Рожкова М. А.* О правовых аспектах использования технологий: RegTech и SupTech // Хозяйство и право. 2020. № 6. С. 5.

[510] Там же.

[511] *Наумов В. Б.* Институт идентификации в информационном праве: дис. … д-ра юрид. наук. М., 2020. С. 242.

Хотя в целом в сфере обеспечения информационной безопасности значение актов технического регулирования весьма велико, большинство из них относится к направлению защиты информации (информационно-технической безопасности). Что же касается области ИПБ, то технические нормы преимущественно регламентируют достаточно узкую область защиты человека от деструктивного ИПВ, исходящего от технических средств. Прежде всего речь идет о технических нормативах предотвращения негативного влияния на человека электромагнитного и оптического излучения, теле- и радиовещания, акустических сигналов, специфических компьютерных вирусов.[512] В качестве примеров можно привести несколько межгосударственных стандартов и санитарных правил.[513] Государственной комиссией по радиочастотам при Минцифры России было принято решение от 29 ноября 2021 г. № 21-60-01 «Об утверждении норм параметров радиоизлучений (приема) радиоэлектронных средств, влияющих на их электромагнитную совместимость с другими радиоэлектронными средствами».[514] Им, в частности, утверждены нормы 18-21 «Радиопередающие устройства гражданского назначения. Требования на допустимые уровни побочных излучений».

Однако изучение содержания указанных актов технического регулирования показывает, что они скорее касаются защиты физического здоровья человека, нежели психики от излучений различных типов. Полагаем, что это отчасти объясняется недостаточной изученностью вопроса оказания деструктивного ИПВ со стороны излучения и иных сигналов от технических устройств. Поэтому направление технического регулирования в механизме обеспечения ИПБ требует дальнейшего развития.

§ 4. Юридическая ответственность в сфере обеспечения информационно-психологической безопасности

Одним из важнейших механизмов правового обеспечения ИПБ выступают меры юридической ответственности за совершение правонарушений в рассматриваемой области. Посредством применения мер государственно-принудительного воздействия гарантируется реализация

---

[512] См.: *Рысин Ю. С.* Социально-информационные опасности телерадиовещания и информационных технологий: учеб. пособие для вузов. М.: Гелиос АРВ, 2007.

[513] ГОСТ 12.1.006–84 «Электромагнитные поля радиочастот. Допустимые поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля», ГОСТ EN12198–1–2012 «Безопасность машин. Оценка и уменьшение опасности излучения, исходящего от машин», ГОСТ 12.4.305–2016 «Система стандартов безопасности труда. Комплект экранирующий для защиты персонала от электромагнитных полей радиочастотного диапазона. Общие технические требования», СанПиН 1.2.3685–21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» и др.

[514] Электронный фонд актуальных правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/727265115#64S0IJ (дата обращения: 23.11.2021).

правовых норм, регламентирующих поддержание состояния защищенности личности, социальных групп и общества от деструктивного ИПВ.

Юридическую ответственность обычно определяют как «применение мер государственного принуждения к правонарушителям для восстановления нарушенного правопорядка и (или) наказания лица, совершившего правонарушение».[515] Она выступает основным способом реализации регулятивно-охранительной функции права, содержанием которой являются «предупреждение и пресечение преступлений и иных правонарушений, защита и восстановление нарушенного права».[516]

И. Л. Бачило подчеркивала, что институт ответственности выступает общим правовым институтом, но применительно к сфере информационных правоотношений он неизбежно оснащается специальными методами и средствами. Она определяла его как «систему норм и процедур, реализуемых в целях пресечения правонарушений и установления вида, формы и мер наказания за совершенные и доказанные преступления или иные правонарушения с учетом их социального вреда и вины правонарушителя».[517]

Д. Д. Савенкова обосновала вывод о межотраслевом характере института юридической ответственности за правонарушения в сфере информационной безопасности.[518] Автор разделяет данную позицию и считает ее справедливой в отношении ИПБ как составной части информационной безопасности.

Основополагающее значение для определения юридической ответственности в информационной сфере имеет ст. 17 Закона об информации. Согласно ч. 1 указанной статьи «нарушение требований данного закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ». Таким образом, Законом об информации установлены четыре вида юридической ответственности за нарушение его норм. Хотя отрасль информационного законодательства не исчерпывается одним Законом об информации, данное правило распространяется на нее в целом.

В силу специфики правовых отношений в области обеспечения ИПБ, выражающих преимущественно публичные интересы, основную роль в механизме их правовой охраны играют нормы уголовного и административно-деликтного законодательства. В условиях активного развития

---

[515] Проблемы теории государств и права: учебное пособие / Под ред. М. Н. Марченко. М.: Юрист, 2005. С. 626.

[516] *Байтин М. И.* Сущность права (Современное нормативное правопонимание на грани двух веков). 2-е изд., доп. М.: ООО ИД «Право и государство», 2005. С. 170.

[517] *Бачило И. Л.* Информационное право: учебник для магистров. М.: Юрайт, 2015. С. 506–507.

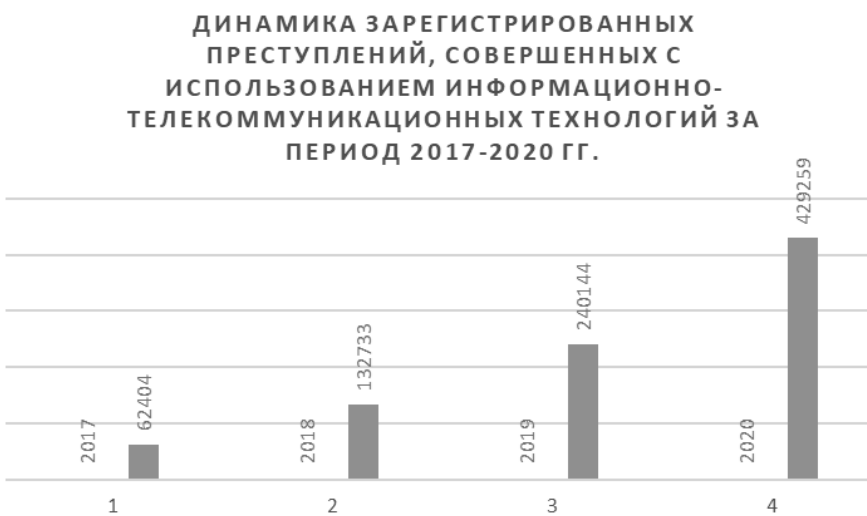
[518] *Савенкова Д. Д.* Институт юридической ответственности в системе правового обеспечения информационной безопасности: автореф. дис. … канд. юрид. наук. М., 2019. С. 11.

информационного общества именно риски цифровой среды выступают одним из ключевых драйверов модернизации УК и КоАП РФ.

Начнем рассмотрение с вопросов уголовной ответственности. *Уголовная ответственность* устанавливается за совершение преступлений в сфере ИПБ, то есть общественно опасных деяний, связанных с оказанием деструктивного ИПВ, запрещенных УК РФ под угрозой наказания.

В целом в последние годы количество преступлений, совершенных с использованием ИКТ, неуклонно растет, причем очень высокими темпами[519] (см. диаграмму 1). В 2021 г. зарегистрировано 517,7 тыс. преступлений данной категории, их удельный вес в общем количестве зарегистрированных преступлений увеличился до 25,8%. Более двух третей (67,9%) таких преступлений совершается с использованием сети Интернет, более трети (42,0%) – с помощью средств мобильной связи. Более чем три четверти таких преступлений (78,4%) составляют кражи и мошенничества.[520]

Диаграмма 1



Изложенная статистика убедительно доказывает активное использование правоохранительными органами статей УК РФ об ответственности за преступления, связанные с использованием ИКТ. Однако в интересующие нас составы преступлений, связанные с оказанием деструктивного

[519] Данные сборников «Состояние преступности в России» ГИАЦ МВД России за 2017–2021 гг. Ист.: Статистика и аналитика // МВД России. URL: https://мвд.рф/Deljatelnost/statistics (дата обращения: 08.01.2022).

[520] Состояние преступности в России за январь – декабрь 2021 г. ГИАЦ МВД России.

ИПВ, входят и другие категории преступлений, например преступления террористического характера и экстремистской направленности.

Проведенный нами ранее анализ норм Особенной части УК РФ показал, что в ней закреплено большое количество составов преступлений, содержанием которых выступают различные виды деструктивного ИПВ, причем как информационного (контентного), так и коммуникационного характера. В большинстве случаев описанное в диспозиции статей УК РФ деяние может проявлять себя одновременно в обоих указанных «регистрах», то есть осуществляться как посредством распространения информации, так и путем коммуникации (клевета, оскорбление, пропаганда терроризма, публичные призывы к совершению преступлений и др.). Значительно реже составы включают в себя только одну форму проявления угроз ИПБ (изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних как пример контентной формы и вовлечение несовершеннолетнего в совершение преступления – как пример коммуникационной).

Несмотря на абсолютное преобладание гибридных форм преступных деяний в диспозициях статей УК РФ, обоснованное нами разграничение двух основных форм угроз является юридически значимым. Например, когда в России остро встал вопрос противодействия деструктивным суицидальным сообществам, подстрекающим детей к совершению самоубийства (2016–2017 гг.), то законодатель ввел не один, а два новых состава в УК РФ.[521] Статья 110.1 «Склонение к совершению самоубийства или содействие совершению самоубийства» принята для привлечения к ответственности так называемых «кураторов» суицидальных сообществ, склонявших детей к самоубийству путем общения в социальных сетях и мессенджерах, тогда как ст. 110.2 «Организация деятельности, направленной на побуждение к совершению самоубийства» закреплена для привлечения к ответственности создателей и администраторов тематических информационных ресурсов в Интернете (пабликов, каналов и групп), которые непосредственно в общение с детьми не вступали. Такой способ позволил Управлению «К» и иным профильным подразделениям МВД России эффективно пресекать деятельность созданной виртуальной сети, подстрекавшей детей к суицидам.

Анализ статей УК РФ также показал, что оказание деструктивного ИПВ преимущественно закреплено как само преступное деяние (распространение материалов, публичные призывы, вербовка и иное вовлечение и т. п.), хотя в некоторых случаях является способом

[521] Федеральный закон от 7 июня 2017 г. № 120-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению» // СЗ РФ. 2017. № 24. Ст. 3489.

совершения преступлений (обман или злоупотребление доверием как способ хищения в мошенничестве).

Особо стоит сказать о правовой категории «психическое насилие», которая охватывает комплекс уголовно-наказуемых видов деструктивного ИПВ. Л. Н. Клоченко определяет уголовно-наказуемое психическое насилие как «противоправное общественно опасное воздействие (способ выполнения деяния) на психику другого лица (или группы лиц) помимо или против его (их) воли, совершаемое с прямым умыслом и способное причинить или причиняющее ему (им) психический, физический или материальный вред (ущерб)».[522] Исследователь указывает, что психическое насилие в закрепленных уголовным законодательством составах преступлений может выступать и как способ совершения преступления, и как одна из характеристик обстановки содеянного, и как последствие преступления.[523] При этом Л. Н. Клоченко отмечает пробельность норм УК РФ в части криминализации реальных проявлений опасного психического насилия, в частности навязчивого преследования.[524] Мы разделяем точку зрения автора и поддерживаем его предложение о дополнении УК РФ статьей об ответственности за преследование.

В действующей редакции УК РФ отсутствуют специальные статьи об ответственности за оказание деструктивного ИПВ в форме сигналов от технических устройств. Однако такие формы деструктивного ИПВ можно имплицитно усмотреть в качестве способов совершения целого ряда преступлений, связанных с причинением вреда жизни и здоровью человека. В качестве примера можно привести необычный, но достаточно резонансный случай, произошедший в Нижнем Новгороде. Там в июле 2021 г. Московским районным судом был осужден мужчина по ч. 2 ст. 117 УК РФ за совершенные истязания в отношении двух и более лиц. Способ такого истязания весьма необычен – систематическое включение в квартире жилого многоэтажного дома громких звуков лошадиного ржания.[525]

В последнее десятилетие законодатель активно прибегал к уголовно-правовым инструментам для противодействия различным формам деструктивного ИПВ. Например, в УК РФ были введены упомянутые ст. 110.1 и ст. 110.2 (2017 г.), ст. 151.2 «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего» (2017 г.), ст. 207.1 «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих

[522] *Клоченко Л. Н.* Психическое насилие: вопросы уголовно-правовой регламентации и квалификации: дис. … канд. юрид. наук. М., 2019. С. 9.

[523] Там же. С. 8–9.

[524] Там же. С. 10.

[525] Вот и посмеялись: суд вынес приговор Юрию Кондратьеву, мучившему соседей конским ржанием на протяжении двух лет // Комсомольская правда. Нижний Новгород. 10 июля 2021 г. URL: https://www.nnov.kp.ru/daily/28301/4442393/ (дата обращения: 12.09.2021).

угрозу жизни и безопасности граждан» (2019 г.), ст. 207.2 «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия» (2019 г.) и др. На повестке дня вопросы установления уголовной ответственности за новые формы деструктивного ИПВ – «треш-стримы»[526] и глубокие фейки.[527]

Вторым видом юридической ответственности за совершение правонарушений в области ИПБ выступает *административная ответственность*. В отличие от уголовной ответственности ее основанием может выступать не только совершение противоправных деяний, связанных с оказанием деструктивного ИПВ, но и с нарушением установленных правил в рассматриваемой области (данный признак определяется отраслевой спецификой). Последняя категория составов административных правонарушений содержится преимущественно в главе 13 «Административные правонарушения в области связи и информации» КоАП РФ.

Несмотря на меньшую общественную опасность в сравнении с преступлениями, административные правонарушения в рассматриваемой нами сфере заслуживают серьезного внимания. А. П. Шергин справедливо подчеркивает недопустимость недооценки опасности административных правонарушений, остающихся «наиболее распространенными видами противоправного поведения».[528]

При составлении перечней противоправного контента и коммуникации нами были отмечены основные статьи КоАП РФ, устанавливающие наказания за совершение административных правонарушений, связанных с оказанием деструктивного ИПВ: 5.61 «Оскорбление», 5.61.1 «Клевета», 6.13 «Пропаганда наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ», 20.1 «Мелкое хулиганство», 20.3 «Пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами», 20.29 «Производство и распространение экстремистских материалов» и др.

Одной из наиболее значимых в структуре КоАП РФ выступает упомянутая выше глава 13. В ней закреплено большое количество статей

[526] См.: Мучителей блокируют. Закон о запрете треш-стримов будет принят к лету // Российская газета. 11.02.2021. URL: https://rg.ru/2021/02/11/zakon-o-zaprete-tresh-strimov-budet-priniat-k-letu.html (дата обращения: 12.04.2021).

[527] Информацию о подготовке такого законопроекта в 2020 г. автору в личной беседе сообщил координатор Центра безопасного Интернета в России У. У. Парфентьев. Однако проект документа до сих пор не оформлен в виде официальной законодательной инициативы.

[528] *Шергин А. П.* Концептуальные основы административно-деликтного права // Научный портал МВД России. 2008. № 1. С. 14.

касательно ответственности за правонарушения в сфере ИПБ. В первую очередь выделим ст. 13.15 «Злоупотребление свободой массовой информации», которая устанавливает административную ответственность за различные формы злоупотребления свободой СМИ. Причем часть содержащихся в этой статье составов правонарушений связана с распространением информации не только в СМИ, но и в информационно-телекоммуникационных сетях, включая сеть Интернет. Именно в данную статью в 2019 г. были внесены составы правонарушений, связанные с распространением фейковой информации[529] (ч. 9–11).

Также отметим ст. 13.21 «Нарушение порядка изготовления или распространения продукции средства массовой информации» КоАП РФ, устанавливающую ответственность за нарушение ряда требований Закона о защите детей от информации. Помимо нее ответственность за нарушение требований данного закона предусмотрена ст. 6.17 «Нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию» и ст. 19.5 «Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль)».

Одним из дискуссионных аспектов юридической ответственности за правонарушения в информационной сфере является *вопрос ответственности информационных посредников*. В российском законодательстве он преимущественно относится к области административной ответственности.

Как отмечает А. К. Жарова, традиционно было принято выделять три категории посредников (провайдеров): провайдеры содержания (контент), провайдеры хостовых услуг и провайдеры доступа. Позже к ним добавились провайдеры в рамках операции по идентификации пользователей.[530] В диссертации Р. Т. Нурулаева также выделены информационные посредники, осуществляющие кеширование и поиск информации.[531]

В российском законодательстве понятие информационного посредника напрямую закреплено в ст. 1253.1 ГК РФ,[532] в которой выделены три вида таких посредников.[533] Закон об информации само понятие

---

[529] Федеральный закон от 18 марта 2019 г. № 27-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СЗ РФ. 2019. № 12. Ст. 1217.

[530] *Жарова А. К.* Право и информационные конфликты в информационно-телекоммуникационной сфере. М.: Янус-К, 2016. С. 103–104.

[531] *Нурулаев Р. Т.* Информационный посредник как субъект информационного права: дис. … канд. юрид. наук. НИУ ВШЭ. М., 2018. С. 9.

[532] Гражданский кодекс Российской Федерации (часть четвертая) от 18 декабря 2006 г. № 230-ФЗ // СЗ РФ. 2006. № 52. Ст. 5496.

[533] Триаду таких информационных посредников составляют: 1) лицо, осуществляющее передачу материала в информационно-телекоммуникационной сети, в том числе в сети «Интернет»; 2) лицо, предоставляющее возможность размещения материала

информационных посредников не использует, хотя регламентирует правовой статус их конкретных видов: ОРИ (ст. 10.1), организатора сервиса обмена мгновенными сообщениями (ст. 10.1), оператора поисковой системы (ст. 10.3), владельца новостного агрегатора (ст. 10.4), владельца аудиовизуального сервиса (ст. 10.5), владельца социальной сети (ст. 10.6).

Глава 13 КоАП РФ как раз регламентирует вопросы административной ответственности информационных посредников за невыполнение требований информационного законодательства[534] для: оператора связи (ст. 13.2.1, 13.30, 13.34), ОРИ (ст. 13.31), владельца новостного агрегатора (ст. 13.32), владельца аудиовизуального сервиса (ст. 13.35, 13.36, 13.37), организатора сервиса обмена мгновенными сообщениями (ст. 13.39), оператора поисковой системы (ст. 13.40), провайдера хостинга (ст. 13.41), владельца сайта/информационного ресурса в сети „Интернет" (ст. 13.41). В качестве наказания за совершение указанных правонарушений предусмотрен административный штраф.

Учитывая длительное и систематическое игнорирование зарубежными информационными компаниями (Google, Facebook, Twitter и др.) требований российских властей об удалении противоправного контента, законодатель пошел на закрепление больших размеров штрафа, исчисляемых миллионами рублей, за такие правонарушения (ст. 13.41 КоАП РФ). Более того, при повторном совершении данных правонарушений для информационных компаний предусмотрен кратный штраф, исчисляемый в виде части от годовой совокупной суммы выручки. Данные нормы впервые были применены в России в конце 2021 г. Мировым судом Таганского района г. Москвы за повторное нарушение порядка ограничения доступа к противоправному контенту компаниям Google LLC и Facebook Inc. назначены штрафы, составляющие долю от их выручки за год в России, – 7,22 млрд рублей и 1,99 млрд рублей соответственно.[535] Столь большие штрафы чувствительны даже для названных IT-гигантов, что позволяет надеяться на изменение занятой ими позиции по игнорированию требований Роскомнадзора об удалении запрещенной информации.

КоАП РФ закрепляет состав административного правонарушения, связанного с оказанием деструктивного ИПВ на подсознание человека (ч. 1 ст. 13.15). Источником угроз здесь выступают сведения (например, текстовая информация при ее подпороговом предъявлении) и другие

или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети; 3) лицо, предоставляющее возможность доступа к материалу в этой сети.

[534] Нами приведены статьи КоАП РФ, закрепляющие составы административных правонарушений, связанных с нарушением требований Закона о связи, Закона об информации, Закона о СМИ и Закона о защите детей от информации, касающихся обеспечения ИПБ.

[535] Российский суд впервые назначил Google и Facebook оборотные штрафы за неудаление запрещенной информации // Роскомнадзор. 24 декабря 2021 г. URL: https://rkn.gov.ru/news/rsoc/news73996.htm (дата обращения: 10.01.2022).

виды информации (например, акустические сигналы определенной частоты), воздействующие на подсознание человека. Проведенный нами подробный анализ данной статьи показал, что в настоящее время фактически отсутствует полноценный механизм ее практической реализации.[536] Поэтому за многие годы зафиксированы лишь единичные факты привлечения к ответственности за данное правонарушение. Поскольку сами средства воздействия на бессознательное не только существуют, но и совершенствуются, необходима проработка вопроса о механизме мониторинга на предмет выявления скрытых вставок в информационной продукции, включая интернет-контент.

Завершая рассмотрение блока уголовной и административной ответственности в сфере обеспечения ИПБ, отметим наличие достаточно тесной связи между ними. Она проявляется в нескольких аспектах:

а) декриминализации ряда преступлений и переводе их в состав административных правонарушений (например, декриминализация оскорбления в 2011 г. и включение данного состава в КоАП РФ, ст. 5.61);

б) наличии схожих составов правонарушений в УК и КоАП РФ, различающихся определенными признаками – субъектом правонарушения, тяжестью последствий и др. (например, закрепление составов клеветы в ст. 128.1 УК РФ для физических лиц и ст. 5.61.1 КоАП РФ для юридических лиц);

в) использовании механизма административной преюдиции (например, после внесенных изменений в законодательство в 2018 г. первичное совершение действий по разжиганию ненависти или вражды влечет административную ответственность по ст. 20.3.1 КоАП РФ, а повторное – уголовную ответственность по ст. 282 УК РФ).

Роль гражданско-правовой ответственности в правовом механизме обеспечения ИПБ незначительна. Здесь прежде всего применимы нормы ГК РФ о компенсации морального вреда (ст. 151), защите чести, достоинства и деловой репутации (ст. 152) и обязательствах вследствие причинения вреда (ст. 1064–1083).

Полагаем целесообразным коснуться вопроса, который часто обходят вниманием при анализе механизмов юридической ответственности в информационной сфере. Речь идет об *информационно-правовой ответственности* как самостоятельном виде юридической ответственности. На наш взгляд, ряд мер государственного принуждения, закрепленных непосредственно информационным законодательством, можно считать мерами информационно-правовой ответственности, причем такие меры имеют очень важное значение в механизме правового обеспечения ИПБ.

[536] *Смирнов А. А.* О проблемах реализации административной ответственности за использование в информационной продукции скрытых вставок, воздействующих на подсознание людей // Административное право и процесс. 2012. № 11. С. 24–27.

В качестве примера можно привести комплекс правовых санкций в отношении СМИ за нарушение запрета о злоупотреблении свободой массовой информации, предусмотренных Законом о СМИ, а именно: а) отказ в регистрации СМИ (п. 3 ч. 1 ст. 13); б) приостановление и прекращение деятельности СМИ (ч. 3 и 5 ст. 16); в) приостановление, аннулирование или прекращение действия лицензии на телевизионное вещание или радиовещание (ст. 31.7). В качестве меры информационно-правовой ответственности в отношении интернет-ресурсов, допускающих распространение противоправного контента и не реагирующих на уведомления регулятора, можно рассматривать ограничение доступа к ним (ст. 15.1–15.9). Хотя, возможно, такие меры более правильно оценивать как меры пресечения.

Целый комплекс правовых санкций установлен недавно принятым федеральным законом.[537] Они названы в законе «мерами понуждения» и применяются в отношении иностранного лица, осуществляющего деятельность в сети Интернет на территории РФ (далее – иностранный субъект). К ним отнесены: 1) информирование пользователей информационного ресурса иностранного субъекта о нарушении последним законодательства РФ; 2) запрет на распространение рекламы иностранного субъекта и его информационного ресурса; 3) запрет на распространение рекламы на информационном ресурсе иностранного субъекта; 4) ограничение осуществления переводов денежных средств и приема платежей в пользу иностранного субъекта; 5) запрет на поисковую выдачу; 6) запрет на сбор и трансграничную передачу персональных данных; 7) частичное или полное ограничение доступа к информационному ресурсу иностранного субъекта. На наш взгляд, по крайней мере часть из перечисленных здесь «мер понуждения» можно квалифицировать в качестве мер информационно-правовой ответственности.

В заключение параграфа отметим следующее. Анализируя вопрос юридической ответственности в сфере обеспечения ИПБ, мы видим отчетливое проявление межотраслевого характера правового института ее обеспечения. Наиболее показательным в этом плане является одна из самых важных законодательных инициатив последнего времени в рассматриваемой сфере, связанная с противодействием распространению фейковой информации, которая была нормативно определена как «заведомо недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений» (ст. 15.3 Закона об информации). Основные составы правонарушений

[537] Федеральный закон от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети „Интернет" на территории Российской Федерации» // СЗ РФ. 2021. № 27. Ст. 5064.

за распространение фейков были закреплены в ч. 9–11 ст. 13.15 КоАП РФ.[538] Кроме того, УК РФ был дополнен двумя новыми составами: ст. 207.1 «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан» и ст. 207.2 «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия».[539] Все указанные составы различаются прежде всего своими общественно опасными последствиями. Механизм ограничения доступа к информационным ресурсам, содержащим фейковую информацию, закреплен поправками в ст. 15.3 Закона об информации.[540] Еще одним логичным шагом должно было стать дополнение ст. 4 Закона о СМИ запретом распространения фейковой информации как новой формы злоупотребления свободой СМИ. Однако этого сделано не было.

Тем не менее применение такого межотраслевого пакетного принципа регламентации правовых механизмов противодействия угрозам ИПБ нам представляется весьма важным. Особенно значимо изначально продумывать вопрос о правовом способе ограничения доступа к противоправному контенту при его криминализации либо введении административной ответственности.

---

[538] Федеральный закон от 18 марта 2019 г. № 27-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СЗ РФ. 2019. № 12. Ст. 121.

[539] Федеральный закон от 1 апреля 2020 г. № 100-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации» // СЗ РФ. 2020. № 14. Ст. 2030.

[540] Федеральный закон от 18 марта 2019 г. № 31-ФЗ «О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2019. № 12. Ст. 1221.

ГЛАВА IV. ОСОБЕННОСТИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В ОТДЕЛЬНЫХ СФЕРАХ

§ 1. Правовое регулирование обеспечения информационно-психологической безопасности в СМИ

Средства массовой информации приобрели в современном цифровом мире особую и весьма влиятельную роль. Они выступают наиболее мощным каналом психологического воздействия на массовое сознание. А. В. Минбалеев подчеркивает системообразующую роль СМИ в развитии информационного общества.[541]

Закон о СМИ определяет дефиницию понятия «средства массовой информации» через перечисление видов СМИ (печатные и сетевые издания, радио-, теле-, видеопрограмма и др.). Но в нем также выделены и сущностные признаки СМИ: постоянное название и периодичность распространения массовой информации (ст. 2). В России официально зарегистрировано 150 492 СМИ.[542]

В социологической науке средства массовой информации определяются как «социальные институты (пресса, книжные издательства, агентства печати, радио, телевидение и т. д.), обеспечивающие сбор, обработку и распространение информации в массовом масштабе».[543] Известный западный исследователь Д. Маккуэйл определяет СМИ *(mass media)* как виды средств широкомасштабной коммуникации, затрагивающих в определенной степени каждого жителя, относя к ним печатные издания, аудиовизуальные материалы, радио и телевидение.[544]

В научной литературе также встречается термин «средства массовой коммуникации». Дискуссия относительно соотношения двух терминов не утихает до сих пор. Но доминирует точка зрения о том, что средства массовой коммуникации включают не только СМИ, но иные средства

---

[541] *Минбалеев А. В.* Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества: автореф. дис. … д-ра юрид. наук. Челябинск, 2012. С. 8.

[542] Перечень наименований зарегистрированных СМИ (по состоянию на 31.12.2021) // Роскомнадзор. URL: https://rkn.gov.ru/mass-communications/reestr/media/ (дата обращения: 31.12.2021).

[543] Средства массовой информации // Энциклопедический социологический словарь / Под общ. ред. академика РАН Г. В. Осипова. М.: ИСПИ РАН, 1995. С. 763.

[544] *McQuail D.* McQuail's Mass Communication Theory. 4th edition. London: Sage Publication, 2000. P. 4.

межличностного или группового общения, включая телефоны, компьютеры, телеграф и др.[545] Но Д. МакКуэйл отмечал происходящее стирание границ между публичной и частной коммуникацией в силу действия фактора цифровой конвергенции,[546] который значительно усилился за последние десятилетия.

СМИ как субъекты массовой коммуникации являются наиболее влиятельными источниками ИПВ на общество в силу массовости, повсеместной доступности и психологической убедительности. Многолетние социологические исследования, проводимые в России ВЦИОМ, Левада-Центром и другими институтами, показывают уверенное доминирование СМИ в качестве источников получения новостей о стране и мире. При этом, несмотря на определенные проблемы доверия людей к СМИ в плане таких новостей, они остаются абсолютными лидерами и значительно опережают по этому показателю «личностные» каналы коммуникации (друзей, родных, соседей).[547] Наряду с этим традиционным СМИ все большую конкуренцию составляют «новые медиа», прежде всего интернет-сайты и социальные медиа.

Для разработки методологических аспектов правового регулирования обеспечения ИПБ в СМИ необходимо правильное понимание особенностей механизма психологического воздействия СМИ на аудиторию. Ему посвящен раздел теории массовых коммуникаций, обозначаемый в российской и западной литературе как «эффекты воздействия СМИ» (*англ.* mass media effects). В рамках него изучаются вызываемые влиянием массовой коммуникации изменения в сознании и поведении граждан.[548]

Проведенный нами анализ тематической литературы[549] позволил выделить следующие *основные характеристики механизма психологического влияния массмедиа на личность и социальные группы*:

1. Влияние СМИ зависит от комплекса факторов: вида СМИ, содержания материала, характера аудитории, условий восприятия информации, социальной среды, содержания контента.

---

[545] *Черных А. И.* Социология массовой коммуникации: учеб. пособие; Гос. ун-т – Высшая школа экономики. М.: Изд. дом ГУ ВШЭ, 2008. С. 49.

[546] *McQuail D.* McQuail's Mass Communication Theory. 4th edition. London: Sage Publication, 2000. P. 4.

[547] Источники новостей и доверие СМИ. Пресс-выпуск от 27.02.2020 // Левада-Центр. URL: https://www.levada.ru/2020/02/27/istochniki-novostej-i-doverie-smi/ (дата обращения: 12.09.2020).

[548] *Назаров М. М.* Массовая коммуникация и общество: введение в теорию и исследования. 4-е изд., перераб. и доп. М.: Книжный дом «ЛИБРОКОМ», 2010. С. 300.

[549] *Назаров М. М.* Массовая коммуникация и общество… С. 301–306; *Черных А. И.* Социология массовой коммуникации. С. 303–384; *Богомолова Н. Н.* Социальная психология массовой коммуникации: учебное пособие для студентов вузов. М.: Аспект Пресс, 2008. С. 152–157; *Землянова Л. М.* Коммуникативистика и средства информации: англо-русский толковый словарь концепций и терминов. М.: Издательство Моск. ун-та, 2004. С. 27–28, 307; *Бакулев Г. П.* Массовая коммуникация: Западные теории и концепции. 2-е изд., перераб. и доп. М.: Аспект-Пресс, 2010. С. 33–143.

2. Аудитория СМИ является активной при выборе и потреблении транслируемой информации и может оказывать сопротивление навязываемым мнениям и оценкам.

3. Аудитория СМИ весьма неоднородна и сегментирована на определенные группы с различающимися ориентациями на определенный вид СМИ и медиаконтента и способностями к усвоению информации.

4. Социальное влияние СМИ включает три основные группы эффектов: когнитивные (влияние на взгляды, мнения, решения, установки, ценностные ориентации, социальные представления и т. д.), аффективные (влияние на индивидуальные и групповые эмоции, чувства, настроения и т. д.) и поведенческие (влияние на индивидуальное и коллективное поведение).

5. Воздействие СМИ может проявляться как в определении предмета общественного внимания («повестки дня»), так и в содержании и характере общественных взглядов и оценок. При этом массмедиа способны успешно продвигать определенную точку зрения и блокировать альтернативные, способствуя раскрутке «спирали умолчания» в обществе.

6. Одним из распространенных эффектов СМИ является социальное научение моделям поведения, транслируемым в массмедиа, которые в последующем могут воспроизводиться в реальной жизни.

7. В более общем плане СМИ формируют особое символическое представление о реальности с присущим ему набором образов, моделей восприятия, ценностных ориентаций, норм поведения и т. п., которое обуславливает образ мышления, чувств и поведения масс людей.

Столь подробное освещение нами базовых теорий эффектов массовой коммуникации не случайно. Оно обусловлено необходимостью показать многообразие подходов к описанию механизма влияния СМИ на личность и социальные группы и, главное, очертить контуры его реального содержания. Авторский опыт изучения юридической литературы, участия в научно-практических конференциях и семинарах, а также общественных комиссиях при органах государственной власти показал, что такое четкое представление, за рамками узкой прослойки профильных специалистов, отсутствует. Как правило, наблюдаются крайние, полярные точки зрения, «рисующие» устрашающие картины тотального влияния СМИ на беспомощную аудиторию либо, напротив, максимально нивелирующие воздействие СМИ. Такая полярность во взглядах проецируется и на сферу законотворчества, когда законодатели либо вообще отказываются принимать меры по защите общества от деструктивного влияния СМИ, ссылаясь на недоказанность однозначного негативного характера такого влияния, либо, наоборот, предлагают «драконовские» законодательные инициативы в рассматриваемой сфере, не соответствующие реальной общественной опасности конкретной угрозы ИПБ.

Основной вывод, который нам хотелось обосновать исходя из вышеизложенного, состоит в следующем: механизм информационно-психологического влияния СМИ на личность, социальные группы и общество в целом носит чрезвычайно сложный, многоаспектный характер.[550] Сила, территориальный масштаб и количественный охват воздействия СМИ обусловлены комплексом факторов, включая вид СМИ, характер контента, особенности целевой группы аудитории, факторы внешней микро- и макросоциальной среды. *Следствием этого для нормотворческой деятельности выступает требование максимальной гибкости правового регулирования с обязательным учетом конкретной специфики регламентируемого аспекта обеспечения ИПБ в СМИ.*

Далее проанализируем нормы действующего российского законодательства в области СМИ, регулирующие вопросы обеспечения ИПБ. Базовым источником в рассматриваемой сфере выступает Закон о СМИ, который декларирует базовый конституционный принцип свободы массовой информации и раскрывает его нормативное содержание. Согласно ст. 1 данного закона в России оборот массовой информации, учреждение и право собственности на СМИ не подвергаются ограничениям. При этом рассматриваемая норма содержит оговорку относительно исключений из этого правила со ссылкой на нормы законодательства о СМИ. Дополним, что ограничения свободы массовой информации устанавливаются не только Законом о СМИ, но и другим российским законодательством.

В качестве важнейшей юридической гарантии свободы массовой Законом о СМИ закреплена недопустимость цензуры (ст. 3). При этом под цензурой массовой информации понимается требование предварительного согласования материалов СМИ со стороны государственных органов и иных организаций и последующее наложение запрета на распространение таких материалов. В России запрещено создание специальных цензурных органов в отношении СМИ. Однако запрет цензуры вовсе не означает недопустимость любого ограничения свободы массовой информации. На нее вполне распространяются общие правила допустимости ограничения основных прав, установленные ч. 3 ст. 55 Конституции РФ.

Важнейшее значение для обеспечения ИПБ в деятельности СМИ имеет ст. 4 Закона о СМИ, в которой закреплена недопустимость злоупотребления свободой массовой информации. В ней нормативно определены возможные формы такого злоупотребления, включая: а) использование СМИ для совершения преступлений, пропаганды (оправдания) терроризма, экстремизма, порнографии, жесткости и насилия; б) применение специальных методов деструктивного воздействия на подсознание человека;

[550] Данную характеристику влияния массмедиа блестяще выразил Б. Берельсон в широко цитируемом выражении: «Некоторого рода сообщения по некоторого рода вопросам, доведенные до сведения некоторого рода людей, при некоторого рода условиях имеют некоторого рода воздействие». См.: *Berelson B.* Communication and Public Opinion. Urbana, 1948. P. 500.

в) распространение сведений о способах изготовления наркотиков, взрывчатых веществ и взрывных устройств; д) распространение персональных данных несовершеннолетних потерпевших; е) распространение иной противоправной информации. Кроме того, к формам злоупотребления свободой массовой информации отнесены невыполнение правил указания запрещенного характера деятельности террористических или экстремистских организаций, выполнения организацией или лицом функций иностранного агента в информационных материалах СМИ.

Также в данной статье отдельно закрепляются особенности освещения в СМИ контртеррористических операций. Следует отметить, что указанные в ст. 4 Закона о СМИ виды информации, распространение которых квалифицируется как злоупотребление свободой массовой информации, регулируются отдельными законодательными актами.

Отдельная статья посвящена такой форме контента, как эротические издания, отличительным признаком которых является стимулирование и использование интереса к сексу (ст. 37). Такие издания не отнесены к противоправным, но для них установлены некоторые ограничения, связанные с запретом радио- и телетрансляции в дневное время (с 5 до 23 часов) и специальными требованиями по распространению в розничной продаже (запечатанная упаковка, специально отведенные помещения для торговых точек).

Отметим еще один значимый момент. В интересах безопасности государства Федеральным законом от 25 ноября 2017 г. № 327-ФЗ[551] Закон о СМИ дополнен нормами, учреждающими правовой статус «иностранных СМИ, выполняющих функции иностранных агентов». Он стал зеркальным ответом на действия Минюста США, потребовавшего от RT America – филиала российской телекомпании – зарегистрироваться в качестве иностранного агента на территории Соединенных Штатов.[552] Согласно внесенным изменениям в ст. 6 Закона о СМИ в качестве иностранных СМИ, выполняющих функции иностранных агентов (далее – СМИ-иноагенты), могут быть признаны иностранные юридические лица либо иные структуры, осуществляющие публичное распространение материалов и сообщений, и получающие финансирование из-за рубежа.

Позже Федеральным законом от 2 декабря 2019 г. № 426-ФЗ[553] были внесены дополнения, которые установили возможность присвоения данного правового статуса физическим лицам. Базовый критерий тот же – иностранное финансирование. Кроме того, согласно принятым поправкам статус СМИ-иноагента также могут получить физические лица или российские юридические лица при условии распространения

[551] СЗ РФ. 2017. № 48. Ст. 7051.

[552] Каков порядок признания СМИ иноагентом и какие издания попали в список // ТАСС. 3 декабря 2019 г. URL: https://tass.ru/info/7117481 (дата обращения: 22.12.2020).

[553] СЗ РФ. 2019. № 49. Ст. 6985.

ими сообщений и материалов, которые созданы и (или) распространены иностранными СМИ-иноагентами и (или) российским юридическим лицом, учрежденным иностранным СМИ-иноагентом, и (или) участия в создании указанных сообщений и материалов (ч. 7 ст. 6 Закона о СМИ).

На СМИ-иноагенты распространили правовой режим, установленный законодательством для некоммерческих организаций-иноагентов (за некоторыми изъятиями). Прежде всего это выражается во включении соответствующих лиц и структур в специальный реестр, а также в усиленном государственном контроле за их деятельностью. Помимо регистрации юридического лица иностранные агенты должны ставить пометку о своем статусе на каждом сообщении и материале не только на сайтах СМИ, но и в соцсетях.[554] За нарушение порядка деятельности СМИ-иноагентов в ст. 19.34.1 КоАП РФ была установлен административный штраф. Помимо прямых юридических аспектов, у правового статуса СМИ-иноагента есть косвенное экономическое следствие – наличие такового сразу снижает привлекательность соответствующего СМИ как рекламодателя.

По состоянию на 30 декабря 2021 г. Реестр СМИ-иноагентов включает 111 позиций.[555] Из них 36 являются организациями, остальные – физическими лицами. Среди организаций – иностранных СМИ в Реестре присутствуют известные со времен «холодной войны» западные пропагандистские ресурсы «Голос Америки» и «Радио Свободная Европа/Радио Свобода» со своими региональными подразделениями, российский «Телеканал Дождь», сетевые издания «Медуза», «Росбалт», Republic, «ОВД инфо», «Медиазона» и др. Также в Реестр включены многие известные проекты так называемой «расследовательской журналистики», которые часто выступали источниками распространения фейков и компрометирующей информации в отношении политического руководства страны: Bellingcat, The Insider, «Важные истории», «Первое антикоррупционное СМИ» (ПАСМИ) и др., а также журналисты-расследователи: Р. А. Анин, Р. С. Баданин, О. В. Шмагун и др.

С точки зрения интересов национальной безопасности учреждение правового механизма признания СМИ-иноагентами организаций и физических лиц, получающих иностранное финансирование и распространяющих массовую информацию, является мощным инструментом снижения деструктивного информационного влияния из-за рубежа. Российские власти неоднократно подчеркивали, что принятие соответствующих поправок в законодательство стало вынужденной ответной мерой на притеснения

[554] Все о статусе иноагента: правовые рекомендации // Центр защиты прав СМИ. 16 февраля 2021 г. URL: https://mmdc.ru/services/common/vse-o-statuse-inoagenta-pravovye-rekomendaczii/ (дата обращения: 12.12.2021).

[555] Реестр иностранных средств массовой информации, выполняющих функции иностранного агента // Министерство юстиции Российской Федерации. URL: https://minjust.gov.ru/ru/documents/7755/. 30 декабря 2021 г. (дата обращения: 31.12.2021).

российских СМИ за рубежом. Кроме того, отмечалось, что попадание в Реестр вовсе не означает запрета деятельности.[556]

Вместе с тем учрежденный правовой механизм небезупречен с точки зрения защиты интересов самих СМИ и журналистов. В этой связи президент России В. В. Путин в декабре 2021 г. поддержал идею журналистского сообщества о дополнительном обсуждении закона о СМИ-иноагентах с профессиональным сообществом. В ходе предшествующего обсуждения на заседании Совета по правам человека звучали предложения о необходимости вынесения предварительного предупреждения о возможности включения в соответствующий реестр, а также снятия такого статуса с организаций и физических лиц.[557]

§ 2. Правовое регулирование обеспечения информационно-психологической безопасности в сети Интернет

С развитием компьютерных технологий и информационно-телекоммуникационной сети Интернет возникает новое поколение массмедиа, обобщенно именуемых *«новыми медиа» (new media).*[558] К ним относят интернет-ресурсы, мультимедийные материалы, компьютерные игры, цифровые аудиовизуальные материалы, виртуальную реальность, цифровые интерфейсы «человек – компьютер.[559] В известной работе Л. Мановича автором выделены основные принципы новых медиа: а) цифровая репрезентация; б) модульность; в) автоматизация; г) вариативность; д) транскодинг.[560]

Ключевую роль среди новых медиа играют многочисленные интернет-ресурсы. В юридическом плане сеть Интернет является каналом распространения массовой информации, но СМИ не является.[561] Под последнюю категорию подпадают только сетевые издания.

В эволюции интернет-технологий массовой коммуникации принято выделять два основных поколения. Первое поколение веб-технологий

---

[556] Песков: статус СМИ-иноагента не запрещает журналистам работать в России // Коммерсант. 16 июля 2021 г. URL: https://www.kommersant.ru/doc/4907460?tg (дата обращения: 12.12.2021).

[557] *Дульнева М.* Путин поддержал идею обсудить закон об иноагентах с журналистами // Forbes. 9 декабря 2021 г. URL: https://www.forbes.ru/society/449161-putin-podderzal-ideu-obsudit-zakon-ob-inoagentah-s-zurnalistami) (дата обращения: 21.12.2021).

[558] Некоторые исследователи отмечают неопределенность и размытость понятия «новые медиа», название которых сформулировано через противопоставление «старым», традиционным медиа. В. В. Савчук наиболее уязвимым называет слово «новое», которое, по его мнению, является «скоропортящимся продуктом», особенно в условиях динамичной социальной реальности. См.: *Савчук В. В.* Медиафилософия. Приступ реальности. СПб.: Издательство РГХА, 2013. С. 104–107.

[559] Новые медиа // Социология: Энциклопедия / Сост.: А. А. Грицанов, В. Л. Абушенко, Г. М. Евелькин и др. Минск: Книжный Дом, 2003. С. 457.

[560] *Манович Л.* Язык новых медиа. М.: Ад Маргинем пресс, 2018. С. 60–84.

[561] *Рихтер А. Г.* Правовые основы интернет-журналистики: учебник. М.: Издательство ИКАР, 2014. С. 52.

(Web 1.0) было ориентировано на передачу и распространение информации. Основным типом интернет-ресурсов выступали интернет-сайты.[562] В 2021 г. в мире насчитывалось свыше 127 млн веб-сайтов.[563]

Второе поколение веб-технологий (Web 2.0) нацелено на обеспечение интерактивной коммуникации интернет-пользователей с помощью социальных сетевых ресурсов. Благодаря им резко выросла интенсивность общения и взаимодействия людей.[564] Именно технологии Web 2.0 способствовали взрывному росту популярности Интернета, который продолжается до настоящего времени. По данным BroadbandSearch, в 2021 г. численность интернет-пользователей в мире достигла значения 4,93 млрд человек, что составляет 63,2% мирового населения.[565] По данным Mediascope, в России количество активных месячных пользователей Интернета в июле – сентябре 2021 г. составляло 100 226,7 тыс. человек.[566] Уже по итогам 2020 г. фиксировалось, что проникновение Интернета в России среди населения в возрасте до 44 лет превысило 90%, а среди самых молодых россиян (12–24 лет) приблизилось к 100%. При этом мобильные устройства являются главным средством для выхода в Интернет среди россиян всех возрастов.[567]

Исследователи все чаще говорят о гиперподключенности, которая соответствует высокому уровню пользовательской активности и максимальным показателям «экранного времени» – времени, проведенного перед экранами смартфона, компьютера или планшета. По данным российских исследователей, показатель гиперподключенности в 2019 г. у российских подростков и взрослых достигал 8–10 часов в сутки, что соответствует половине времени бодрствования человека, причем тенденция роста данного показателя отчетливо прослеживалась с 2009 г.[568]

Ключевую роль в развитии Web 2.0 сыграли *социальные сети (social networks services*) – интерактивные веб-платформы, предназначенные для общения пользователей и размещения контента. В 2021 г. в мире

[562] Закон об информации определяет сайт в сети Интернет как «совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети Интернет» (п. 13 ст. 2).

[563] Key Internet Statistics to Know in 2022 (Including Mobile) // BroadbandSearch. URL: https://www.broadbandsearch.net/blog/internet-statistics (дата обращения: 10.01.2022).

[564] *Лебедев П. А., Петухова С. И.* Социальные медиа: показатель развития информационного общества? // Мониторинг общественного мнения. 2010. № 5. С. 18–19.

[565] Key Internet Statistics to Know in 2022 (Including Mobile).

[566] Количество интернет-пользователей (июль 2021 – сентябрь 2021) // Mediascope. URL: https://webindex.mediascope.net/general-audience (дата обращения: 10.01.2022).

[567] Аудитория Интернета в России в 2020 году // Mediascope. 12.01.2021 URL: https://mediascope.net/news/1250827/ (дата обращения: 22.02.2021).

[568] *Солдатова Г. У., Войскунский А. Е.* Социально-когнитивная концепция цифровой социализации: новая экосистема и социальная эволюция психики // Психология. Журнал Высшей школы экономики. 2021. Т. 18. № 3. С. 438.

насчитывалось 3,96 млрд пользователей социальных сетей.[569] Наиболее популярной социальной сетью в мире является Facebook[570] (2,7 млрд пользователей), второе место занимает YouTube (2 млрд пользователей).[571] В России тройку лидеров среди социальных сетей составляют YouTube, сеть «ВКонтакте» и Instagram.[572]

Помимо социальных сетей как основного канала интернет-коммуникации во втором десятилетии XXI столетия широкое развитие получили интернет-мессенджеры (Instant messaging) – приложения для мгновенного обмена сообщениями через Интернет. Самым популярным среди них в России является WhatsApp, также активно используются Telegram, Viber и другие мессенджеры.[573] Они стали весьма значимым каналом распространения контента и коммуникации, в том числе деструктивных типов.

Следствием развития технологий Web 2.0 применительно к теме нашего исследования является то, что *интернет-ресурсы, в отличие от традиционных СМИ, выступают источником не только контентных, но и коммуникационных угроз ИПБ*. Другими словами, опасность для интернет-пользователей составляет не только распространяемая в сети информация, но и деструктивная коммуникация между ними. В. Б. Наумов подчеркивает, что при всех многочисленных достоинствах Интернета и предоставляемых им уникальных возможностях сеть несет и серьезные опасности, связанные с деструктивной коммуникацией между людьми.[574] В качестве примеров губительного воздействия сетевых ресурсов на сознание и поведение граждан А. Н. Савенков называет сайты о детских клубах самоубийц, каналы вербовщиков запрещенной в России ИГИЛ, форумы «колумбайнеров».[575]

Социологические исследования показывают, что новые медиа в лице интернет-сайтов, социальных сетей, мессенджеров и веб-приложений уже вовсю теснят традиционные СМИ как в плане времени потребления,

---

[569] Key Internet Statistics to Know in 2022 (Including Mobile). Следует отметить, что согласно докладу «DIGITAL 2021: The latest insights into the 'State of Digital'» данный показатель в 2020 г. уже превышал 4 млрд. См.: *Kemp S.* DIGITAL 2021: The latest insights into the 'State of Digital' // We Are Social Inc. 27 January 2021. URL: https://wearesocial.com/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital (дата обращения: 21.02.2021).

[570] Владелец соцсетей Facebook и Instagram компания Meta Platforms признана в России экстремистской организацией.

[571] Key Internet Statistics to Know in 2022 (Including Mobile).

[572] Топ-10 ресурсов. Desktop&Mobile, Monthly Reach. Сентябрь 2021 // Mediascope. URL: https://webindex.mediascope.net/top-resources (дата обращения: 22.12.2021).

[573] Там же.

[574] *Наумов В. Б.* Институт идентификации в информационном праве: дис. …д-ра юрид. наук. М., 2020. С. 296.

[575] *Савенков А. Н.* Философия права, правовое мышление и глобальные проблемы современной цивилизации // Трансформация парадигмы права в цивилизационном развитии человечества: доклады членов РАН / Под общ. ред. чл.-корр. РАН А. Н. Савенкова. М.: ИГП РАН, 2019. С. 81–82.

так и по силе влияния.[576] Данная тенденция, несомненно, продолжится, а потому *именно новые медиа становятся основными источниками ИПВ на общество, а следовательно, и основными источниками угроз ИПБ*. Этому также способствуют некоторые отличительные признаки новых медиа.

На основе анализа научной литературы и собственных исследований нами выделены ключевые характеристики интернет-ресурсов, имеющие большое значение в контексте правового регулирования обеспечения ИПБ:

1. *Трансграничность и глобальный характер.* Интернет является глобальной информационно-телекоммуникационной сетью, обеспечивающей трансграничный мгновенный доступ к информации, хранящейся в любой точке земного шара.[577] Это вызывает огромные сложности в плане национального правового регулирования и осуществления государственного управления в сфере интернет-отношений. В контексте темы ИПБ данный признак расширяет географию источников информационных угроз до глобальных масштабов и существенно затрудняет возможности их нейтрализации.

2. *Фактор относительной анонимности виртуального общения.* Регистрация граждан в социальных сетях и иных интерактивных ресурсах преимущественно осуществляется ими самостоятельно при весьма ограниченной верификации указанных персональных данных. Это создает возможность использования фейковых учетных записей. В реальности у технологических компаний и спецслужб в арсенале имеется широкий инструментарий, позволяющий во многих случаях установить личность владельца/пользователя интернет-ресурса. Для большинства пользователей специальные средства сокрытия подлинной личности недоступны по причине своей сложности. Вне зависимости от объективного наличия анонимности ее субъективное восприятие пользователем во многих случаях способствует «растормаживанию» его сетевой активности и проявлению деструктивных ее форм.

3. *Предоставление возможности размещения пользовательского контента.* Это означает наличие у пользователей социальных сетей и иных интернет-ресурсов возможности самостоятельного распространения контента на массовую аудиторию.[578] В этом состоит главное отличие новых

---

[576] *Kemp S.* DIGITAL 2021: The latest insights into the 'State of Digital'; Источники новостей и доверие СМИ. Пресс-выпуск от 27 февраля 2020 г. (Левада-Центр).

[577] А. Г. Лисицын-Светланов подчеркивал, что киберпространство изначально лишено территориального начала. См.: *Лисицын-Светланов А. Г.* Философия права: классические идеи и вызовы современности // Трансформация парадигмы права в цивилизационном развитии человечества: доклады членов РАН / Под общ. ред. чл.-корр. РАН А. Н. Савенкова. М.: ИГП РАН, 2019. С. 164.

[578] Предоставление Интернетом возможности «размещения информации для неограниченного круга лиц» зафиксировано в качестве сущностного признака в правовой дефиниции Интернета в Модельном законе «Об основах регулирования Интернета», принятом постановлением МПА СНГ от 25 ноября 2016 г. № 45–12.

медиа от традиционных СМИ, и значение данного фактора поистине революционно. Традиционная схема однонаправленной трансляции сведений от СМИ к аудитории трансформируется в новую модель «транзактной медийной коммуникации»,[579] в которой каждый человек становится потенциальным источником массовой информации. Генерируемый пользователями контент уже сейчас составляет основную часть информации в глобальной сети[580], и этот тренд с каждым годом усиливается. В контексте темы обеспечения ИПБ рассматриваемый фактор означает прежде всего мультипликативный рост числа источников информационных угроз и их «дисперсное распыление». В плане правового регулирования его следствием выступает сложность осуществления контроля за размещаемым контентом из-за большого количества его авторов.

4. *Предоставление информации по запросу пользователя.* В противоположность прежним аудиовизуальным СМИ, предполагающим централизованную модель вещания, когда пределы усмотрения аудитории ограничиваются рамками единого «информационного меню», Интернет дает своим пользователям полную свободу выбора информации, причем в глобальном масштабе. Вместе с трансфертом селекции от редакции СМИ к самому пользователю частично происходит и перенос ответственности за ее результаты. Впрочем, в последнее время в социальных сетях ключевую роль в выстраивании информационной ленты для пользователя играют рекомендательные алгоритмы, работающие по непрозрачной схеме.[581]

5. *Важная роль поисковых систем.*[582] Данные системы обеспечивают отыскание нужной пользователю информации среди гигантского массива данных Всемирной паутины. Наиболее известными являются Google, Bing, Yahoo, Baidu, «Яндекс». Изменяя порядок отображения информации в результатах поисковой выдачи (который формируется по определенным алгоритмам), можно влиять на просмотр контента. Данный фактор учитывается при обеспечении ИПБ (например, крупные поисковые системы

[579] *Брайант Дж., Томпсон С.* Основы воздействия СМИ. Пер. с англ. М.: Издательский дом Вильямс, 2004. С. 396.

[580] Так, по данным доклада Brand Analytics, в месяц в России публикуется 1,2 млрд постов в совокупности в семи наиболее популярных социальных сетях. См.: Социальные сети в России. Осень 2020 // Brand Analytics. URL: https://drive.google.com/file/d/1L51qJJYysVOHig2WaUtKC61ZvxXPA0ts/view (дата обращения: 12.01.2021).

[581] *Harris T.* How Technology is Hijacking Your Mind – from a Magician and Google Design Ethicist // Medium. May 18, 2016. URL: https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3 (дата обращения: 14.01.2021); *Горелкин А.* Куда ведут алгоритмы социальных сетей // Газета.ру. 16 марта 2021 г. URL: https://www.gazeta.ru/comments/2021/03/16_a_13513226.shtml (дата обращения: 17.05.2021).

[582] Поисковая система – информационная система, осуществляющая по запросу пользователя поиск в сети Интернет информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети Интернет для доступа к запрашиваемой информации, расположенной на сайтах в сети Интернет, принадлежащих иным лицам (п. 20 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации»).

не отображают в итогах поисковой выдачи сайты с детской порнографией). Однако роль поисковых систем снижается вследствие повышения роли социальных сетей и роста количества мобильных приложений.

Описанные выше механизмы ИПВ массовой коммуникации вполне применимы и к новым медиа. Вместе с тем их существенные отличительные черты потребовали изучения изменившихся механизмов их социально-психологического влияния. Данные вопросы находятся в фокусе новейших исследований в области психологии, социологии и коммуникативистики.[583]

Общественные отношения, связанные с использованием сети Интернет, выступают предметом правового регулирования различных отраслей российского права. Информационному праву среди них отводится ключевая роль. Один из ведущих исследователей правового регулирования Интернета в России И. М. Рассолов определял интернет-право как комплексный межотраслевой институт, включающий «совокупность взаимосвязанных правовых норм, объединенных общностью регулирования отношений в виртуальном пространстве Интернета».[584] В. В. Архипов отмечает, что попытки некоторых авторов определить интернет-право как самостоятельную отрасль права не имеют под собой достаточных оснований прежде всего из-за отсутствия самостоятельного метода правового регулирования.[585]

Учитывая отсутствие отдельного закона об Интернете, регулирующие его правовые нормы прежде всего находят отражение в Законе об информации и Законе о связи. При этом следует учитывать распространение действия общих принципов права и норм других правовых актов, не посвященных специально Интернету, но применимых к интернет-отношениям с учетом их специфики.[586]

Как справедливо отмечено в диссертации А. В. Минбалеева, проблемы распространения «вредной» информации в сети Интернет и защиты нравственности были одним из драйверов расширения сферы

---

[583] *Войскунский А. Е.* Психология и Интернет. М.: Акрополь, 2010; *Кузнецова Ю. М., Чудова Н. В.* Психология жителей Интернета. 3-е изд. М.: URSS, 2015; *Белинская Е. П.* Психология интернет-коммуникации: учеб. пособие. М.: МПСУ; Воронеж: МОДЭК, 2013; *Колозариди П. В.* Интернет-исследования как направление социальных наук: теоретико-методологический анализ: дис. … канд. социолог. наук. М., 2017; *Прокопенко Т. В.* Роль социальных сетей в российской системе политической коммуникации: дис. … канд. полит. наук. М., 2020; An Introduction to Cyberpsychology. Edited By Irene Connolly, Marion Palmer, Hannah Barton, Gráinne Kirwan. London, Routledge, 2016; Cyberpsychology and Society Current Perspectives. Edited By Andrew Dr Power London, Routledge, 2018.

[584] *Рассолов И. М.* Право и Интернет. Теоретические проблемы. 2-е изд., доп. М.: Норма, 2009. СПС «КонсультантПлюс».

[585] *Архипов В. В.* Интернет-право: учебник и практикум для вузов. М.: Юрайт, 2021. С. 31.

[586] *Михайленко Е. В.* Проблемы информационно-правового регулирования отношений в глобальной компьютерной сети Интернет: автореф. дис. … канд. юрид. наук. М., 2004. С. 17.

правового регулирования интернет-отношений.[587] В практическом плане это выразилось в первую очередь в закреплении в Законе об информации организационно-правовых механизмов ограничения доступа к противоправному контенту.

Первый такой механизм был введен Федеральным законом от 28 июля 2012 г. № 139-ФЗ[588] (получившим известность как «Закон о черных списках сайтов»). Им был учрежден Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в РФ запрещено (далее – Реестр). Введение в действие Реестра (1 ноября 2012 г.) стало важнейшим шагом на пути совершенствования механизма противодействия распространению негативной информации в сети Интернет в нашей стране.

В дальнейшем законодатель начал вводить все новые механизмы ограничения доступа к противоправному контенту. В основном речь шла о контенте, оказывающем негативное ИПВ, хотя встречались и примеры противоправной информации другого рода (например, ст. 15.2 Закона об информации касается ограничения доступа к пиратскому контенту). Представим в табличном виде обобщенные сведения об интересующих нас видах вредной информации, доступ к которой ограничивается по состоянию на 31 декабря 2021 г. (табл. 4).

Таблица 4

Виды негативной информации, к которой ограничивается доступ согласно Закону об информации

№ п/п	Вид негативного контента	Орган, принимающий решение
1.	Материалы с порнографическими изображениями несовершеннолетних и (или) объявления о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера (ст. 15.1)	Роскомнадзор
2.	Информация о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений (ст. 15.1)	МВД России/Роскомнадзор*
3.	Информация о способах совершения самоубийства, а также призывы к совершению самоубийства (ст. 15.1)	Роспотребнадзор/ Роскомнадзор*
4.	Информация о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами (ст. 15.1)	Росмолодежь/ Роскомнадзор*
	* *В случае размещения информации в продукции СМИ, распространяемой посредством сети Интернет*	

[587] *Минбалеев А. В.* Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества: автореф. дис. … д-ра юрид. наук. Челябинск, 2012. С. 10.

[588] СЗ РФ. 2012. № 31. Ст. 4328.

№ п/п	Вид негативного контента	Орган, принимающий решение
5.	Информация, нарушающая требования законодательства о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи, а также информация, обеспечивающая возможность совершения действий по переводу денежных средств через иностранных поставщиков платежных услуг, включенных в установленные законодательством перечни (ст. 15.1)	ФНС России
6.	Информация, содержащая предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством (ст. 15.1)	Росалкогольрегулирование
7.	Информация, направленная на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц (ст. 15.1)	Росмолодежь
8.	Информация, содержащая предложение о розничной торговле лекарственными препаратами, в том числе дистанционным способом, розничная торговля которыми ограничена или запрещена в соответствии с законодательством, и (или) информация, содержащая предложение о розничной торговле лекарственными препаратами, в том числе дистанционным способом, лицами, не имеющими лицензии и разрешения на осуществление такой деятельности, если получение лицензии и разрешения предусмотрено законодательством об обращении лекарственных средств (ст. 15.1)	Росздравнадзор
9.	Информация, распространение которой в РФ запрещено (ст. 15.1)	Суд
10.	Информация, порочащая честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица (ст. 15.1)	Судебный пристав-исполнитель
11.	Информация, выражающая в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам РФ, Конституции РФ или органам, осуществляющим государственную власть в РФ (ст. 15.1–1)	Генеральная прокуратура РФ
12.	Информация, распространяемая в сети Интернет, порочащая честь, достоинство или деловую репутацию гражданина (физического лица) или подрывающая его репутацию и связанная с обвинением гражданина (физического лица) в совершении преступления (ст. 15.1–2)	Генеральная прокуратура РФ
13.	Информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка (ст. 15.3)	Генеральная прокуратура РФ
14.	Недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи (ст. 15.3)	Генеральная прокуратура РФ
15.	Информационные материалы иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории РФ в соответствии с законодательством, а также сведения, позволяющие получить доступ к указанным информации или материалам (ст. 15.3)	Генеральная прокуратура РФ

№ п/п	Вид негативного контента	Орган, принимающий решение
16.	Информация о возможности получения банковских услуг, страховых услуг, услуг на рынке ценных бумаг, а также услуг, связанных с привлечением и (или) размещением денежных средств юридических и физических лиц, распространяемая с нарушением законодательства РФ, регулирующего отношения на финансовом рынке, и содержащая сведения о получении указанных услуг со стороны лиц, не имеющих права на их оказание в соответствии с законодательством РФ (ст. 15.3)	Генеральная прокуратура РФ
17.	Информация, побуждающая к участию в деятельности по привлечению денежных средств и (или) иного имущества физических лиц и (или) юридических лиц, при которой выплата дохода и (или) предоставление иной выгоды … осуществляются за счет привлеченных денежных средств и (или) иного имущества иных физических лиц и (или) юридических лиц при отсутствии инвестиционной и (или) иной законной предпринимательской или иной деятельности, которая связана с использованием привлеченных денежных средств и (или) иного имущества и за которую предусмотрена уголовная или административная ответственность (ст. 15.3)	Генеральная прокуратура РФ
18.	Информация, распространяемая с нарушением требований законодательства РФ о выборах и референдумах, и (или) агитационные материалы, изготовленные и (или) распространяемые с нарушением требований законодательства РФ о выборах и референдумах (ст. 15.3–1)	ЦИК России или иная избирательная комиссия

Закон об информации также предусматривает возможность ограничения доступа к интернет-ресурсам, которые облегчают получение противоправного контента или иным образом способствуют его обороту и потреблению, либо не выполняют требования законодательства РФ. В частности, это относится к ограничению доступа к аудиовизуальному сервису (ст. 10.5), ресурсу ОРИ (ст. 15.4), программно-аппаратным средствам обхода блокировок (ст. 15.8), информационному ресурсу СМИ-иноагента (ст. 15.9).

Оператором всех предусмотренных Законом об информации реестров доступа к информации выступает Роскомнадзор. В большинстве случаев процедура ограничения доступа к информации предполагает инициативное реагирование на обнаруженный противоправный контент со стороны государственных органов и направление информации в соответствующие структуры. Так, в рамках исполнения ст. 15.1 Закона об информации решения о включения доменных имен и (или) указателей страниц сайтов в сети Интернет, а также сетевых адресов в Реестр, принимают следующие государственные органы: МВД России, Роспотребнадзор, ФНС России, Росалкогольрегулирование, Росмолодежь, Роскомнадзор, Росздравнадзор.[589] Более детально информация изложена в таблице,

[589] Постановление Правительства Российской Федерации от 26 октября 2021 г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-

представленной выше. Из ее анализа видно, что законодательством РФ предусмотрен преимущественно внесудебный порядок ограничения доступа к вредной информации, когда решение о блокировке выносится органами исполнительной власти или прокуратуры.

Вместе с тем необходимо понимать, что норма п. 2 ч. 15 Закона об информации, закрепляющая в качестве основания для включения в Реестр «решение суда о признании информации, распространяемой посредством сети Интернет, информацией, распространение которой в Российской Федерации запрещено», на самом деле покрывает гораздо большее количество видов негативного контента, чем установлено для внесудебного порядка. По сути, в судебном порядке принимается решение о признании запрещенной к распространению любой иной информации, предусмотренной нормами УК РФ и КоАП РФ. Выше нами было показано, насколько объемный перечень противоправного контента они содержат, причем он постоянно дополняется.

Кратко остановимся на анализе процессуальных аспектов механизмов ограничения доступа к информации. Особенностью функционирования данных механизмов является то, что при высокой схожести их работы законодателем установлены разные процедуры (алгоритмы) блокировки для каждого из них. Детально рассматривать каждый такой алгоритм мы не будем, выделим лишь их общие черты и обозначим ключевые различия.

Общим для всех механизмов выступает организация взаимодействия между органом, инициирующим процедуру ограничения доступа, и Роскомнадзором, а также участниками в цепочке «Роскомнадзор – провайдер хостинга – владелец информационного ресурса – оператор связи». То есть после обращения компетентного органа или принятого им решения Роскомнадзор начинает взаимодействовать с информационными посредниками, прежде всего с провайдером хостинга и оператором связи. Провайдером хостинга обеспечиваются идентификация владельца информационного ресурса и направление ему уведомления Роскомнадзора о необходимости удаления противоправного контента. В случаях, когда данное требование исполняется владельцем, процедура непосредственной блокировки дальше не реализуется. Если же этого не происходит, то реализуются следующие стадии работы алгоритма блокировки: ограничения доступа к ресурсу со стороны провайдера хостинга, а при невыполнении данного шага – ограничение доступа к ресурсу со стороны оператора связи. Поэтому статистика работы различных реестров ограничения доступа к информации обычно отражает показатели только блокировок на уровне операторов связи. Тогда как не менее значимыми выступают предыдущие два этапа работы алгоритма, первый из которых предполагает физическое удаление вредного контента с информационного ресурса,

телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // СЗ РФ. 2012. № 44. Ст. 6044.

а второй – блокировку на уровне хостинга. Оба данных метода позволяют полностью исключить доступ к негативной информации, тогда как блокировка на уровне оператора связи – только частично. Она может быть преодолена через использование анонимайзеров и других инструментов.

Основное различие в механизмах ограничения доступа к информации состоит в том, в какой момент применяется блокировка на уровне операторов связи. Если для работы реестров, указанных в ст. 15.1, 15.1–1, 15.1–2 Закона об информации, предусмотрено применение такой блокировки на самой последней стадии, когда все предыдущие шаги не привели к результату, то реестры, установленные ст. 15.3 и 15.3.1 Закона об информации, закрепляют упреждающую блокировку ресурса оператором связи, после которой начинается взаимодействие уже с провайдером хостинга и владельцем ресурса.

Поскольку информационное законодательство, несомненно, будет дальше развиваться в плане введения все новых реестров, требуется определенная унификация их работы. На наш взгляд, вполне рациональным будет создание Единого реестра интернет-ресурсов, содержащих запрещенную для распространения информацию. Это будет особенно значимо при возможной кодификации информационного законодательства РФ. К тому же такой подход облегчит работу Роскомнадзора по администрированию одного Реестра вместо множества подобных.

Следует отметить, что длительное время весьма острой проблемой оставалось ограничение доступа к противоправному контенту в социальных сетях. Это обусловлено тем, что предусмотренные Законом об информации механизмы блокировки затруднительно применить к отдельным страницам социальных сетей, не поставив под угрозу блокировку всего ресурса. В этой связи удаление контента или ограничение доступа к нему обеспечивалось через взаимодействие государственных органов и администрации социальных сетей. Однако здесь возникали очень большие сложности, особенно при взаимодействии с иностранными социальными сетями. Так, в пресс-релизе Роскомнадзора от 27 октября 2021 г. отмечалось систематическое невыполнение видеохостингом YouTube требований российских властей по удалению противоправного контента, включая материалы, пропагандирующие террористические и экстремистские идеи, подстрекающие подростков к социально опасному поведению («зацепингу», «руфингу») и участию в незаконных публичных акциях, а также содержащие пронаркотические и фейковые сведения. Общее количество такой незаконной информации превышает 2,4 тыс. единиц.[590] В этой связи Роскомнадзор вынужден прибегать к механизмам административной ответственности.

[590] Google привлекут к административной ответственности за повторное неудаление запрещенных материалов // Роскомназдор. 27 октября 2021 г. URL: https://rkn.gov.ru/news/rsoc/news73928.htm (дата обращения: 12.12.2021).

Мы уже неоднократно отмечали революционное значение ст. 10.6 Закона об информации, закрепившей обязательства по осуществлению мониторинга социальной сети в целях выявления противоправного контента. При этом перечень такого контента объединяет категории противоправной информации, закрепленной ст. 15.1, 15.1–1 и 15.3 Закона об информации. Но указанной статьей владельцу такой сети предписано также обеспечивать блокировку незаконного контента. Таким образом, законодатель пошел по пути государственно-правового регулирования вопроса, который ранее регламентировался внутренними правилами социальной сети.

Законодательная процедура ограничения доступа выглядит следующим образом. В случае выявления противоправной информации в ходе мониторинга, по результатам рассмотрения обращений или получения предписания Роскомнадзора владелец социальной сети должен незамедлительно ограничить доступ к таким сведениям. В случае возникновения затруднений с идентификацией противоправного контента владелец социальной сети направляет запрос в Роскомнадзор, одновременно временно ограничивая доступ к контенту до принятия решения. Роскомнадзор, в свою очередь, направляет полученный запрос по системе взаимодействия в соответствующие органы для изучения и принятия решений. В качестве правовой гарантии защиты прав пользователей социальной сети закреплено их право обжалования блокировок, осуществленных владельцем социальной сети, или в Роскомнадзор (ч. 8 и 9 ст. 10.6 Закона об информации).

Отметим еще один важный момент. Норма ч. 18 ст. 10.6 Закона об информации закрепила право направления Роскомнадзором предписания о проведении мониторинга социальной сети ее владельцу с целью выявления контента, схожего до степени смешения с ранее удаленной информацией.

В целях реализации контрольно-надзорных полномочий за социальными сетями Роскомнадзору предписано вести *реестр социальных сетей*. В него должны включаться все социальные сети,[591] суточная аудитория которых превышает 500 тыс. интернет-пользователей, находящихся на территории РФ. Согласно сообщению Роскомнадзора от сентября 2021 г. в реестр социальных сетей уже включены Facebook, Twitter, Instagram, TikTok, Likee, Youtube, «ВКонтакте» и «Одноклассники».

[591] Понятие социальной сети определено законом следующим образом: «…информационный ресурс, который предназначен и (или) используется его пользователями для предоставления и (или) распространения посредством созданных ими персональных страниц информации на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации, других языках народов Российской Федерации, на котором может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации».

В данном пресс-релизе изложена правовая оценка новых механизмов ограничения доступа. Роскомнадзор выразил надежду на оперативность зачистки негативного контента администрацией социальных сетей и выполнение ими новых законодательных требований о самоконтроле в интересах безопасности граждан.[592] Насколько такие ожидания оправданы, покажет время. Пока Роскомнадзору приходится, по сути, принуждать крупные иностранные социальные сети к выполнению этих требований, в основном путем штрафных санкций.

Кроме того, для воздействия на крупных информационных посредников, не выполняющих требований российских регуляторов, могут использоваться технические средства противодействия угрозам устойчивости, безопасности и целостности функционирования сети Интернет и сети связи общего пользования на территории РФ (п. 5.1 ст. 46 Закона о связи). Такой прецедент имел место в марте 2021 г., когда Роскомнадзор применил в отношении компании Twitter техническую меру воздействия в виде замедления трафика. В сообщении ведомства причиной такого решения называлось игнорирование сервисом требований об удалении противоправного контента. Поэтому распространение информации интернет-сервисом Twitter внесено в перечень угроз и произведено «первичное замедление скорости работы сервиса».[593]

Значимость проблемы принуждения глобальных IT-корпораций (BigTech) к исполнению российского законодательства обуславливается также и политическими причинами, прежде всего необходимостью адекватного ответа на используемые ими практики откровенной политической цензуры в отношении российских СМИ и журналистов.[594] Г. Г. Камалова также подчеркивает, что проводимая глобальными ИТ-корпорациями цензура в информационном пространстве обусловила введение государствами организационных, правовых и иных мер, направленных на обеспечение права на доступ к информации и своей национальной безопасности.[595]

Одним из последних ответных шагов российских властей в данном направлении явилось принятие Федерального закона от 1 июля

---

[592] Роскомнадзор приступил к формированию реестра социальных сетей // Роскомнадзор. 22 сентября 2021 г. (дата обращения: 23.11.2021).

[593] Роскомнадзор принял меры по защите российских граждан от влияния противоправного контента // Роскомнадзор. 10 марта 2021 г. URL: https://rkn.gov.ru/news/rsoc/news73464.htm (дата обращения: 12.05.2021).

[594] Официальный представитель МИД России Мария Захарова отметила по этому поводу следующее: «Чем больше будут изыматься „модераторами" из интернет-оборота и подвергаться цензуре неудобные с политической точки зрения материалы, тем быстрее и жестче будут вводиться регулятивные ограничения на действия платформ по всему миру» // *Захарова М.* Публикация в личном аккаунте в социальной сети Facebook от 13 марта 2021 г. // Facebook. URL: https://www.facebook.com/maria.zakharova.167/posts/10225625097763943 (дата обращения: 13.03.2021).

[595] *Камалова Г. Г.* Цензура в цифровую эпоху: вопросы правового обеспечения национальной безопасности // Информационное право. 2021. № 2. С. 32–36.

2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации»[596] (далее – Закон о деятельности иностранных лиц). Данным законом для иностранных лиц установлен комплекс правовых обязанностей, включая соблюдение требований, запретов и ограничений, предусмотренных законодательством РФ, а также обязанность создания филиала либо открытия представительства или учреждения российского юридического лица и обеспечения их функционирования на территории РФ. Последняя обязанность носит весьма важный характер, поскольку создает предпосылки для организации надлежащего взаимодействия иностранных IT-компаний с Роскомнадзором при ограничении доступа к противоправному контенту. Собственно, из-за ее ключевого значения сам данный закон в СМИ называют законом о «приземлении» IT-гигантов.[597] За неисполнение установленных обязанностей Закон о деятельности иностранных лиц предусматривает широкий комплекс правовых санкций, которые были рассмотрены нами выше.

На основе вышеизложенного можно смело утверждать, что государство за последние годы заложило целый комплекс правовых гарантий и механизмов, направленных на обеспечение выполнения требований российского законодательства отечественными и зарубежными технологическими компаниями. Это позволяет надеяться, что многолетняя практика игнорирования такими компаниями требований и предписаний российских регуляторов подходит к концу. Вместе с тем здесь возникают риски применения крайних мер к этим компаниям, что может привести к прекращению работы принадлежащих им цифровых сервисов на территории нашей страны. Будем надеяться, что до этого не дойдет и проблема будет решена путем взаимного диалога.

§ 3. Правовые механизмы защиты детей от информации, причиняющей вред их здоровью и развитию

Ключевое значение в системе правового обеспечения ИПБ имеет правовая защита детей от информационно-психологических угроз. Дети выступают одновременно наиболее активной и наиболее уязвимой частью медиааудитории. Проанализированные нами международные стандарты делают акцент на обязательствах государств по особой правовой охране детей от вызовов и рисков цифровой среды.

Как отмечается в Концепции информационной безопасности детей 2016 г. (далее – Концепция ИБ детей), с развитием ИКТ современные дети сталкиваются с новыми угрозами цифровой среды. Агентами

[596] СЗ РФ. 2021. № 27. Ст. 5064.

[597] Принят закон о «приземлении» IT-гигантов // Государственная Дума Федерального Собрания Российской Федерации. 17.06.2021. URL: http://duma.gov.ru/news/51828/ (дата обращения: 12.11.2021).

социализации в «гиперинформационном обществе» выступают не только институты семьи и школы, но и СМИ и Интернет. Причем последние теснят традиционные формы просвещения и обучения молодого поколения.

При выстраивании системы правового обеспечения ИПБ детей важно понимать структуру их современного медиапотребления, которая за последние два десятилетия поменялась самым радикальным образом. Так, уже в 2010 г. исследователями фиксировались существенное снижение интереса к чтению и возрастающая борьба за внимание молодежной аудитории между телевидением и Интернетом.[598] Новейшие исследования показывают, что ведущие каналы медиапотребления современных школьников сосредоточены в Интернете. Цифровым источникам информации отдали предпочтение 83,8% респондентов. Во время качественных интервью школьники говорили, что Интернет стал значимой частью их жизни, без него они могут прожить, но не долго.[599] Наиболее востребованными источниками информации выступают социальные сети (42,2%) и интернет-сайты (41,6%), а телевидение (6,4%), мессенджеры (5,7%) и другие медиа значительно уступают им.

Социально-психологические исследования, проведенные в 2010–2018 гг. коллективом ученых под руководством Г. У. Солдатовой, показали происходящие под влиянием цифровой среды значительные метаморфозы когнитивного и личностного развития современных детей, практик их взаимодействия с окружающим миром и социумом. Среди таких изменений выделены: а) раннее освоение мобильных гаджетов; б) рост длительности нахождения детей в онлайне; в) активное и самостоятельное освоение детьми любых доступных интернет-ресурсов и сервисов, содержащих познавательный и развлекательный контент; г) использование возможностей социальных сетей для самовыражения и освоения социальных ролей; д) существенное расширение круга социального общения подростков за счет виртуальных друзей, с некоторыми из которых они не знакомы в реальной жизни; е) наличие цифрового разрыва между детьми и их родителями, снижения роли последних в их взаимоотношениях.[600] Особо отметим установленное исследователями постоянное столкновение подростков с широким кругом контентных, коммуникационных и иных онлайн-рисков, что несет серьезную опасность по причине отсутствия необходимых компетенций по обеспечению цифровой безопасности у детей и их родителей.[601]

---

[598] СМИ в меняющейся России: монография / Под ред. Е. Л. Вартановой. М.: Аспект Пресс, 2010. С. 234.

[599] Медиапотребление «цифровой молодежи» в России: монография / Под ред. Д. В. Дунаса. М.: Факультет журналистики МГУ: Издательство Московского университета, 2021. С. 119.

[600] *Солдатова Г. У.* Цифровая социализация в культурно-исторической парадигме: изменяющийся ребенок в изменяющемся мире // Социальная психология и общество. 2018. Т. 9. № 3. С. 73–74.

[601] Там же.

Концепция ИБ детей закрепила комплекс приоритетных задач в области обеспечения информационной безопасности детей, включая повышение медийной грамотности детей, формирование у них позитивной и адекватной картины мира, морально-нравственное развитие детей и развитие у них творческих способностей. Признавая значимость выделенных направлений, нельзя не отметить отсутствие среди них собственно активной деятельности государства и гражданского общества по выявлению и нейтрализации угроз информационной безопасности детей. В целом в данном документе сделан избыточный крен в сторону адаптации детей к новой цифровой среде и формирования у них навыков ответственного медиапотребления. Надеемся, что в подготавливаемой в настоящее время новой редакции Концепции ИБ детей данный недостаток будет устранен.

Принятие в 2010 г. Закона о защите детей от информации стало ключевым шагом по формированию системы правового обеспечения ИПБ детей как наиболее уязвимой социальной группы. В его основу были заложены основополагающие международные стандарты и апробированный зарубежный опыт правового регулирования.

До этого момента в России отсутствовал полноценный механизм правовой охраны детей от деструктивного информационно-психологического воздействия. В Федеральном законе от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»[602] декларативно устанавливалась обязанность государственных органов реализовывать меры по защите детей от «информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию», включая различные формы нетерпимости, рекламы алкогольной и табачной продукции, пропаганды неравенства, жестокости, насилия, порнографии, наркомании и антисоциального поведения (ч. 1 ст. 14). Нормами ч. 2 и 3 данной статьи предусматривалась возможность правового закрепления на федеральном или региональном уровне нормативов распространения информационной продукции, не рекомендуемой для детей, а также проведения экспертизы компьютерных и иных игр, детских игрушек и игровых сооружений (далее – игры и игрушки).

Для введения в действие механизма экспертизы в 2000 г. был принят отдельный приказ Минобразования России,[603] закрепивший временный порядок ее проведения государственными учреждениями. Согласно этому порядку все игры и игрушки, которые производятся в стране или импортируются из-за рубежа, должны

[602] СЗ РФ. 1998. № 31. Ст. 3802.

[603] Приказ Минобразования России от 26 июня 2000 г. № 1917 «Об экспертизе настольных, компьютерных и иных игр, игрушек и игровых сооружений для детей» // Вестник образования. 2000. № 17.

проходить обязательную социально-психолого-педагогическую экспертизу. Субъектами проведения такой экспертизы назывались «Федеральный экспертный совет» Минобразования и государственные учреждения, формируемые региональными органами управления образованием. Данный механизм оказался неработоспособным, а в 2007 г. сам приказ № 1917 был признан утратившим силу.

Ситуация изменилась только после принятия Закона о защите детей от информации, который закрепил процедуру экспертизы информационной продукции. Однако значение этого закона гораздо шире. Он является законодательным актом, закрепляющим широкий набор правовых средств защиты детей от негативной информации, включая: а) классификацию вредной информации и определение правового режима ее оборота; б) определение возрастных категорий информационной продукции; в) маркировку информационной продукции; г) требования к обороту отдельных видов и возрастных категорий информационной продукции; д) экспертизу; е) государственный и общественный контроль в рассматриваемой сфере.

В ходе непосредственного участия в подготовке проекта федерального закона № 155209–5 «О защите детей от информации, причиняющей вред их здоровью и развитию» ко второму чтению мы анализировали поступившие многочисленные поправки к законопроекту и готовили правовую позицию по ним. Одним из острых дискуссионных вопросов было распространение норм закона на рекламу. Компромиссным решением она была выведена из предмета регулирования Закона о защите детей от информации. Позже Закон о рекламе был дополнен новыми нормами, касающимися защиты детей в рекламе. Также в ходе обсуждений процедура экспертизы информационной продукции перестала носить обязательный и тотальный характер. Мотивом такого решения послужило опасение повторения печальной судьбы, постигшей механизм экспертизы игр и игрушек, который не заработал из-за отсутствия развитой сети экспертных учреждений.

1 сентября 2012 г. вступили в силу сам Закон о защите детей от информации и корреспондирующий ему Федеральный закон от 21 июля 2011 г. № 252-ФЗ,[604] содержащий комплекс поправок в законы о СМИ, об информации, о рекламе и другие законодательные акты в части обеспечения информационной безопасности детей. В Закон о защите детей от информации впоследствии также неоднократно вносились изменения, касающиеся, в частности, закрепления требований к знакам маркировки информационной продукции, порядка проведения ее экспертизы, корректировки перечня вредной информации, совершенствования государственного контрольно-надзорного механизма и других аспектов.

[604] СЗ РФ. 2011. № 30. Ст. 4600.

Кратко остановимся на анализе основных положений Закона о защите детей от информации. Закон подразделяет вредную информацию на две основных категории: 1) информацию, запрещенную для распространения среди детей; 2) информацию, распространение которой среди детей определенных возрастных категорий ограничено. Изложим в табличном виде виды вредной информации (табл. 5).

Таблица 5

Виды информации, причиняющей вред здоровью и развитию детей согласно Закону о защите детей от информации

№ п/п	Информация, запрещенная для распространения среди детей	Информация, распространение которой среди детей определенных возрастных категорий ограничено
1.	Побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий	Представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия
2.	Способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством	Вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме насильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий
3.	Обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным	Представляемая в виде изображения или описания половых отношений между мужчиной и женщиной
4.	Содержащая изображение или описание сексуального насилия	Содержащая бранные слова и выражения, не относящиеся к нецензурной брани
5.	Отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи	
6.	Оправдывающая противоправное поведение	
7.	Содержащая нецензурную брань	
8.	Содержащая информацию порнографического характера	
9.	О несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия)	

На основе разделения вредной для детей информации на две группы и использования механизма возрастной классификации и маркировки информационной продукции выстроен правовой режим оборота такой продукции:

1) *для информационной продукции, запрещенной для детей (18+):* общий запрет на оборот с оговорками (ч. 1 ст. 11); запрет оборота в местах, доступных для детей, без применения организационных и программно-технических мер защиты детей (ч. 2 ст. 11); обязанность не допускать детей на зрелищные мероприятия категории 18+ (ч. 7.1 ст. 11); запрет распространения в теле- и радиовещании с 4 часов до 23 часов, за некоторыми исключениями (ч. 1 ст. 13); запрет размещения на обложке (первой странице) и упаковке печатных изданий и продукции при распространении ее для неопределенного круга лиц в местах, доступных для детей (ч. 1 ст. 16); наличие запечатанной упаковки для печатной продукции, содержащей запрещенную для детей информацию и распространяемой в местах, доступных для детей (ч. 2 ст. 16); запрет распространения в предназначенных для детей образовательных и иных организациях, а также на расстоянии менее чем сто метров от таких организаций, за определенными исключениями (ч. 3 и 4 ст. 16); запрет продажи, проката, аренды, а также выдачи детям в библиотеках (ч. 5 ст. 16); запрет продажи с использованием автоматов (ч. 6 ст. 16); запрет демонстрации фрагментов фильмов, содержащих запрещенную для детей информацию, при размещении их анонсов в кинотеатрах перед началом показа фильмов возрастных категорий от 0+ до 16+;

2) *для информационной продукции для детей определенных возрастных категорий (0+, 6+, 12+, 16+)*: обязательное наличие возрастной маркировки (знака), за определенными исключениями (ч. 4 ст. 11); размещение маркировки на афишах, входных билетах, объявлениях и иных документах зрелищных мероприятий, звуковое оповещение о недопустимости присутствия детей определенных возрастных категорий (ч. 6 и 7 ст. 11); размещение возрастной маркировки в программах теле- и радиопередач, каталогах информационной продукции, в интернет-материалах (ч. 4 ст. 12); демонстрация маркировки при телевещании (ч. 3 ст. 13); предупредительное звуковое сообщение при радиовещании (ч. 4 ст. 13); наличие возрастной маркировки и (или) текстового предупреждения в аудиовизуальном сервисе (ч. 3 ст. 14).

Кроме того, Законом о защите детей от информации установлены и некоторые общие нормы для защиты детей от любой категории вредной информации. Так, согласно ч. 1 ст. 14 данного закона предоставление доступа к информации в сети Интернет доступных для детей местах возможно при условии применения специальных технических и организационных средств защиты детей от вредного контента.

Таким образом, основными правовыми механизмами обеспечения ИПБ детей в Законе о защите детей от информации выступают возрастная классификация и маркировка информационной продукции, а также введение правовых ограничений на оборот информационной продукции, запрещенной для детей или предназначенной для детей определенных

возрастных категорий, а также на доступ детей к такой информации. Очень важно, что указанный закон распространяется не только на продукцию СМИ, но и другие виды информационной продукции, включая печатные издания, аудиовизуальную продукцию, компьютерные программы и базы данных, интернет-контент.

В отношении распространения действия Закона о защите детей от информации на сеть Интернет необходимо сделать пояснение. Несмотря на включение интернет-контента в перечень видов информационной продукции в ст. 2 Закона, механизм возрастной классификации и маркировки на него не распространяется, о чем сделана оговорка в ч. 4 ст. 11. Вместе с тем в ч. 2 ст. 14 закреплено, что интернет-сайт, не являющийся сетевым изданием, может содержать возрастную маркировку (в том числе машиночитаемую) и (или) текстовое предупреждение о нежелательности для детей определенных возрастных категорий. Данная диспозитивная норма в основном применяется на «сайтах для взрослых» категории 18+ и иногда дополняется механизмом проверки возраста пользователя.

На стадии обсуждения законопроекта в Государственной Думе было принято компромиссное решение о выведении рекламы из-под сферы его действия. Но в дальнейшем ряд значимых поправок был внесен в Закон о рекламе. В частности, они коснулись статей 5 (общие требования к рекламе) и 6 (защита несовершеннолетних в рекламе) данного закона. Вообще Закон о рекламе содержит большое количество норм, касающихся обеспечения ИПБ не только детей, но и взрослых.

Закон о защите детей от информации неоднократно попадал под острую общественную критику. Однако приводимые его оппонентами аргументы при сильной эмоциональной составляющей нередко содержали недостоверные или некорректные аргументы (например, о якобы запрете для детей советского мультфильма «Ну, погоди!», что оказалось фикцией). Кроме того, имелись случаи критики с позиции определенных политических убеждений, разделяемых узкой социальной группой внутри страны и активно лоббируемой из-за рубежа. Наиболее ярким подобным примером выступал шквал замечаний, обрушившихся на Закон после включения в перечень запрещенной информации для детей пропаганды ЛГБТ и неуважения к семейным ценностям. Однако подавляющая часть российского общества поддержала внесенные поправки.[605]

И. С. Иванов на основе исследования систем возрастной классификации информационной продукции в зарубежных странах пришел к выводу о признании экспертным сообществом полезности таких систем для защиты

[605] По данным опроса ВЦИОМ, 88% россиян поддержали введение запрета на пропаганду гомосексуализма, против высказались 7%. См.: Закон о пропаганде гомосексуализма: за и против. ВЦИОМ. Пресс-выпуск № 2320. 11 июня 2013 г. URL: http://wciom.ru/index.php?id=459&uid=114190 (дата обращения: 15.08.2013).

интересов детей. Несмотря на критику отдельных критериев возрастной классификации, среди экспертов есть понимание невозможности угодить всем.[606] В этой связи полагаем, что любые инициативы по изменению возрастных категорий и критериев их выделения, содержащихся в Законе о защите детей от информации, требуют тщательной научной проработки.

Споры вокруг механизма возрастной классификации и маркировки не утихают. Основная критика касается правоприменительной практики в данной области, а именно маркировки конкретных образцов информационной продукции (причем как в стороны занижения, так и завышения). В последние несколько лет депутат Государственной Думы Е. А. Ямпольская вела активную кампанию, направленную на изменение существующей системы возрастной классификации информационной продукции. Основной приводимый ею аргумент состоял в том, что вследствие работы данной системы под ограничение и запрет попадают произведения классической литературы и искусства. В целях устранения данной проблемы Е. А. Ямпольской вместе с коллегами был подготовлен законопроект,[607] которым предлагалось вывести из-под действия ФЗ № 436 использование произведений литературы и искусства, предоставление и распространение «культурных ценностей и культурных благ» организациями культуры. Но главным шагом должна была стать отмена обязательного характера возрастной классификации информационной продукции. Мы возражаем против данной меры, поскольку считаем ее необоснованной.[608]

Но выявленная депутатом Е. А. Ямпольской проблема неправильного применения норм Закона об информации в части возрастной классификации и маркировки классических произведений действительно существует.

---

[606] *Иванов И. С.* Правовая защита детей от информации, причиняющей вред их здоровью и развитию. Расширенный научно-практический комментарий. Подготовлен для СПС «КонсультантПлюс», 2012.

[607] Проект федерального закона № 717228–7 «О внесении изменений в статью 30 Закона Российской Федерации «Основы законодательства Российской Федерации о культуре» и отдельные законодательные акты Российской Федерации в связи с совершенствованием законодательных механизмов, регулирующих доступ детей к культурным ценностям и культурным благам» // Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/bill/717228–7 (дата обращения: 18.05.2021).

[608] Кругом экспертов с нашим участием была проведена правовая оценка законопроекта, по итогам которого они пришли к заключению о дефектности его концепции законопроекта и нецелесообразности его принятия. См.: Заключение на проекты федеральных законов № 717228–7 «О внесении изменений в статью 30 Закона Российской Федерации «Основы законодательства Российской Федерации о культуре» и отдельные законодательные акты Российской Федерации в связи с совершенствованием законодательных механизмов, регулирующих доступ детей к культурным ценностям и культурным благам» и № 717204–7 «О внесении изменений в статью 6.17 Кодекса Российской Федерации об административных правонарушениях» (подготовлено коллективом авторов в составе Абраменковой В. В., Елизарова В. Г., Ермолаевой О. Я., Пристанской О. В., Смирнова А. А. 10 июля 2019 г.) // Российский научно-исследовательский институт культурного и природного наследия им. Д. С. Лихачева. URL: https://heritage-institute.ru/wp-content/uploads/2019/07/Заключение-на-ПФЗ-N-717228-7-и-N-717204–7_26-июля-2019-БП.pdf (дата обращения: 18.05.2021).

Для ее решения, по нашему мнению, требуется принятие специального постановления Правительства, закрепляющего критерии выделения информационной продукции, имеющей значительную историческую, художественную или иную культурную ценность для общества. На их основе Минкультуры России должно формировать реестр данной информационной продукции, подлежащий размещению в сети Интернет.

Также имеются пробелы в области организации государственного контроля (надзора) за соблюдением норм Закона о защите детей от информации. Данный вопрос регламентируется ст. 20 Закона о защите детей от информации и основанными на ее нормах подзаконными нормативными правовыми актами. В изначальной редакции данная функция закреплялась за уполномоченным федеральным органом исполнительной власти. По факту Правительством РФ был определен не один, а несколько уполномоченных органов: Рособрнадзор, Роспотребнадзор, Роскомнадзор и Минкультуры России, у каждого из которых был свой сектор ответственности.[609]

В 2014 г. диспозиция ч. 1 ст. 20 была изменена. Вместо бланкетной нормы, отсылающей к акту Правительства РФ, в самом ее содержании были непосредственно обозначены три ФОИВ, осуществляющих контрольно-надзорные функции за соблюдением требований законодательства РФ в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию: Роскомнадзор, Роспотребнадзор и Рособрнадзор. Трудно понять логику законодателя в части исключения из этого перечня Минкультуры России, поскольку контрольно-надзорные полномочия за ним сохранялись в соответствии с п. 5.4.10.15 Положения о нем.[610] Однако эта логика нашла дальнейшее развитие, когда в 2021 г. данный пункт был исключен из Положения о Минкультуры.[611] Окончательно данная линия была доведена до логического завершения в подзаконном акте Правительства РФ,[612] сохранившем триаду государственных контрольно-надзорных органов.

Получается, что полномочия Минкультуры России по осуществлению контрольно-надзорных функций за соблюдением требований законодательства к обороту информационной продукции, относящейся к аудиовизуальной

---

[609] Постановление Правительства РФ от 24 октября 2011 г. № 859 «О внесении изменений в некоторые акты Правительства Российской Федерации в части распределения полномочий федеральных органов исполнительной власти в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию» // СЗ РФ. 2011. № 44. Ст. 6272.

[610] Положение о Министерстве культуры Российской Федерации (утв. постановлением Правительства РФ от 20 июля 2011 г. № 590) // СЗ РФ. 2011. № 31. Ст. 4758.

[611] Постановление Правительства РФ от 10 апреля 2021 г. № 577 «О внесении изменений в Положение о Министерстве культуры Российской Федерации и признании утратившим силу отдельного положения постановления Правительства Российской Федерации от 24 октября 2011 г. № 859» // СЗ РФ. 2021. № 16. Ст. 2796.

[612] Положение о федеральном государственном контроле (надзоре) за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию (утв. постановлением Правительства РФ от 25 июня 2021 г. № 1019) // СЗ РФ. 2021. № 28. Ст. 5502.

продукции, на любых видах носителей, а также информационной продукции, распространяемой посредством зрелищных мероприятий, никому не были переданы. Такое положение является недопустимым, поскольку целый сектор контрольно-надзорной деятельности попросту выпал. Требуется либо восстановление данного полномочия у Минкультуры России, либо закрепление его за другим ФОИВ, например Роспотребнадзором.

Еще один вопрос организационно-правового плана связан с механизмом возрастной классификации информационной продукции, предусмотренным Законом о защите детей от информации. Согласно нормам данного закона возрастная классификация и маркировка информационной продукции осуществляется ее производителями или распространителями самостоятельно (ст. 6 и 12). Разработчики указанного закона предусмотрели издержки такого порядка (который был компромиссным решением) и заложили страховочный механизм в виде возможности проверки правильности классификации продукции в ходе проведения ее экспертизы. В случае установления наличия в данной информационной продукции вредных для детей сведений либо неправильности присвоенной возрастной маркировки Роскомнадзор выносит предписание об устранении выявленного нарушения. Такое предписание носит обязательный характер для производителя (распространителя) информационной продукции. Указанные субъекты должны привести знак информационной продукции в соответствие, а также обеспечить надлежащий правовой режим оборота данной продукции.

Данный механизм имеет существенные недостатки, обусловленные платностью и длительностью экспертизы информационной продукции. В качестве главного пути совершенствования данного механизма автором еще в 2013 г. предлагалось *учреждение медиаиндустрией специальной структуры (совета) по классификации информационной продукции подобно западным аналогам* (например, британским BBFC или голландским NICAM). Такой совет должен состоять из профессиональных экспертов, а финансирование его деятельности может осуществляться медиакомпаниями.

Данное предложение не утратило своей актуальности. Формирование подобной структуры и наделение ее статусом единого для страны учреждения по возрастной классификации и маркировке информационной продукции позволили бы устранить различия в толковании и выполнять данные процедуры в рамках единой методологии на профессиональной основе.[613]

Еще одно наше предложение касалось *введения контентной маркировки информационной продукции, обозначающей вид содержащегося*

[613] Л. Л. Ефимовой предлагается альтернативный способ решения задачи постановки возрастной классификации и маркировки информационной продукции на профессиональную основу. Он состоит в профессиональном обучении и аттестации маркировщиков, находящихся в штате СМИ. См.: *Ефимова Л. Л.* Правовое регулирование информационной безопасности детей как новый правовой институт информационного права // Аграрное и земельное право. 2018. № 6. С. 131–138.

в ней негативного контента. Такая маркировка должна дополнить существующую возрастную маркировку. Ее основная задача состоит в том, чтобы проинформировать родителей и педагогов о нежелательности информации для детей определенного возраста. Однако люди ей не всегда доверяют, поскольку не знают критериев возрастной классификации и не осведомлены о содержащейся в конкретной продукции вредной информации. Контентная маркировка устранила бы этот недостаток. В качестве образца вполне может быть рекомендована система контентных обозначений европейской системы PEGI.

В случае введения такой маркировки необходимо обязательное проведение упреждающей информационно-разъяснительной работы по информированию граждан о ее назначении и сути. К сожалению, этого не было сделано применительно к возрастной маркировке, что значительно снизило ее эффективность.

Подводя итог анализу норм Закона о защите детей от информации, мы оцениваем его как важнейший нормативный акт, регламентирующий вопросы обеспечения ИПБ детей при обороте широкого перечня информационной продукции, включая продукцию СМИ, печатную продукцию, аудиовизуальную продукцию на любых видах носителей, программы для ЭВМ и базы данных, а также зрелищные мероприятия. Для этой цели указанный закон использует апробированные мировой практикой правовые механизмы возрастной классификации и маркировки информационной продукции, установления ограничений и специальных требований для оборота информационной продукции.

Однако основным недостатком Закона о защите детей от информации выступает его минимальное распространение на ресурсы сети Интернет, прежде всего интернет-сайты и социальные сети, которые и выступают ключевыми источниками угроз ИПБ для детей. Кроме того, сама концепция закона ограничивает поле его регулирования именно вопросами противодействия контентным угрозам. Поэтому угрозы деструктивной коммуникации в сетевом пространстве находятся за пределами его действия.

Хотелось бы также сказать о принятии в 2020 г. весьма важного документа – *Плана мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 годы*[614] (далее – План мероприятий). План мероприятий стал первым государственным программным документом, посвященным обеспечению информационной безопасности детей. До этого подобные мероприятия либо реализовывались институтами гражданского общества при поддержке государства, либо включались в структуру более широких программ по развитию

[614] Приказ Минцифры России от 1 декабря 2020 г. № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 годы» // Вестник образования России. 2021. № 1.

информационного общества. Содержащиеся в документе мероприятия можно условно подразделить на несколько групп:

1) *организационно-правовые мероприятия* (мониторинг законодательства о защите детей от информации, причиняющей вред их здоровью и развитию; подготовка предложений по изменению Концепции ИБ детей; аккумулирование лучших практик проведения мероприятий по обеспечению информационной безопасности детей в субъектах РФ; мониторинг реализации методических рекомендаций по основам информационной безопасности для обучающихся общеобразовательных организаций);

2) *мероприятия государственной поддержки* (оказание поддержки реализации социально значимых проектов в области печатных и электронных СМИ для детей и молодежи со стороны государства);

3) *реализация тематических проектов и акций* (Всероссийского конкурса по разработке информационной продукции для детей «Премия Сетевичок»; Всероссийского конкурса социальной рекламы антинаркотической направленности и пропаганды здорового образа жизни «Спасем жизнь вместе»; Единого урока безопасности в сети Интернет, цикла мероприятий «Сетевичок»);

4) *проведение образовательных и научно-исследовательских мероприятий* (организация повышения компетенции родителей (законных представителей) и работников организаций детства в области цифровой грамотности и информационной безопасности на портале «Учеба.онлайн»; повышение квалификации и профессиональная переподготовка профессорско-преподавательского состава в области информационной безопасности; организация проведения исследования детей и родителей (законных представителей несовершеннолетних) «Образ жизни подростков в сети»);

5) *проведение информационно-технических мероприятий* (реализация информационной платформы для размещения материалов, авторами которых являются дети и детские коллективы образовательных организаций; ограничение доступа к сайтам (страницам сайтов) в сети Интернет, содержащим информацию, распространение которой в Российской Федерации запрещено).

Отдельно стоит выделить такое важное мероприятие, как мониторинг сети Интернет, в том числе закрытых сообществ в социальных сетях, в целях выявления контента, пропагандирующего деструктивное поведение подростков, субкультуры криминального характера, а также деятельность неформальных молодежных объединений противоправной направленности (п. 25).

На основе изложенного можно сделать вывод о весьма прогрессивном характере Плана мероприятий. Главной задачей на ближайшие годы станет его надлежащая реализация ответственными исполнителями.

§ 4. Правовая регламентация информационного противоборства и контрпропаганды

Одной из ключевых угроз информационной безопасности в условиях глобального информационного общества выступает нарастающее информационное противоборство. Еще в Стратегии НБ 2015 отмечалась тенденция нарастания противоборства в глобальном информационном пространстве, вызванная стремлением ряда иностранных государств использовать ИКТ для достижения собственных геополитических целей, используя для это манипулятивные технологии и фальсификацию истории.

Существенное внимание данной угрозе уделено и в новой Стратегии НБ 2021. В ней акцентируется внимание на том, что «рядом государств предпринимаются попытки целенаправленного размывания традиционных ценностей, искажения мировой истории, пересмотра взглядов на роль и место России в ней, реабилитации фашизма, разжигания межнациональных и межконфессиональных конфликтов» (п. 19). Также в документе отмечаются враждебные информационные кампании по дискредитации образа нашей страны и обвинению ее в нарушении международных обязательств, политика дискриминации русского языка, российских СМИ и информационных ресурсов (там же).

У понятия информационного противоборства (далее – ИП) имеется множество определений. Одним из наиболее точных среди них, на наш взгляд, выступает дефиниция С. Н. Гриняева, определившего ИП как «широкомасштабную информационную борьбу с применением средств информационного воздействия на противника в интересах достижения целей воздействующей стороны».[615]

Информационное противоборство (информационные войны) рассматривается как одна из ключевых угроз международной информационной безопасности. Объемное и содержание определение информационной войны содержится в Соглашении ШОС в области МИБ, которое трактует ее как форму противоборства между государствами. Среди методов ее ведения выделена «массированная психологическая обработка населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны» (приложение № 1). В данной дефиниции четко просматривается блок, связанный с деструктивным ИПВ.

Выделение информационно-психологической войны (далее – ИПсВ) как направления информационной войны признается большинством экспертов.[616] Причем теория и практика ИПсВ возникли задолго до

[615] *Гриняев С. Н.* Поле битвы – киберпространство: теория, приемы, средства, методы и системы ведения информационной войны. Минск: Харвест, 2004. С. 83.

[616] Например, в одном из последних диссертационных исследований по данной теме ее автор А. В. Виловатых заключает: «На современном этапе развития

появления концепции информационных войн.[617] Нами разработана авторская концепция такой войны, определены субъекты, направления и формы ведения.[618]

Е. А. Соловьева в своей диссертации 2011 г. пришла к заключению о том, что применение методов ИП в нашей стране связано с противостоянием информационной агрессии в сети Интернет».[619] Разделяем данное мнение, однако считаем необходимым рассматривать в качестве «арены» информационного противоборства не только Интернет, но и СМИ и офлайновые коммуникации. Хотя киберпространство, безусловно, выступает ключевой ареной ИП.

Следует отметить, что инструменты и методы ИП используются в настоящий момент не только государствами, но и иными акторами международной политики, включая: террористические и экстремистские организации; средства массовой информации и блогеров; сообщества хакеров и хактивистов; сообщества журналистов-расследователей и гражданских активистов; отдельных лиц; неправительственные организации; коммерческие организации.[620]

В контексте проблематики ИПБ особое внимание заслуживает деструктивная информационная активность террористических и экстремистских организаций. В Стратегии НБ 2021 отмечается стремление террористических и экстремистских организаций усилить пропагандистско-вербовочную деятельность в отношении граждан России, в том числе в целях вовлечения российской молодежи в противоправные действия (п. 44). Также обращается внимание на использование экстремистами методов дезинформации, включая акции «телефонного терроризма», подстрекательства к массовым беспорядкам, участию в незаконных публичных акциях, совершению суицида (п. 52).

информационное противоборство интегрирует совокупность информационных операций, реализующихся в двух основных формах: информационно-психологического воздействия на массовое и индивидуальное сознание, а также информационно-технического воздействия, нацеленного на кибернетическую сферу». См.: *Виловатых А. В.* Информационное противоборство в политическом процессе: тренды цифровой реальности: дис. … д-ра полит. наук. М., 2021. С. 13.

[617] *Лайнбарджер П.* Психологическая война / Пер. с англ. М.: Воениздат, 1962; *Зазворка Г.* Психологическая война НАТО. М.: Воениздат, 1963; *Бобиков А. Ф.* Психологическая война империалистических государств против стран социализма и пути борьбы с подрывной пропагандой противника: дис. … канд. пед. наук. М., 1966; *Волкогонов Д. А.* Психологическая война: подрывные действия империализма в области общественного сознания. М.: Воениздат, 1984.

[618] *Смирнов А. А.* Информационно-психологическая война. Об одном средстве международного информационного противоборства // Свободная мысль. 2013. № 6. С. 81–96.

[619] *Соловьева Е. А.* Информационное противоборство в сети Интернет: политологический анализ: автореф. дис. … канд. полит. наук. Пятигорск, 2011. С. 9.

[620] *Смирнов А. А.* Негосударственные акторы в современных информационных войнах // Международная жизнь. 2018. № 5. С. 83–99.

Проведенный автором совместно с профессором И. Ю. Сундиевым анализ научной литературы по теме[621] позволил выделить следующие ключевые направления использования СМИ и интернет-ресурсов в террористических и экстремистских целях: 1) пропаганда и устрашение; 2) вербовка и подстрекательство; 3) подготовка (обучение); 4) планирование и координация деятельности; 5) финансирование; 6) кибератаки на информационные системы (кибертерроризм).[622] Как видим, значительная часть перечисленного связана с оказанием деструктивного ИПВ, что позволяет отнести их к угрозам ИПБ. Более того, именно пропаганда экстремистской идеологии выступает, на наш взгляд, главной формой информационного терроризма и экстремизма.

Ключевая мысль автора состоит в том, что *для противодействия использованию методов ИП со стороны иностранных государств и иных акторов международной политики необходимы ответные действия с применением информационных инструментов, то есть ведение встречного или упреждающего информационного противоборства*.

Понимание информационного противоборства как целостного и самостоятельного направления деятельности правоохранительных органов и вооруженных сил уже давно сложилось в научной литературе политологического и военного профилей. ИП постепенно «пробивает себе дорогу» в нормативных актах и документах стратегического планирования.

Так, если в Доктрине ИБ 2016 совершенствование сил и средств информационного противоборства было выделено в качестве

---

[621] *Цыганов В.* Медиа-терроризм. Терроризм и средства массовой информации. Киев: Ника-Центр, 2004; Психология и психопатология терроризма. Гуманитарные стратегии антитеррора. Сборник статей под ред. проф. М. М. Решетникова. СПб.: Восточно-Европейский Институт Психоанализа, 2004; *Гарев В. А.* Информационные угрозы современного международного терроризма. М.: Институт Африки РАН, 2010; *Мкртычян А. А.* Влияние средств массовой информации на психологические последствия терроризма: автореф. дис. … канд. психол. наук. М., 2012; *Вейман Г.* Как современные террористы используют Интернет. Специальный доклад № 116 // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/analytics/Tropina_01/ (дата обращения: 12.04.2013); *Конвей М.* Использование террористами сети Интернет и борьба с этим явлением // Владивостокский центр исследования организованной преступности. URL: http://www.crime.vl.ru (дата обращения: 12.05.2013); Использование Интернета в террористических целях. Управление Организации Объединенных Наций по наркотикам и преступности, 2013; *Горбатова В. В.* Информационно-пропагандистская политика радикальных исламских организаций (на примере Хамас, «Хизбаллы» и «Аль-Каиды»): автореф. дис. … канд. полит. наук. М., 2013; Основы борьбы с киберпреступностью и кибертерроризмом. Хрестоматия / Овчинский В. С. (сост.). М.: Норма, 2017.

[622] *Сундиев И. Ю., Смирнов А. А.* Использование информационных сетей в экстремистской и террористической деятельности // Научный портал МВД России. 2014. № 1. С. 84–91; *Сундиев И. Ю., Смирнов А. А.* Медиаресурсы в экстремистской и террористической деятельности: функциональный анализ // Свободная мысль. 2014. № 4. С. 55–72; *Сундиев И. Ю., Смирнов А. А., Кундетов А. И., Федотов В. П.* Теория и практика информационного противодействия экстремистской и террористической деятельности: монография. М.: ФГКУ «ВНИИ МВД России», 2014. С. 21–79.

направления обеспечения информационной безопасности в области обороны страны (пп. «б» п. 21), то в новой Стратегии НБ 2021 развитие таких сил и средств уже обозначено в числе ключевых задач государственной политики обеспечения информационной безопасности в целом (пп. 10 п. 57). Участие в проведении мероприятий информационного противоборства нормативно закреплено в перечне задач ряда правоохранительных органов и спецслужб, в частности ФСБ России (пп. 20.3 п. 9 Положения о ФСБ России),[623] ФСО России (пп. 23.1 п. 12 Положения о ФСО России)[624] и Росгвардии (пп. 50 п. 9 Положения о Росгвардии).[625]

В контексте обеспечения ИПБ главную роль играет ведение информационно-психологического противоборства, основу которого составляет *контрпропаганда*. В действующей Доктрине ИБ 2016 контрпропаганда не упоминается, тогда как в Доктрине ИБ 2000 содержался ряд релевантных положений. В частности, в числе основных мероприятий в области обеспечения информационной безопасности РФ в сфере внутренней политики упоминалась «активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России» (раздел 6).

Под контрпропагандой понимается «деятельность по оказанию информационно-психологического воздействия на людей и социальные группы в целях нейтрализации пропаганды противника».[626] Нами разработана практическая модель организации контпропагандистской работы применительно к области борьбы с терроризмом и экстремизмом.[627]

Значимость контрпропаганды как направления обеспечения ИПБ определяется следующими факторами: 1) преимущественно превентивный характер; 2) безальтернативность в случае невозможности воздействия на источник угроз ИПБ или канал передачи информации; 3) способность ослаблять или нейтрализовывать влияние самих деструктивных идей, лежащих в основе многих видов ИПВ.

---

[623] Положение о Федеральной службе безопасности Российской Федерации (утв. Указом Президента РФ от 11 августа 2003 г. № 960) // СЗ РФ. 2003. № 33. Ст. 3254.

[624] Положение о Федеральной службе охраны Российской Федерации (утв. Указом Президента РФ от 7 августа 2004 г. № 1013) // СЗ РФ. 2004. № 32. Ст. 3314.

[625] Положение о Федеральной службе войск национальной гвардии Российской Федерации (утв. Указом Президента РФ от 30 сентября 2016 г. № 510) // СЗ РФ. 2016. № 41. Ст. 5802.

[626] *Смирнов А. А.* Организация контрпропаганды в области борьбы с терроризмом и экстремизмом: научно-практическое пособие / А. А. Смирнов; под ред. А. П. Новикова. М.: АТЦ СНГ, 2020. С. 14.

[627] *Сундиев И. Ю., Смирнов А. А., Кундетов А. И., Федотов В. П.* Теория и практика информационного противодействия экстремистской и террористической деятельности: монография. М.: ФГКУ «ВНИИ МВД России», 2014; *Смирнов А. А.* Организация контрпропаганды в области борьбы с терроризмом и экстремизмом: научно-практическое пособие. М.: АТЦ СНГ, 2020.

Информационно-психологическое воздействие в ходе ведения контрпропаганды может оказываться как на источник угроз ИПБ, так и на объекты ИПБ – человека, социальные группы и общество – в целях повышения их психологической сопротивляемости внешнему вредоносному воздействию.

Проведенный анализ правового регулирования контрпропаганды в области борьбы с терроризмом и экстремизмом в России и других странах СНГ показал, что оно носит весьма фрагментарный характер.[628] В нашей стране в Федеральном законе от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»[629] (далее – Закон о противодействии терроризму) к полномочиям органов местного самоуправления отнесено проведение «информационно-пропагандистских мероприятий по разъяснению сущности терроризма и его общественной опасности, а также по формированию у граждан неприятия идеологии терроризма» (ст. 5.1). Подчеркивая важность данной нормы Закона о противодействии терроризму, нельзя не указать на странность, заключающуюся в наделении полномочиями по проведению информационно-пропагандистских мероприятий исключительно органов местного самоуправления. Дело в том, что начиная с 2008 г. мероприятия по противодействию идеологии терроризма осуществляются в рамках межведомственных комплексных планов, утверждаемых президентом РФ.[630] В настоящее время действует Комплексный план противодействия идеологии терроризма на 2019–2023 гг. Основными исполнителями мероприятий данного плана выступают именно федеральные и региональные органы власти, поэтому для них также необходимо законодательно закрепить полномочия по ведению контрпропаганды в сфере противодействия терроризму, внеся соответствующие дополнения в профильный федеральный закон.

Необходимо отметить, что на уровне СНГ имеется положительный пример правовой регламентации контрпропаганды в рассматриваемой сфере. В модельном законе СНГ «О противодействии терроризму» от 3 декабря 2009 г.[631] содержится отдельная глава III, посвященная информационно-пропагандистскому противодействию терроризму. В ней регламентированы цели и задачи государственных органов (ст. 8), обязательства СМИ в данной сфере и меры ответственности за их невыполнение (ст. 9 и 10).

К числу целей осуществления контрпропаганды в модельном законе отнесены: а) разъяснение опасности терроризма; б) разоблачение

---

[628] *Смирнов А. А.* Правовое регулирование контрпропаганды в области борьбы с терроризмом в законодательстве государств – участников СНГ // Содружество. 2019. № 4. С. 38–43.

[629] СЗ РФ. 2006. № 11. Ст. 1146.

[630] Противодействие терроризму в Российской Федерации: сборник учебных материалов. Аппарат Национального антитеррористического комитета. М., 2019. С. 100.

[631] Информационный бюллетень МПА СНГ. 2010. № 46. С. 256–283.

форм, методов и приемов пропаганды идеологии терроризма; в) формирование антитеррористического сознания и др.

Сложность в правовом регулировании контрпропаганды, как и информационного противоборства в целом, состоит в том, что они в полной мере не относятся к традиционным видам правоохранительной деятельности и включают комплекс уникальных средств и методов ИП. Поэтому *контрпропаганда требует правовой институционализации, но не в самостоятельном виде, а в составе правового института информационного противоборства, которое также включает в себя направление информационно-технического воздействия*.

Данная идея отчасти воплощена в принятом в 2018 г. модельном законе ОДКБ «Об информационном противоборстве терроризму и экстремизму».[632] Однако на национальном уровне подобных законов в странах ОДКБ и СНГ до настоящего времени нет. Авторская точка зрения состоит в том, что не следует ограничивать предмет правового регулирования исключительно вопросами информационного противоборства терроризму и экстремизму. Инструментарий ИП применим для противодействия широкому комплексу информационных угроз внутреннего и внешнего характера, причем средства, методы, формы и каналы оказания информационного воздействия являются общими вне зависимости от сферы проявления таких угроз. Полагаем необходим учесть данное методологическое замечание при совершенствовании модельного законодательства СНГ и ОДКБ в сфере ИП, равно как и российского законодательства.

В случае разработки отдельного законодательного акта в сфере ИП в нем должны быть закреплены правовые дефиниции базовых понятий, основные виды мероприятий ИП, субъекты и общие условия их проведения, включая вопросы допустимости ограничения прав граждан.

---

[632] Модельный закон ОДКБ «Об информационном противоборстве терроризму и экстремизму» (утв. постановлением Парламентской ассамблеи ОДКБ от 30 октября 2018 г. № 11–3.3) // Парламентская ассамблея ОДКБ. URL: https://paodkb.org/documents/modelnyy-zakon-odkb-ob-informatsionnom-protivoborstve-terrorizmu (дата обращения: 12.09.2019).

ГЛАВА V. ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

§ 1. Развитие системы органов обеспечения информационно-психологической безопасности

Обеспечение национальной безопасности предполагает осуществление целенаправленной, широкомасштабной и многоплановой деятельности различных субъектов. Важнейшим условием эффективности их работы является создание соответствующим образом организованной системы, предполагающей определенное объединение усилий субъектов, упорядочение их функций и взаимоотношений, целенаправленное использование их возможностей в изменяющихся условиях противодействия возникающим угрозам в различных сферах общественной жизни.[633]

Институциональная подсистема является элементом системы обеспечения ИПБ наряду с правовым и инструментальным компонентами, охватывающими перечень субъектов такого обеспечения. С другой стороны, она также может рассматриваться как часть общей системы обеспечения информационной безопасности РФ, которая представляется собой совокупность сил и средств обеспечения информационной безопасности (пп. «ж» п. 2 Доктрины ИБ 2016).

Мы поддерживаем позицию исследователей о целесообразности условного подразделения системы обеспечения безопасности на две подсистемы: государственную, включающую органы публичной власти, и негосударственную, охватывающую граждан и общественные институты.[634]

Основным субъектом обеспечения безопасности было и остается государство, несмотря на тенденции роста потенциала негосударственных акторов на внутриполитической и международной арене. В Доктрине ИБ 2016 закреплено, что организационную основу системы обеспечения информационной безопасности составляют органы публичной власти,

[633] Правовая основа обеспечения национальной безопасности Российской Федерации: монография / Под ред. проф. А. В. Опалева. М.: ЮНИТИ-ДАНА, 2004. С. 83.

[634] *Выборнов В. Я.* Развитие, угрозы, безопасность в XXI веке и Россия. М.: ИВ РАН, 2007. С. 109–110; Общая теория национальной безопасности: учебник / Под общ. ред. А. А. Прохожева. 2-е изд., доп. М.: РАГС, 2005. С. 169; Основы обеспечения безопасности России: учебное пособие / М. И. Дзлиев, А. Д. Урсул; Рос. гос. торгово-экон. ун-т, НИИ проблем безопасности и устойчивого развития. М.: Экономика, 2003. С. 53–61.

включая палаты Федерального Собрания, Правительство РФ, Совет Безопасности, межведомственные и иные органы (п. 33). Они выступают субъектами обеспечения ИПБ и реализуют свои функции в данной сфере в пределах своих полномочий. Среди субъектов обеспечения ИПБ ключевую роль играют профильные федеральные органы исполнительной власти (далее – ФОИВ). В ранее действовавшем Законе РФ «О безопасности» предусматривалось образование государственных органов обеспечения безопасности для непосредственной реализации функций в области безопасности (ст. 4). Такие органы в основном относятся к группе ФОИВ, руководство деятельностью которых осуществляет Президент РФ. Однако в рассматриваемой сфере не менее значима роль и иных ФОИВ, не входящих в «силовой блок», руководство деятельностью которых осуществляет Правительство РФ. К ним, например, можно отнести Минцифры и Роскомнадзор.

Рассмотрим задачи и функции наиболее значимых ФОИВ в области обеспечения ИПБ.

1. Министерство внутренних дел Российской Федерации (МВД России) является ФОИВ, осуществляющим нормативные и правоприменительные функции в сфере внутренних дел. Деятельность органов внутренних дел регламентируется комплексом нормативных правовых актов, главным из которых является Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»[635] (далее – Закон о полиции). Правовой статус МВД России закреплен в Положении о Министерстве[636] (далее – Положение о МВД).

Анализ норм Закона о полиции и Положения о МВД, действующей структуры центрального аппарата МВД России позволил выделить четыре основных направления деятельности органов внутренних дел в сфере обеспечения ИПБ:

1) противодействие преступности в сфере ИПБ – включает предупреждение, выявление, пресечение, раскрытие и расследование преступлений, связанных с оказанием деструктивного ИПВ. Задачи в области профилактики преступлений и иных правонарушений возложены на многие подразделения органов внутренних дел (патрульно-постовую службу, подразделения ГИБДД и др.), но основную роль здесь играют служба участковых уполномоченных полиции[637] и подразделения по делам несовершеннолетних.[638] Борьбу с преступностью

[635] СЗ РФ. 2011. № 7. Ст. 900.

[636] Положение о Министерстве внутренних дел Российской Федерации (утв. Указом Президента РФ от 1 марта 2011 г. № 248) // СЗ РФ. 2016. № 52. Ст. 7614.

[637] Приказ МВД России от 29 марта 2019 г. № 205 «О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организации этой деятельности» // СПС «СТРАС-Юрист».

[638] Приказ МВД России от 15 октября 2013 г. № 845 «Об утверждении инструкции по организации деятельности подразделений по делам несовершеннолетних органов внутренних дел Российской Федерации» // СПС «СТРАС-Юрист».

осуществляют оперативные подразделения органов внутренних дел, включая уголовный розыск, подразделения экономической безопасности и противодействия коррупции, по противодействию экстремизму, по борьбе с преступлениями, совершаемыми с использованием информационных технологий (Управление «К»);

2) противодействие административной деликтности в сфере ИПБ – включает предупреждение и выявление административных правонарушений, связанных с оказанием деструктивного ИПВ либо нарушением правил в сфере ИПБ, а также производство по делам о таких правонарушениях. Полиция наделена полномочиями по выполнению «полного цикла» производства по делам об административных правонарушениях, начиная с приема заявлений об административных правонарушениях и завершая исполнением административных наказаний. Анализ п. 1 ч. 2 ст. 28.3 КоАП РФ позволяет выделить большой перечень составов административных правонарушений, относящихся к сфере ИПБ, по которым должностные лица органов внутренних дел вправе составлять протоколы об административных правонарушениях, в том числе: «Пропаганда наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ» (ст. 6.13); «Изготовление юридическим лицом материалов или предметов с порнографическими изображениями несовершеннолетних и оборот таких материалов или предметов» (ст. 6.20); «Пропаганда нетрадиционных сексуальных отношений среди несовершеннолетних» (ст. 6.21); «Заведомо ложный вызов специализированных служб» (ст. 19.13); «Мелкое хулиганство» (ст. 20.1); «Производство и распространение экстремистских материалов» (ст. 20.29) и др.;

3) противодействие терроризму и экстремизму – включает реализацию мер, направленных на предупреждение, выявление и пресечение экстремистской деятельности граждан и организаций (п. 16 ч. 1 ст. 12 Закона о полиции), противодействие терроризму (п. 17 ч. 1 ст. 12). Основную роль в противодействии экстремизму и терроризму в системе МВД России играют подразделения по противодействию экстремизму, которые реализуют широкий комплекс мероприятий по противодействию угрозам ИПБ экстремистского толка. Проводится целенаправленная профилактическая работа в Интернете, пресекаются факты публичных призывов к осуществлению экстремистской деятельности, возбуждения ненависти либо вражды, а равно унижения человеческого достоинства. Отдельное внимание уделяется пресечению противоправной деятельности различных деструктивных сект и тоталитарных культов, практикующих насилие над личностью, причиняющих вред физическому

и психическому здоровью, совершающих иные злоупотребления при реализации свободы совести и вероисповедания.[639] Важное значение придается информационному противодействию угрозам терроризма и экстремизма. Подготовленные с участием автора научно-методические издания по данной тематике[640] успешно внедрены в работу профильных подразделений МВД России;

4) информационное сопровождение деятельности МВД России – включает реализацию мер по доведению до общества информации о деятельности органов внутренних дел и реагирование на резонансные информационные поводы. Данная задача возложена на подразделения информации и общественных связей МВД России. В контексте обеспечения ИПБ большое значение имеет использование информационной работы МВД России для профилактики угроз в цифровой среде. Посредством выступлений официального представителя министерства и иных должностных лиц в СМИ, размещения информации на ведомственных ресурсах МВД России в сети Интернет, распространения тематических печатных изданий и иной информационной продукции полиция осуществляет оповещение общества о существующих информационных угрозах, формах и способах их проявления, а также методах и средствах защиты от них.[641] Кроме того, подразделения информации и общественных связей во взаимодействии с другими подразделениями министерства выполняют важную функцию противодействия дискредитации ведомства и отдельных сотрудников полиции.[642]

2. Федеральная служба безопасности Российской Федерации (ФСБ России) является ФОИВ, осуществляющим широкий круг функций по обеспечению безопасности, в том числе в сфере информационной безопасности. Правовую основу деятельности ФСБ России составляют Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности»[643]

---

[639] Не допустить ненависти и вражды. Начальник Главного управления по противодействию экстремизму МВД России генерал-майор полиции Олег Ильиных // Полиция России. 2019. № 9. С. 10–14.

[640] *Сундиев И. Ю., Смирнов А. А., Кундетов А. И., Федотов В. П.* Теория и практика информационного противодействия экстремистской и террористической деятельности: монография. М.: ФГКУ «ВНИИ МВД России», 2014; *Смирнов А. А.* Организация контрпропаганды в области борьбы с терроризмом и экстремизмом: научно-практическое пособие; под ред. А. П. Новикова. М.: АТЦ СНГ, 2020.

[641] Так, в настоящий момент на сайте МВД России имеется тематический раздел «Безопасный Интернет – детям». См.: Безопасный Интернет – детям // МВД России. URL: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/безопасный-интернет-детям (дата обращения: 01.07.2021).

[642] Приказ МВД России от 19 декабря 2018 г. № 850 «Об организации защиты чести, достоинства и деловой репутации сотрудников органов внутренних дел Российской Федерации, федеральных государственных гражданских служащих и работников системы МВД России в связи с осуществлением ими служебной деятельности, деловой репутации подразделений системы МВД России» // СПС «СТРАС-Юрист».

[643] СЗ РФ. 1995. № 15. Ст. 1269.

(далее – Закон о ФСБ), Положение о Службе[644] (далее – Положение о ФСБ) и иные правовые акты.

Анализ Положения о ФСБ показывает, что основные задачи и функции ФСБ в сфере обеспечения информационной безопасности скорее относятся к защите информации (включая сведения, составляющие государственную тайну) и информационных систем. Вместе с тем Служба выполняет и ряд функций, касающихся обеспечения ИПБ, в частности в рамках разведывательной и контрразведывательной деятельности, борьбы с терроризмом и преступностью (ст. 9–11 Закона о ФСБ). 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» (ст. 9 Закона о ФСБ). По нашему мнению, «иная деятельность» иностранных структур может включать и подрывную деятельность информационно-психологического характера, направленную на дестабилизацию обстановки в стране и провоцирование социальных конфликтов.

Отдельно стоит сказать о противодействии терроризму. Помимо решения основного комплекса задач по силовой борьбе с терроризмом органами безопасности также осуществляется деятельность по профилактике терроризма, в том числе по противодействию идеологии терроризма. Эти задачи возложены на Национальный антитеррористический комитет (далее – НАК) – коллегиальный орган, координирующий и организующий антитеррористическую деятельность в масштабах страны.[645] Председателем НАК является Директор ФСБ России.

В рамках закрепленных направлений деятельности ФСБ России органы безопасности наделены полномочиями по проведению разведывательных и оперативно-разыскных мероприятий, следственных действий, процессуальных действий в рамках производства по делам об административных правонарушениях, использованию специальных методов и средств, осуществлению внешних сношений со специальными службами и правоохранительными органами иностранных государств и другими полномочиями (ст. 13 Закона о ФСБ).

3. Министерство обороны Российской Федерации (Минобороны России) является ФОИВ, осуществляющим функции по обеспечению обороны страны. Правовую основу деятельности Минобороны России составляют Федеральный закон от 31 мая 1996 г. № 61-ФЗ «Об обороне» (далее – Закон об обороне), Положение о Министерстве[646] (далее – Положение о Минобороны).

---

[644] Положение о Федеральной службе безопасности Российской Федерации (утв. Указом Президента РФ от 11 августа 2003 г. № 960) // СЗ РФ. 2003. № 33. Ст. 3254.

[645] Цели и задачи // Национальный антитеррористический комитет. URL: http://nac.gov.ru/nak/celi-i-zadachi.html (дата обращения: 12.01.2021).

[646] Положение о Министерстве обороны Российской Федерации (утв. Указом Президента РФ от 16 августа 2004 г. № 1082) // СЗ РФ. 2004. № 34. Ст. 3538.

Необходимо отметить, что под обороной, выступающей сферой деятельности профильного министерства, понимаются система политических, экономических, военных, социальных, правовых и иных мер по подготовке к вооруженной защите и вооруженная защита РФ, целостности и неприкосновенности ее территории (ч. 1 ст. 1 Закона об обороне). Оборона выступает элементом безопасности и одной из важнейших функций государства.[647] Ключевое положение Минобороны России в системе организации обороны проявляется в управлении им Вооруженными Силами Российской Федерации (далее – ВС РФ). Министерство решает широкий круг задач в области обеспечения обороны страны, организации деятельности ВС РФ и подведомственных ФОИВ (п. 3 Положения о Минобороны).

Деятельность Минобороны России в сфере обеспечения ИПБ осуществляется в рамках трех основных направлений: 1) противодействие психологическим операциям вооруженных сил противника; 2) противодействие внутренним угрозам ИПБ для ВС РФ; 3) информационное обеспечение деятельности государственной политики в области обороны и деятельности ВС РФ.

Первое направление предполагает получение информации о намерениях, планах и действиях вооруженных сил иностранных государств по ведению психологических операций и реализацию комплекса мер по противодействию им. Данные функции в основном реализуются Генеральным штабом ВС РФ.[648] Второе направление осуществляется в рамках воспитания военнослужащих ВС РФ, психологической работы, мероприятий по социологическому и психологическому мониторингу в ВС РФ, а также военно-политической работы в ВС РФ (п. 40–41 Положения о Минобороны). В настоящее время данные функции выполняют воссозданное Главное военно-политическое управление ВС РФ и Департамент психологической работы Минобороны России. Третье направление традиционно относится к деятельности пресс-служб. Данная работа осуществляется Департаментом информации и массовых коммуникаций Минобороны России и пресс-секретарем министра обороны.

4. Министерство иностранных дел Российской Федерации (МИД России) является ФОИВ, реализующим функции в области международных отношений России. Нормативную основу деятельности МИД России составляют федеральные законы и Положение о Министерстве[649] (далее – Положение о МИД).

---

[647] Военное право: учебник для военно-учебных заведений Вооруженных Сил РФ / Под ред. Н. И. Кузнецова. М.: Военный университет МО РФ, 1996. С. 22.

[648] Указ Президента Российской Федерации от 23 июля 2013 г. № 631 «Вопросы Генерального штаба Вооруженных Сил Российской Федерации» // СЗ РФ. 2013. № 30. Ст. 4085.

[649] Положение о Министерстве иностранных дел Российской Федерации (утв. Указом Президента РФ от 11 июля 2004 г. № 865) // СЗ РФ. 2004. № 28. Ст. 2880.

МИД России решает широкий круг задач, связанных с разработкой и реализацией стратегии внешней политики РФ, защиты безопасности и интересов России на международной арене с использованием дипломатических и международно-правовых средств. Министерство осуществляет свою деятельность как непосредственно, так и через загранучреждения.

Роль МИД в сфере обеспечения информационной безопасности состоит в продвижении национальных интересов России в данной области на международной арене, организации международного сотрудничества в области противодействия информационным угрозам и обеспечении МИБ. Во многом благодаря квалифицированной работе МИД России вопросы МИБ были впервые включены в повестку Генеральной ассамблеи ООН, создав основу для конструктивного международного диалога. Ранее данной темой занимался Департамент по вопросам новых вызовов и угроз, однако в 2019 г. был создан отдельный Департамент международной информационной безопасности.

Значимой функцией МИД России также выступает информационное обеспечение внешней политики и противодействие негативным информационным вбросам, исходящим от зарубежных государств и иностранных негосударственных акторов, а также международных организаций. Эта работа осуществляется Департаментом информации и печати МИД России совместно с загранучреждениями.

5. Федеральное агентство по делам Содружества Независимых Государств, соотечественников, проживающих за рубежом, и по международному гуманитарному сотрудничеству (Россотрудничество) является ФОИВ, осуществляющим функции в сфере международных отношений РФ со странами СНГ и иными государствами, а также международного гуманитарного сотрудничества. Его правовой статус определен Положением об агентстве[650] (далее – Положение о Россотрудничестве). Россотрудничество подведомственно МИД России.

За рубежом Россотрудничество реализует свои функции преимущественно через российские центры науки и культуры, информационно-культурные центры, дома науки и культуры и иные представительства (п. 5 Положения о Россотрудничестве). Согласно данным официального сайта агентства, по состоянию на 2021 г. Россотрудничество представлено в 80 странах мира 97 представительствами: 73 российскими центрами науки и культуры в 62 странах, 24 представителями агентства в составе посольств в 21 стране.[651]

---

[650] Положение о Федеральном агентстве по делам Содружества Независимых Государств, соотечественников, проживающих за рубежом, и по международному гуманитарному сотрудничеству (утв. Указом Президента РФ от 6 сентября 2008 г. № 1315) // СЗ РФ. 2008. № 37. Ст. 4181.

[651] О Россотрудничестве // Россотрудничество. URL: https://rs.gov.ru/ru/about (дата обращения: 23.06.2021).

В настоящее время Россотрудничество выступает ключевым субъектом, формирующим и использующим «мягкую силу» внешнего воздействия России на сообщества иностранных государств. Одной из форм работы Россотрудничества выступает реализация целевых проектов (программ), направленных на укрепление международных связей, тесное сотрудничество в гуманитарной сфере и формирование позитивного имиджа России за рубежом. Среди реализуемых программ можно отметить следующие: «Стратегические коммуникации российского СМР», программа краткосрочных ознакомительных поездок в РФ молодых представителей политических, общественных, научных и деловых кругов иностранных государств «Новое поколение» и др.[652]

Таким образом, Россотрудничество обеспечивает ИПБ путем формирования положительного образа России в мире, трансляции российских ценностей за рубежом, противодействуя таким образом целенаправленной политике и враждебным информационным кампаниям иностранных государств, направленным на дискредитацию нашей страны.

6. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) является ФОИВ, осуществляющим нормотворческие и правоприменительные функции в сфере информационных технологий, электросвязи и почтовой связи, массовых коммуникаций и средств массовой информации. Правовой статус Минцифры закреплен Положением о Министерстве[653] (далее – Положение о Минцифры).

Роль Минцифры России в обеспечении ИПБ прежде всего состоит в выработке государственной политики и правовом регулировании вопросов обеспечения безопасности в сфере массовых коммуникаций, включая подготовку законопроектов, актов Президента РФ и Правительства РФ, а также принятие собственных нормативных правовых актов (п. 5.1 и 5.2 Положения о Минцифры).

Вторым важным направлением работы Минцифры России по обеспечению ИПБ являются выработка политики и нормотворчество в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию. В отличие от первого направления, которое носит весьма широкий характер и включает аспекты безопасности среди многих других, данное направление полностью относится к сфере ИПБ. Здесь Минцифры осуществляет разработку документов стратегического планирования, проектов федеральных законов, нормативных правовых актов Президента РФ и Правительства РФ, а также подготовку и реализацию мероприятий по обеспечению информационной безопасности детей.

---

[652] Государственные программы // Россотрудничество. URL: https://rs.gov.ru/ru/pages/2 (дата обращения: 23.06.2021).

[653] Положение о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации (утв. постановлением Правительства РФ от 2 июня 2008 г. № 418) // СЗ РФ. 2008. № 23. Ст. 2708.

В рамках реализации данных полномочий Минцифры России (ранее – Минкомсвязи России) была подготовлена Концепция информационной безопасности детей, принят ряд приказов в рамках реализации Закона о защите детей, а также утвержден план тематических мероприятий.[654]

Помимо рассмотренных двух ключевых сфер роль Минцифры России в обеспечении ИПБ проявляется и в области публичной дипломатии в рамках обеспечения участия российских СМИ в формировании положительного имиджа России у зарубежных аудиторий (п. 5.3.3 Положения о Минцифры).

7. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является ФОИВ, осуществляющим контрольно-надзорные функции в сфере средств массовой информации и коммуникации. Правовой статус Роскомнадзора регламентируется Положением о Службе[655] (далее – Положение о Роскомнадзоре).

Роскомнадзор находится в ведении Минцифры России и занимается теми же сферами обеспечения ИПБ, что и головное Министерство. Однако в отличие от него служба реализует не регулятивные, а контрольно-надзорные функции в указанных областях. В соответствии с Положением о Роскомнадзоре этот орган осуществляет контрольно-надзорные функции в сферах СМИ и массовых коммуникаций, телевизионного вещания и радиовещания (п. 5.1.1.1) и защиты детей от информации, причиняющей вред их здоровью и (или) развитию (п. 5.1.1.6). При выявлении правонарушений Роскомнадзор уполномочен принимать меры реагирования, предусмотренные законодательством, включая возбуждение, производство и рассмотрение дел об административных правонарушениях.

Роскомнадзор выполняет и иные значимые функции по обеспечению ИПБ. Во-первых, служба обеспечивает создание, формирование и ведение Реестра запрещенной информации (п. 5.1.7). Его правовой режим функционирования определен постановлением Правительства РФ № 1101. Также служба реализует меры по ограничению доступа к интернет-ресурсам (п. 5.1.7(1)).

В сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, Роскомнадзор реализует следующие полномочия:

1) регламентирует порядок аккредитации экспертов и экспертных организаций, выполняющих экспертизу информационной продукции (п. 5.2(1).7);

2) ведет реестр экспертов и экспертных организаций и осуществляет контроль за их деятельностью (п. 5.2.6);

---

[654] План мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 годы.

[655] Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (утв. постановлением Правительства РФ от 16 марта 2009 г. № 228) // СЗ РФ. 2009. № 12. Ст. 1431.

3) организует проведение экспертизы информационной продукции в целях обеспечения информационной безопасности детей (п. 5.3.7).

Таким образом, Роскомнадзор в настоящее время выступает наиболее значимым несиловым органом обеспечения ИПБ, выполняющим контрольно-надзорные и иные функции в сфере СМИ и массовых коммуникаций, защиты детей от негативной информации. Особо стоит отметить выполнение службой важнейшей функции ограничения доступа к информационным ресурсам в сети Интернет.

Наряду с рассмотренными федеральными органами исполнительной власти важную роль в институциональной подсистеме обеспечения ИПБ играют и иные ФОИВ, такие как Министерство юстиции РФ, Министерство просвещения РФ, Министерство науки и высшего образования РФ, Министерство культуры РФ, Министерство здравоохранения РФ, Федеральная служба по надзору в сфере образования и науки, Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека. Однако объемы параграфа не позволяют отдельно рассмотреть их полномочия.

Проанализировав институциональную подсистему обеспечения ИПБ, мы увидели большое количество ФОИВ, выполняющих отдельные задачи в рассматриваемой области в соответствии со своим профилем деятельности (оборона, государственная безопасность, массовые коммуникации и СМИ и т. д.). Среди экспертов иногда возникает дискуссия относительно необходимости создания специализированного органа по обеспечению информационной безопасности. На наш взгляд, на текущем этапе развития российской государственности целесообразности в этом нет, поскольку сфера информационной безопасности, в которую входит ИПБ, чрезвычайно обширна и включает множество направлений, которые весьма затруднительно объединить в целостный функционал одного государственного органа.

Нами предлагается другой путь совершенствования институциональной подсистемы обеспечения ИПБ – *создание государственной системы реагирования на информационно-психологические угрозы*. Такая система должна быть создана по образцу государственной системы обнаружения, предупреждения и ликвидации компьютерных атак[656] (ГосСОПКА). Предлагаемая нами система (условное название – система «ПСИ-РАДАР») должна сформировать сеть территориально распределенных центров выявления и реагирования на информационно-психологические угрозы, объединяющих государственные органы федерального и регионального уровней, органы местного самоуправления, заинтересованные

[656] Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (выписка) // СЗ РФ. 2013. № 3. Ст. 178.

общественные объединения, иные НКО, СМИ и другие институты гражданского общества (в частности, кибердружины). В рамках данной системы необходима координация работы по линии информационного противоборства.

В качестве профильного федерального ведомства, ответственного за организацию работы системы «ПСИ-РАДАР», мы предлагаем определить Роскомнадзор. А уже внутри системы выделить четыре основных сектора угроз: внутренние (МВД России), внешние (ФСБ России), военные (Минобороны России) и международные (МИД России).

Второе наше предложение касается укрепления потенциала одного из ключевых органов обеспечения ИПБ – МВД России. Мы полагаем целесообразным *создание в структуре министерства подразделения по противодействию новым информационным угрозам.* Необходимость его учреждения обуславливается широким распространением в России новых деструктивных молодежных субкультур: «Колумбайна», «АУЕ», «МКУ», иных агрессивных, девиантных, радикальных и депрессивных сообществ.[657] Опыт научно-исследовательской и практической работы автора во ВНИИ МВД России и центральном аппарате МВД России показал, что данная линия не закреплена в полном объеме ни за одним подразделением министерства. Учитывая нетрадиционный характер угроз, компетенция нового подразделения должна носить гибридный характер, сочетающий оперативно-разыскные, профилактические и информационные формы деятельности. При этом акцент должен быть сделан именно на мониторинге, профилактике и контрпропаганде в цифровой среде.

Помимо органов публичной власти важные задачи в сфере обеспечения ИПБ выполняют институты гражданского общества и иные структуры, входящие в негосударственную подсистему обеспечения безопасности. Доктрина ИБ 2016 называет таких субъектов «участниками системы обеспечения информационной безопасности» и относит к ним организации ИТ-отрасли, СМИ, образовательные организации, общественные объединения, а также граждан (п. 33).

Применительно к сфере ИПБ роль негосударственной подсистемы исключительно важна. В первую очередь это обусловлено потребностью задействовать мощнейший потенциал общественных институтов в интересах обеспечения безопасности. Кроме того, в сфере массовой коммуникации основная часть СМИ, интернет-ресурсов и интернет-посредников находится в частной собственности, а потому без их участия невозможно эффективно противодействовать информационным рискам.

[657] *Чернова И. Г., Нечаева Ю. Б., Бабина Е. В.* Дети в сети: методическая памятка для переживающих взрослых. Экспертный КИБЕРсовет Ресурсного центра профилактики деструктивного влияния информации на несовершеннолетних в Пермском крае. Пермь, 2019.

К основным негосударственным участникам системы обеспечения ИПБ автор относит: 1) средства массовой информации; 2) владельцев (администраторов) интернет-сайтов, аудиовизуальных сервисов и социальных сетей; 3) создателей контента, включая блогеров; 4) информационных посредников; 5) производителей средств обеспечения информационной безопасности; 6) общественные и религиозные объединения, иные некоммерческие организации; 7) образовательные и научно-исследовательские учреждения (организации).

Среди перечисленных негосударственных участников особо выделим специализированные объединения и НКО в сфере обеспечения ИПБ. К их числу относятся центры безопасного Интернета (Центр безопасного Интернета в России,[658] Лига безопасного Интернета,[659] Центр изучения и сетевого мониторинга молодежной среды[660]), исследовательские и просветительские институты (Фонд Развития Интернет,[661] Институт развития Интернета[662]), центры психологического консультирования (Линия помощи «Дети онлайн»,[663] региональные центры психологической помощи населению). Указанные институты осуществляют выявление угроз ИПБ посредством самостоятельного мониторинга и приема обращений, информирования о них правоохранительных органов и компаний IT-сферы, оказания психологической помощи пострадавшим, реализации образовательных и просветительских проектов в данной области.

Одной из устоявшихся форм общественного участия в обеспечении информационной безопасности в нашей стране выступают *кибердружины*. Как правило, они представляют собой организованные на местах на общественных началах коллективы инициативных граждан, осуществляющих мониторинг сети Интернет в целях выявления противоправного контента и передачи сведений о нем в правоохранительные органы. Также они занимаются исследовательской и просветительской работой. Подобные кибердружины функционируют во многих субъектах РФ. В 2018 г. была предпринята попытка легализовать их правовой статус путем принятия специального федерального закона.[664] В ходе состоявшегося в Общественной палате РФ так называемого нулевого чтения

[658] Центр безопасного интернета в России. URL: https://www.saferunet.ru/ (дата обращения: 24.05.2021).

[659] Лига безопасного интернета. URL: http://ligainternet.ru/ (дата обращения: 24.05.2021).

[660] Центр изучения и сетевого мониторинга молодежной среды. URL: https://www.cism-ms.ru/ (дата обращения: 24.05.2021).

[661] Фонд Развития Интернет. URL: http://www.fid.su/ (дата обращения: 24.05.2021).

[662] Институт развития Интернета. URL: https://ири.рф/ (дата обращения: 24.05.2021).

[663] Линия помощи «Дети онлайн». URL: http://detionline.com/ (дата обращения: 24.05.2021).

[664] В Госдуме подготовили законопроект о кибердружинах // РИА Новости. 02.11.2018. URL: https://ria.ru/20181102/1531986218.html (дата обращения: 20.02.2021).

законопроекта он был подвергнут весьма острой критике.[665] Видимо, это предрешило судьбу данной законодательной инициативы, которая была «отложена в стол». Однако сама потребность принятия такого закона не отпала, поскольку он подведет определенную правовую базу под важное направление общественной активности и упорядочит его, в том числе в целях исключения злоупотреблений со стороны кибердружинников.

Кибердружины чаще всего функционируют на региональном или местном уровне. В этой связи, на наш взгляд, требуется определение какой-то координирующей их работу структуры федерального уровня. Помимо координации такая структура могла бы оказывать методическую помощь кибердружинам, а также обеспечивать взаимодействие с центральными аппаратами правоохранительных ведомств в случае, когда полученные одной или несколькими кибердружинами данные требуют участия федерального ведомства.

Представляется, что такой федеральной координационной структурой для кибердружин могла бы стать автономная некоммерческая организация «Центр изучения и сетевого мониторинга молодежной среды» (далее – ЦИСМ, Центр), учрежденная по поручению президента России в октябре 2018 г. Центр был создан в целях выработки системы по защите молодого поколения, детей и подростков от воздействия негативной информации. ЦИСМ выявляет контент, связанный с суицидальными проявлениями, кибербуллингом, криминальной субкультурой и другими деструктивными тенденциями в молодежной среде.[666]

ЦИСМ наряду с Росмолодежью, Роскомнадзором и МВД России определен в качестве исполнителя мероприятия по мониторингу Интернета в целях выявления деструктивных сообществ, субкультур и негативного контента, предусмотренного п. 25 Плана мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 годы.

По имеющейся информации, в настоящее время Центр функционирует как самостоятельная мониторинговая и информационно-просветительская структура. Закрепление за ним задачи координации деятельности территориальных кибердружин может быть полезным обеим сторонам. Для ЦИСМ это значительно расширило бы объем получаемой информации о противоправном контенте, а кибердружинам дало бы возможность методической и организационной поддержки со стороны структуры федерального уровня.

В качестве альтернативных вариантов в качестве федерального общественного координатора деятельности кибердружин можно было

[665] «Нам надо, чтобы дружинники не гоняли стиляг». В Общественной палате прошло нулевое чтение закона о кибердружинах // Коммерсант. 05.03.2019. URL: https://www.kommersant.ru/doc/3903344 (дата обращения: 02.04.2019).

[666] Об организации // Центр изучения и сетевого мониторинга молодежной среды. URL: https://www.cism-ms.ru/ob-organizatsii/ (дата обращения: 08.07.2021).

также рассмотреть Центр безопасного Интернета или Лигу безопасного Интернета. В организационно-правовом плане решение о закреплении такого статуса не может быть осуществлено директивным путем, поскольку речь идет о независимых общественных объединениях. Более целесообразно учреждение некоего альянса кибердружин во главе с центральной координирующей организацией, вступление в который будет сугубо добровольным.

§ 2. Приоритетные направления совершенствования законодательства Российской Федерации в сфере обеспечения информационно-психологической безопасности

Проведенный анализ действующего законодательства России показал наличие достаточно развитой системы правового обеспечения ИПБ. Вместе с тем нами обнаружен ряд пробелов в правовом регулировании. Кроме того, в связи с чрезвычайно высокой динамикой развития информационной сферы в условиях цифровой трансформации необходимо «заглядывать за горизонт» и вырабатывать правовые решения, позволяющие успешно подготовиться к появлению новых инфоугроз. Поэтому в настоящем параграфе мы сформулируем ряд авторских концептуальных предложений по совершенствованию системы правового обеспечения ИПБ.

Один из наиболее явных выявленных нами пробелов в действующем информационном законодательстве РФ состоит в том, что при наличии широкого перечня правовых механизмов обеспечения ИПБ в базовых источниках информационного права отсутствуют основополагающие положения и отправные начала информационно-психологической безопасности. При этом для другого ключевого элемента информационной безопасности – защиты информации – такие основополагающие нормы закреплены в Законе об информации. Статья 16 данного закона закрепляет правовую дефиницию защиты информации, определяет методы и содержание государственного регулирования отношений в данной сфере, а также устанавливает ряд правовых обязанностей и требований по защите информации.

Справедливости ради надо отметить, что базовых отправных норм нет в Законе об информации и для информационной безопасности в целом. Причина этого очевидна – название данного закона совершенно неадекватно отражает его современный предмет регулирования, поскольку блок информационной безопасности выходит далеко за рамки защиты информации.

В Модельном законе СНГ «Об информации, информатизации и обеспечении информационной безопасности» 2014 г. (далее – модельный

закон об информации), разработанном с участием видных российских ученых (И. Л. Бачило, М. А. Вуса и др.), данный недостаток был устранен. В этом законе имеется отдельная глава 4 «Основы правового регулирования обеспечения информационной безопасности и ответственности за правонарушения в сфере информатизации». Уже не в первый раз мы сталкиваемся с ситуацией, когда передовые отечественные разработки в сфере правового регулирования получают поддержку на уровне модельного законодательства СНГ, но не находят воплощения в российском законодательстве.

Нами обосновывается предложение *о дополнении Модельного информационного кодекса для государств – участников СНГ*[667] *положениями об основах правового обеспечения информационно-психологической безопасности*. В данном модельном акте имеется глава 4, закрепляющая нормы о противодействии обороту негативной информации. Однако положения этой главы закрепляют весьма ограниченный набор правовых средств обеспечения ИПБ и к тому же ограничиваются вопросами защиты от контентных угроз. Поэтому закрепление предшествующего блока норм о понятии, правовых принципах и средствах обеспечения ИПБ представляется нам весьма важным.

Придание информационной безопасности статуса стратегического национального приоритета в Стратегии НБ 2021 требует изменения сложившейся ситуации и полноценной правовой регламентации основ обеспечения информационной безопасности на уровне федерального закона. Наиболее перспективной нам представляется идея кодификации информационного законодательства и выделения в структуре будущего Информационного кодекса отдельного раздела по информационной безопасности. В 2014 г. авторским коллективом Института государства и права РАН под руководством И. Л. Бачило была подготовлена концепция Информационного кодекса Российской Федерации. На состоявшейся в том же году конференции в ИГП РАН разработанная концепция была поддержана большинством авторитетных российских экспертов по информационному праву.[668] Однако, к сожалению, такой поддержки на государственном уровне идея кодификации пока не получила, в связи с чем ее перспективы остаются весьма туманными.

В этой связи на современном этапе мы считаем архиважной реализацию предложения А. А. Чеботаревой об изменении названия Закона об информации и дополнении его содержания базовыми нормами об обеспечении информационной безопасности. *Наше авторское предложение заключается во внесении в данный закон отдельной статьи, касающейся*

[667] Модельный информационный кодекс для государств – участников СНГ (принят постановлением МПА СНГ от 23 ноября 2012 г. № 33–15) // Информационный бюллетень МПА СНГ. 2013. № 57 (часть 1). С. 44–73.

[668] См.: Систематизация и кодификация информационного законодательства: сб. науч. работ / Отв. ред. И. Л. Бачило. М.: ИГП РАН, Изд-во «Канон+», 2015.

обеспечения ИПБ. Такое решение обеспечит построение логичной и целостной системы правового регулирования информационной безопасности, включающей сначала базовые отправные начала ее обеспечения, а затем правовые нормы, касающиеся двух фундаментальных направлений ее обеспечения – защиты информации и информационно-психологической безопасности.

Автором разработан проект федерального закона о внесении изменений в Закон об информации (приложение № 2), нормативно воплощающий предложение автора. При его разработке за основу нами взяты нормы модельного закона об информации, а также российских законов о разных видах безопасности.

На конференциях автору часто задавали вопрос о необходимости разработки отдельного федерального закона об ИПБ. Как отмечалось выше, в конце 1990-х гг. такой законопроект разрабатывался группой ученых и депутатов Государственной Думы, однако так и не был принят парламентом. Проведенный нами анализ положений данного законопроекта показал, что он преимущественно регламентирует цели, задачи, принципы и направления обеспечения ИПБ, организацию государственной системы обеспечения ИПБ и международного сотрудничества в данной области. Это вполне отвечает его названию. Однако, на наш взгляд, такой широкий круг вопросов обеспечения ИПБ целесообразно нормативно закрепить в документе стратегического планирования. Авторский проект такого документа – *Концепции информационно-психологической безопасности в Российской Федерации* – представлен в приложении № 1. Данный документ обобщает итоги научной разработки темы информационно-психологической безопасности и описывает целостную модель ее обеспечения. Механизм ее практического использования может быть различным – как использование в качестве основы для разработки официального документа стратегического планирования с таким названием, так и применение при обновлении Доктрины информационной безопасности РФ. Каждое из решений имеет свои достоинства и недостатки. Например, основным аргументом в пользу единого документа выступает тесная взаимосвязь информационно-психологических и информационно-технических угроз, равно как и деятельности государственных органов по противодействию им.

Что касается законодательства в сфере обеспечения ИПБ, то *оптимальной стратегией его развития нам видится закрепление правовых начал обеспечения ИПБ в модифицированном базовом Законе об информации (в перспективе – Информационном кодексе РФ) на основе разработанного законопроекта в сочетании с регламентацией отдельных направлений и аспектов обеспечения ИПБ в самостоятельных законодательных актах.*

Следующее наше предложение касается насущной и весьма острой социальной проблемы – *деструктивных молодежных субкультур*. К ним

относятся субкультуры «АУЕ»,[669] «Колумбайн» (скулшутинг),[670] суицидальные субкультуры («группы смерти»), «МКУ» и др. Опасность данных субкультур состоит не только в распространении ими негативного контента и опасных идей, а в прямом или косвенном подстрекательстве ими девиантного поведения, включая совершение преступлений и аутодеструктивных действий. Так, за последние пять лет в России произошел целый ряд громких групповых убийств в учебных заведениях Керчи, Казани, Перми и других городов, совершенных подростками под влиянием субкультуры «Колумбайн». Количество предотвращенных правоохранительными органами подобных нападений исчисляется десятками и сотнями.[671]

Проведенное специалистами компании «Крибрум» исследование Рунета в период 2018–2019 гг. показало, что негативному воздействию деструктивных субкультур подвергается около 7 млн российских подростков.[672] Виды деструктивных сообществ и численность их последователей представлены в таблице 6.

Таблица 6

Деструктивные движения в Рунете
(показатели и динамика за период с марта 2018 г. по март 2019 г.)

Тематика	Общее число	Число подростков
АУЕ, ультрадвижение	24 млн (+9 млн)	4 млн (+2 млн)
Наркотики	1,3 млн (+702 тыс.)	103 тыс. (+23 тыс.)
Школьные расстрелы, убийства и убийцы	470 тыс. (+125 тыс.)	112 тыс. (+20 тыс.)
Издевательства, травля	12 млн (–500 тыс.)	2,5 млн (=)
Суицидальные группы	350 тыс. (=)	133 тыс. (=)
Прочие деструктивные группы	876 тыс. (+560 тыс.)	275 тыс. (+210 тыс.)

(Источник: Касперская Н. Проблема деструктивных движений в Рунете, 2019)

Директор Лиги безопасного Интернета Е. Мизулина в ходе выступления на дискуссионной экспертной площадке в МГЮА 1 июля 2021 г. привела данные о том, что каждый второй ребенок в России подвергается деструктивному воздействию в социальных сетях. В период с 2018 по 2021 г. число детей и подростков, состоящих в деструктивных сообществах в Интернете, практически удвоилось (с 5 до 9,5 млн).

[669] Движение «АУЕ» в 2020 г. было признано Верховным Судом РФ экстремистской организацией.

[670] Международное молодежное движение «Колумбайн» в 2022 году признано Верховным Судом РФ террористической организацией.

[671] *Башурина Е.* Природа скулшутинга: почему происходят массовые расстрелы в школах и как их предотвратить // Forbes. 17 мая 2021 г. URL: https://www.forbes.ru/forbeslife/429493-priroda-skulshutinga-pochemu-proishodyat-massovye-rasstrely-v-shkolah-i-kak-ih (дата обращения: 12.11.2021).

[672] *Касперская Н.* Проблема деструктивных движений в Рунете. Доклад на форуме «Цифровая гигиена» 28 марта 2019 г. М., 2019. См. также: Методическое пособие по выявлению признаков риска поведения в социальных медиа. М.: Крибрум, 2019.

В качестве основных тенденций, продвигаемых среди детей и подростков в социальных медиа, ею были названы: социопатия, сатанизм и культы, наркомания, нацизм и национализм, массовые и серийные убийства, обесценивание собственной жизни и стремление к смерти, ритуальные убийства и самоубийства, насильственные видео и треш-стримы, шок-контент, призывы к участию в незаконных акциях и митингах, экстремизм и терроризм, ультрадвижение, кибербуллинг, пропаганда оружия, скулшутинг.[673]

Одной из значимых площадок продвижения деструктивных субкультур длительное время выступали имиджборды. Они представляют собой форумы, на которых текстовое сообщение может дополняться изображением.[674] Наиболее известным имиджбордом в России является «Двач» (2ch), русскоязычный аналог мирового имиджборда 4chan. С ростом популярности социальных сетей и мессенджеров имиджборды получили свое развитие в виде тематических пабликов. Наиболее популярными среди них являются: MDK, 4ch («Форч»), 2ch («Двач»), «Кб» и др. Каждый из них имеет сотни тысяч, а некоторые – миллионы подписчиков. Лидер среди упомянутых пабликов – MDK – стабильно фигурирует в числе наиболее популярных сообществ в сети «ВКонтакте»[675] и, согласно рейтингу «Медиалогии», входит в число наиболее влиятельных пабликов в Рунете.[676]

Проведенное специалистами компании «Крибрум» исследование по техническому заданию, подготовленному автором совместно А. Н. Курицыным, показало значительное присутствие в публикуемой имиджбордами информации большого перечня деструктивных идей и концептов, оказывающих негативное ИПВ на подростков, включая: расизм/национализм; интимные отношения с несовершеннолетними/педофилию; насилие; оскорбление чувств верующих; наркотики/алкоголь/табак; антисоциальные нормы поведения и т. п.[677]

---

[673] *Мизулина Е. М.* Мониторинг распространения деструктивного контента в интернет-среде. Доклад на дискуссионной экспертной площадке «Противодействие деструктивной пропаганде среди молодежи в интернет-среде» 1 июля 2021 г. М., Университет им. О. Е. Кутафина (МГЮА), 2021.

[674] Имиджборда // Словарь языка интернета.ru / Под ред. М. А. Кронгауза. М.: АСТ-ПРЕСС КНИГА, 2016. С. 190.

[675] По состоянию на март 2021 г. число его подписчиков составляет 11,6 млн.

[676] ТОП-20 пабликов ВКонтакте – январь 2021 // Медиалогия. URL: https://www.mlg.ru/ratings/socmedia/vk/8137/ © (дата обращения: 16.03.2021).

[677] Ретроспективный анализ социополитической активности имиджбордов 2ch, 4ch и MDK в открытых источниках социальных медиа. М.: Крибрум, 2017. В рамках исследования был осуществлен количественный и качественный анализ российских средств массовой информации и блогосферы за период с января 2016 г. по декабрь 2017 г. Инструментом сбора статей в СМИ и упоминаний в блогосфере стала система мониторинга Крибрум, которая при помощи языка запросов позволила получить массивы информации, посвященные проблеме распространения социологической активности имиджбордов 2ch, 4ch и MDK в открытых источниках социальных медиа.

Однако в последние годы для продвижения деструктивных субкультур в основном создаются и используются тематические паблики и сообщества, где степень радикальности и жесткости контента стремится к точке максимума. В 2020 г. общественное внимание привлекла новая форма распространения шокирующего контента – так называемые «треш-стримы», прямые видеотрансляции с элементами интерактивности, демонстрирующие треш-контент.[678] Законодатели оперативно откликнулись на новый вид интернет-угроз,[679] хотя, на наш взгляд, проблема интернет-ресурсов с мерзким, отвратительным и устрашающим контентом требует комплексного решения.

Однако вернемся к самим деструктивным субкультурам. Борьба с их распространением представляет большую сложность и требует применения комплексного подхода, включающего привлечение лиц к ответственности за пропаганду и распространение деструктивных субкультур, удаление и блокировку используемых для этого интернет-ресурсов, ведение разъяснительной и контрпропагандистской работы. Так, для противодействия суицидальным сообществам («группам смерти») УК РФ в 2017 г. был дополнен двумя новыми составами преступлений, установившими ответственность за склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110.1) и организацию деятельности, направленной на побуждение к совершению самоубийства (ст. 110.2). В том же году поправками в УК РФ закреплена ответственность за вовлечение несовершеннолетнего в совершение действий, представляющих опасность для его жизни (ст. 151.2). Закон об информации в 2018 г. был дополнен нормой, предусмотревшей включение в Реестр запрещенного контента информации, подстрекающей детей к совершению действий, опасных для их жизни и здоровья (пп. «ж» п. 1 ч. 5 ст. 15.1).

Еще одним мощным механизмом противодействия деструктивным молодежным субкультурам выступает использование инструментов, предусмотренных Федеральным законом «О противодействии экстремистской деятельности». Так, в 2020 г. Верховным Судом РФ международное общественное движение «Арестантское уголовное единство» (АУЕ) было признано экстремистской организацией. Как отмечено в пресс-релизе Генеральной прокуратуры РФ, «в судебном заседании установлено, что АУЕ является хорошо структурированной и управляемой организацией – молодежным движением экстремистской

Кроме того, в рамках исследования были использованы все источники информации, которые являются открытыми для пользователей русскоязычного сегмента Интернет.

[678] *Смирнова Е.* Треш-стрим как образ жизни // Эксперт. 14 декабря 2020 г. URL: https://expert.ru/expert/2020/51/tresh-strim-kak-obraz-zhizni/ (дата обращения: 16.02.2021).

[679] Совфед планирует законодательно запретить «треш-стримы» // РИА Новости. 16.12.2020. URL: https://ria.ru/20201216/internet-1589441976.html (дата обращения: 16.02.2021).

направленности. В рамках движения и в его интересах участниками АУЕ совершались экстремистские правонарушения, а также массовые беспорядки». В движение, по данным Генпрокуратуры, «активно вовлекались подростки и молодежь, чья психика наиболее подвержена деструктивному воздействию».[680] Такое решение сразу позволило правоохранительным органам задействовать целый арсенал правовых средств противодействия экстремизму для борьбы с распространением субкультуры АУЕ в информационном пространстве.

Однако такое решение не является универсальным. Дело в том, что и АУЕ выступало скорее как субкультурное образование, нежели полноценная организация. Но в возникшем на основе субкультуры движении все же присутствовали признаки организованности (создание молодежных банд в российских регионах). Другие опасные субкультуры, такие как «группы смерти» и «Колумбайн», принципиально не предполагают создания каких-либо организованных групп, поскольку направлены на стимулирование индивидуальной активности. Поэтому признание их экстремистскими или террористическими организациями представляет большую сложность.[681]

В этой связи нами *обосновывается предложение об учреждении в российском законодательстве правового 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. Возможны и другие варианты решения.

Реализацию данного предложения в ближайшее время мы считаем исключительно значимой, поскольку оно создает важный правовой инструмент противодействия деструктивным субкультурам в информационном пространстве и обусловленным ими актам насилия в реальной жизни.

Заключительное авторское предложение касается совершенствования законодательного регулирования перспективных источников угроз ИПБ, а именно систем виртуальной и дополненной реальности. Поясним, о чем идет речь.

Понятие виртуальной реальности очень часто используется в гуманитарных науках в контексте дискурса о цифровых технологиях. Однако вкладываемое в него содержание, в зависимости от контекста, заметно отличается. Нас интересует сугубо прикладное понимание «виртуальной

[680] *Гликин К.* Верховный Суд признал экстремистской организацией уголовную субкультуру АУЕ // Ведомости. 18 августа 2020 г. URL: https://www.vedomosti.ru/society/articles/2020/08/17/836930-ekstremistskoi-aue (дата обращения: 13.09.2021).

[681] Хотя в феврале 2022 года Верховный Суд РФ признал Международное молодежное движение «Колумбайн» террористической организацией.

реальности» (virtual reality, VR) как совокупности технических устройств и программного обеспечения, создающих для человека иллюзию присутствия в искусственном мире и в ряде случаев позволяющих манипулировать его объектами.[682] В настоящее время наиболее массовым видом систем виртуальной реальности являются шлемы виртуальной реальности.

В контексте проблематики ИПБ особую значимость представляет такое отличительное свойство VR-систем от телевизоров, консолей компьютерных игр и иных устройств отображения информации, как чрезвычайно высокая степень правдоподобности формируемого искусственного образа. Она достигается за счет одновременного задействования множества сенсорных каналов (зрительного, слухового, тактильного, вестибулярного и др.) и изоляции (экранирования) от внешней реальности. Следствием такой убедительности выступает высокая сила психологического воздействия VR-систем, значительно превосходящая традиционные источники угроз ИПБ. Показательно, что производители VR-устройств уже оговаривают в своих инструкциях возможные негативные последствия их использования.[683]

В более длительной перспективе (до конца текущего столетия) с развитием интерфейсов «мозг – компьютер» системы виртуальной реальности получат настолько мощное развитие, что станут новой средой человеческого существования.[684] Прообразами таких виртуальных миров выступают VR-проекты компании Linden Lab «Second life» и «Sansar».

Дополненная реальность (augmented reality, AR) представляет собой среду, в реальном времени дополняющую физический мир, каким мы его видим, цифровыми данными с помощью каких-либо устройств (планшетов, смартфонов или других) и программной части. В дополненной реальности виртуальные объекты проецируются на реальное окружение (этим она отличается от VR).[685] Среди известных устройств AR можно назвать очки Microsoft Hololens, в плане программного обеспечения – игру

---

[682] Технология виртуальной реальности VR // Увлекательная реальность. URL: https://funreality.ru/technology/virtual_reality/ (дата обращения: 11.12.2020).

[683] Так, к числу таких последствий в руководстве к шлему виртуальной реальности GEAR VR компании Samsung отмечены возможные соматические (судороги, потеря сознания, подергивания глаз или мышц и т. п.) и психические (измененное, размытое или двойное видение или другие визуальные аномалии, бред) отклонения. См.: Samsung опубликовала пугающий перечень рисков, связанных с Gear VR // Hi-News.ru. 11 декабря 2014 г. URL: http://hi-news.ru/gadgets/samsung-opublikovala-pugayushhij-perechen-riskov-svyazannyx-c-gear-vr.html (дата обращения: 12.12.2021).

[684] *Стерледева Т. Д.* Электронно-виртуальная реальность как новая ниша человеческого существования: философский прогноз // Вызовы современности и философия: материалы круглого стола, посвященного Дню философии ЮНЕСКО. Кыргызско-Российский Славянский университет / Под общ. ред. И. И. Ивановой. Бишкек, 2004. С. 164–172.

[685] AR – Дополненная Реальность // Хабр. 6 августа 2018 г. URL: https://habr.com/ru/post/419437/ (дата обращения: 23.02.2021).

Pokemon Go. В качестве примера применения AR-технологий также часто приводят систему целеуказания на современных истребителях. Технологии дополненной реальности находятся в начале пути своего развития, хотя уже существуют запущенные проекты развлекательной, образовательной и коммерческой направленности.

Автор долгое время не рассматривал AR в контексте проблематики ИПБ, поскольку в плане психологического воздействия они представляли собой устройства, обеспечивающие лишь новый формат визуализации контента – трехмерный с проекцией на окружающую действительность вместо традиционных мониторов. Однако наше мнение изменилось после просмотра серии «Игровой тест» (Playtest) научно-фантастического сериала «Черное зеркало» (Black Mirror). В сюжете показано тестирование на человеке игры продвинутой дополненной реальности, которая подключается через вживленный в голову микрочип и проецирует на реальность жуткие образы, синтезируемые на основе анализа индивидуальных страхов человека, причем эти образы пользователь не может самостоятельно выключить.

Полагаем появление таких AR-систем в будущем весьма возможным. Им будут свойственны: а) непосредственное вживление в организм человека; б) максимальная правдоподобность изображения с задействованием множества сенсорных систем; в) персонализация образов на основе анализа индивидуальной психики. Поэтому сила их ИПВ будет вполне сопоставима с перспективными VR-платформами.

Мощный стимул развитию систем виртуальной и дополнительной реальности придала инициатива развития так называемых *«метавселенных»*. Осенью 2021 г. руководитель компании Facebook Марк Цукерберг на онлайн-презентации Facebook Connect 2021 анонсировал проект «метавселенной» (metaverse).[686] Придуманный в научно-фантастическом романе Нила Стивенсона «Лавина» 1992 г., этот термин обозначает конвергенцию физической, виртуальной и дополненной реальности в общем онлайн-пространстве. По сути, речь идет о развитом виртуальном мире, в котором пользователи будут взаимодействовать между собой. Как выразился сам Цукерберг, в метавселенной вместо просмотра контента люди будут погружаться в него.[687] По его словам, метавселенная будет

[686] *Бабаева Р.* Meta-вселенная Facebook: главное из интервью Марка Цукерберга The Verge // РБК. Обновлено: 10.12.2021. URL: https://trends.rbc.ru/trends/industry/617fbbc79a79476037fa0591 (дата обращения: 06.01.2022); *Логинов Н.* Разбор Метавселенной: что это – неизбежное будущее цифровых технологий или пустая фантазия // TJ. 8 ноября 2021 г. URL: https://tjournal.ru/tech/466466-razbor-metavselennoy-chto-eto-neizbezhnoe-budushchee-cifrovyh-tehnologiy-ili-pustaya-fantaziya (дата обращения: 06.01.2022).

[687] *Newton C.* MARK IN THE METAVERSE. Facebook's CEO on why the social network is becoming 'a metaverse company' // The Verge. Jul 22, 2021. URL: https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview (дата обращения: 06.01.2022).

доступна на различных компьютерных платформах, включая VR и AR, а также на ПК, мобильных устройствах и игровых консолях. О серьезности намерений компании свидетельствует переименование Facebook в Meta, а также задействование для разработки метавселенной более 10 тыс. сотрудников.

О развитии своих метавселенных заявили также другие крупные IT-компании (Microsoft, Epic Games, SK Telecom). В этой связи возникает целый комплекс вопросов обеспечения безопасности пользователей таких виртуальных пространств.[688] Но в метавселенных могут проявляться и другие угрозы ИПБ контентного и коммуникационного характера.

Поскольку системы виртуальной и дополненной реальности уже существуют и им предстоит пройти бум развития в ближайшие десятилетия, возникает потребность в правовом регулировании отношений, связанных с использованием таких систем. В этой связи нами *обосновывается необходимость разработки и принятия федерального закона «О системах виртуальной и дополненной реальности»*. Предмет регулирования данного закона должен быть широким и охватывать базовые вопросы изготовления, оборота и применения таких систем.

Безопасность систем виртуальной и дополненной реальности, включая вопросы ИПБ, должна выступать важным элементом предмета данного закона и включать следующие аспекты: 1) безопасность устройств подключения VR/AR-систем к организму человека; 2) безопасность передвижения в пространстве при использовании VR/AR-устройств; 3) классификацию контента для VR/AR-систем; 4) возрастные, временные и иные ограничения на использование VR/AR-систем; 5) плановые и экстренные механизмы прекращения использования VR/AR-систем; 6) систему мониторинга активности пользователей VR/AR-систем; 7) механизмы направления и рассмотрения жалоб на действия пользователей VR/AR-систем; 8) механизмы блокировки пользователей VR/AR-систем.

Данные предложения представляют актуальность на ближайшую и среднесрочную перспективы. В более дальнем горизонте событий, по мере утверждения онтологического статуса виртуальных миров в качестве новой среды существования человечества, *возникнет потребность в создании полноценной системы правового регулирования жизни в виртуальных мирах (метавселенных)*. Речь идет даже

[688] В частности, в недавнем докладе подчеркивается важность регулирования «растущих взаимодействий и проецируемых реальностей, которые открывают новые возможности для манипуляций и дезинформации, создавая эхо-камеры, в которых человек будет запираться со своими единомышленниками и провоцировать появление новых типов угроз» // Каспарьянц Д. Метавселенная: возможности и риски новой реальности // Научно-технический центр ФГУП «ГРЧЦ». 29.12.2021. URL: https://rdc.grfc.ru/author/d-kasparyants/ (дата обращения: 30.12.2021).

не об отдельной отрасли права, а скорее о *создании второго межотраслевого контура правового регулирования в дополнение к существующему первому контуру для офлайн-реальности (действующей правовой системе РФ)*.

§ 3. Формирование культуры информационной безопасности

В условиях усиливающейся цифровой трансформации большое значение приобретают адаптация граждан к новым условиям жизни в цифровой среде, повышение осведомленности и обучение навыкам противостояния информационным угрозам и рискам.

Ранее нами была представлена авторская концептуальная модель обеспечения ИПБ, включающая четыре направления. Среди них выделяются два основных: противодействие угрозам ИПБ и повышение жизнестойкости объектов ИПБ. В настоящее время основное внимание в государственной политике придается именно борьбе с угрозами ИПБ. Это во многом правильно, поскольку задача государства состоит в том, чтобы максимально оградить личность и социум от деструктивного влияния информационных рисков.

Однако к настоящему времени в экспертном сообществе сложилось понимание того, что информационную среду нельзя сделать абсолютно стерильной и исключить любые угрозообразующие факторы. Это обусловлено многими причинами: сложностью выявления угроз ИПБ, латентным характером их действия, многочисленностью источников угроз ИПБ, ограниченной эффективностью методов пресечения распространения деструктивной информации и т. д.

Кроме того, нельзя забывать о том, что в правовом демократическом государстве степень его вмешательства в общественную жизнь, в том числе в духовную сферу, должна быть строго лимитированной. Попытки государственного директивного навязывания взглядов и ценностей, пресечения любого инакомыслия несовместимы с принципами демократического устройства. Эти идеи нашли свое отражение в Конституции Российской Федерации, закрепляющей принципы идеологического и политического плюрализма (ст. 13), свободу мысли, слова и информации, гарантированность свободы массовой информации (ст. 29) и допускающей строго лимитированное ограничение прав и свобод (ст. 55).

В связи с этим требуется усиление другого магистрального направления обеспечения ИПБ – повышения жизнестойкости объектов ИПБ, их способности самостоятельно блокировать или снижать до приемлемых значений деструктивное влияние угроз ИПБ. Данную задачу можно обозначить как *формирование информационного иммунитета личности и общества.* В правовых актах и научной литературе данное направление обеспечения безопасности обычно обозначается как формирование

информационной грамотности и цифровой компетентности, культуры информационной безопасности. Г. Г. Шинкарецкая и А. М. Берман обоснованно рассматривают проведение политики государства по повышению цифровой и информационной грамотности населения в качестве важного инструмента формирования доверия общества к цифровым технологиям.[689]

Соответствующие положения закреплены в российских документах стратегического планирования. В Доктрине ИБ 2016 обозначена задача «формирования культуры личной информационной безопасности» (пп. «д» п. 27). Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (далее – Стратегия РИО) закрепляет, что для создания информационного пространства знаний необходимо развитие правосознания граждан и ответственное использование ими ИКТ (пп. «н» п. 26). В Концепции ИБ детей в качестве базовых принципов государственной политики в данной сфере названы: «необходимость формирования у детей умения ориентироваться в современной информационной среде», «воспитание у детей навыков самостоятельного и критического мышления» и «обучение детей медиаграмотности» (раздел II).

В 2002 г. Генеральная Ассамблея ООН впервые приняла резолюцию, посвященную созданию глобальной культуры кибербезопасности[690] (далее – резолюция 57/239). В преамбуле среди предпосылок ее принятия отмечается, что обеспечение кибербезопасности зависит не только от работы правоохранительных структур, но от превентивных мер, а также осведомленности и ответственности владельцев и пользователей ИКТ. Последние два аспекта закреплены в числе элементов глобальной культуры кибербезопасности в приложении к резолюции 57/239.

Проведенный нами анализ правовых актов ЕС в сфере обеспечения кибербезопасности, в частности программы ЕС «Безопасный Интернет», показал, что повышение осведомленности детей, родителей и педагогов о правилах безопасного использования сети выделялось в качестве одного из приоритетных направлений работы.[691]

Еще до активного развития Интернета в европейских и иных странах мира при активной поддержке ЮНЕСКО сформировалось специфическое направление «медиаобразование» (media education), призванное помочь школьникам и студентам лучше адаптироваться

---

[689] *Шинкарецкая Г. Г., Берман А. М.* Цифровизация и проблема обеспечения национальной безопасности // Образование и право. 2020. № 5. С. 258.

[690] Резолюция Генеральной ассамблеи ООН A/RES/57/239 от 20 декабря 2002 г. «Создание глобальной культуры кибербезопасности» // Организация Объединенных Наций. URL: https://undocs.org/ru/A/RES/57/239 (дата обращения: 12.02.2021).

[691] *Смирнов А. А.* Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского союза: монография. М.: ЮНИТИ-ДАНА, Закон и право, 2012. С. 91–97.

в мире медиакультуры и направленное на достижение медиаграмотности (media literacy).[692] *Медиаграмотность* определяется как «грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков».[693]

С появлением и ростом популярности Интернета исследователи стали говорить о *«цифровой грамотности»*, которую П. Гилстер определил как «способность критически понимать и использовать информацию, получаемую посредством компьютера в различных форматах из широкого диапазона источников».[694] А. Мартин выделил в качестве компетенций цифровой грамотности умения правильного использования цифровых средств для манипуляций с информационными ресурсами и общения с людьми в цифровой среде.[695]

Существенный рост возможностей Интернета и его плотное вхождение в повседневную жизнь человека привели исследователей к обращению к понятию *цифровой компетентности*, под которой понимается «способность индивида уверенно, эффективно, критично и безопасно выбирать и применять инфокоммуникационные технологии в разных сферах жизнедеятельности (информационная среда, коммуникации, потребление, техносфера), а также его готовность к такой деятельности».[696]

За последние десятилетия в нашей стране подготовлен комплекс добротных научных и методических трудов, посвященных формированию информационной (медийной, цифровой) грамотности и культуры информационной безопасности.[697] Особо отметим вклад в разработку данной проблематики руководителя Фонда Развития Интернет, профессора факультета психологии МГУ имени М. В. Ломоносова Г. У. Солдатовой и ее коллег, проведших целый ряд прикладных социологических исследований и разработавших собственную концепцию цифровой компетентности. В ней выделены четыре ее разновидности: информационная

---

[692] *Федоров А. В.* Медиаобразование и медиаграмотность. Таганрог: Изд-во Кучма, 2004. С. 10–11.

[693] *Пристанская О. В., Кочетова В. С.* Уроки медиабезопасности для школьников и родителей: методическое пособие для Уполномоченных по правам ребенка. М.: ФОРМАТ, 2011. С. 4.

[694] *Солдатова Г. У., Рассказова Е. И., Нестик Т. А.* Цифровое поколение России: компетентность и безопасность. 2-е изд., стер. М.: Смысл, 2018. С. 150.

[695] Там же.

[696] Там же. С. 152.

[697] *Федоров А. В.* Медиаобразование и медиаграмотность. Таганрог: Изд-во Кучма, 2004; Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г. У. Солдатова, Т. А. Нестик, Е. И. Рассказова, Е. Ю. Зотова. М.: Фонд Развития Интернет, 2013; *Солдатова Г. У., Рассказова Е. И., Нестик Т. А.* Цифровое поколение России: компетентность и безопасность. 2-е изд., стер. М.: Смысл, 2018; *Малюк А. А.* Глобальная культура кибербезопасности. М.: Горячая линия – Телеком, 2018.

и медиакомпетентность, коммуникативная, техническая и потребительская компетентность.[698]

Еще одним продуктивным методологическим подходом к формированию культуры информационной безопасности выступает концепция *цифровой (кибер-) гигиены*, развиваемая рядом исследователей. Как отмечается на тематическом ресурсе «Лаборатории Касперского», «кибергигиена – это формирование полезных привычек в отношении кибербезопасности, позволяющих не стать жертвой киберугроз и избегать проблем сетевой безопасности».[699] Эксперты компании изложили чек-лист правил кибергигиены, включающий безопасное хранение паролей, использование многофакторной аутентификации и т. д.[700] Однако он направлен в большей мере на обеспечение защиты информации, что объяснимо профилем самой компании.

Для ИПБ большее значение имеют правила цифровой гигиены, изложенные видными российскими экспертами И. Ашмановым и Н. Касперской: 1) не выдавать личной информации; 2) не делать того, за что будет стыдно потом; 3) не брать смартфон в секретные поездки или походы; 4) не верить и не доверять незнакомцам; 5) не выкладывать ничего важного и секретного в облако.[701] Также ими сформулирован свод общих принципов цифровой гигиены: 1) быть внимательным и осознанным; 2) помнить и заботиться о своем будущем; 3) распознавать манипуляцию и манипуляторов; 4) соблюдать разумную умеренность и воздержание; 5) быть источником знаний; 6) соблюдать личную цифровую гигиену.[702]

Анализируя связь цифровой компетентности и столкновения с онлайн-рисками, исследователи пришли к выводу о наличии прямой корреляции между ними: чем чаще подростки соприкасались с онлайн-рисками, тем выше у них был уровень цифровой компетентности.[703] Однако такой способ формирования цифровой компетентности путем «наступания на грабли» является опасным, поскольку может повлечь неприемлемый ущерб. Поэтому *главная задача состоит в обучении детей, родителей, учителей и иных категорий граждан навыкам и умениям, составляющим содержание цифровой грамотности (компетентности)*.

В этом направлении в России за последнее десятилетие проделана очень большая работа. Проводятся замеры уровня цифровой

---

[698] *Солдатова Г. У., Рассказова Е. И., Нестик Т. А.* Цифровое поколение России: компетентность и безопасность. 2-е изд., стер. М.: Смысл, 2018. С. 153.

[699] Соблюдение кибергигиены поможет обеспечить безопасность в сети // Лаборатория Касперского. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-hygiene-habits (дата обращения: 12.01.2022).

[700] Там же.

[701] *Ашманов И., Касперская Н.* Цифровая гигиена. СПб.: Питер, 2022. С. 120–121.

[702] Там же. С. 369–372.

[703] *Солдатова Г. У., Рассказова Е. И., Нестик Т. А.* Цифровое поколение России: компетентность и безопасность. 2-е изд., стер. М.: Смысл, 2018. С. 156.

грамотности,[704] запущен портал цифровой грамотности,[705] в образовательных учреждениях проводятся уроки кибербезопасности.[706] Исключительно важной мерой является введение тематических занятий по информационной безопасности в состав школьного курса ОБЖ. Об этом не одно десятилетие говорили ведущие российские эксперты в данной области. Отрадно отметить, что в 2020 г. был издан учебник по предмету ОБЖ, в котором нашли отражение темы информационной и психологической безопасности.[707]

Проведенное аналитическим центром НАФИ исследование показало, что по итогам 2021 г. уровень цифровых компетенций россиян вырос: сократилась доля граждан с начальным уровнем цифровой грамотности, выросла доля россиян с базовым уровнем. Однако доля тех, кто обладает продвинутым уровнем цифровых компетенций, остается неизменной с 2019 г. и составляет 27%. Многие россияне по-прежнему обладают недостаточными знаниями и навыками в сфере цифровых технологий. Индекс цифровой грамотности населения РФ в первой половине 2021 г. составил 64 пункта по шкале от 0 до 100. Он оценивается по пяти параметрам, включая цифровую безопасность. По данному параметру подиндекс составил 65 пунктов.[708]

Важным направлением работы по формированию культуры информационной безопасности выступает *стимулирование проектов повышения медийной и цифровой грамотности граждан*. Работа в этой области давно ведется различными общественными и иными некоммерческими организациями общероссийского, регионального и местного уровней, причем нередко по собственной инициативе. Среди крупных организаций, реализующих информационно-просветительские и образовательные проекты в изучаемой области, можно назвать Региональный общественный центр интернет-технологий (РОЦИТ), Фонд Развития Интернет, Координационный центр доменов.RU/.РФ, Лигу безопасного Интернета, Центр безопасного Интернета в России, Российскую государственную детскую библиотеку и другие структуры. В 2019 г. был запущен тематический интернет-портал «Цифровая грамотность».[709] В субъектах

[704] Например, РОЦИТ при поддержке исследовательской группы «ЦИРКОН» в период 2015–2018 гг. ежегодно проводилось исследование индекса цифровой грамотности граждан РФ. В последующие годы он измерялся в рамках проведения «цифрового диктанта».

[705] Цифровая грамотность. URL: https://цифроваяграмотность.рф.

[706] Единый урок безопасности // Дети в информационном обществе. № 26. Специальный выпуск.

[707] В курс ОБЖ для школьников включена тема информационной безопасности // ТАСС. 5 мая 2020. URL: https://tass.ru/obschestvo/8399641 (дата обращения: 12.12.2021).

[708] Вынужденная цифровизация: исследование цифровой грамотности россиян в 2021 году. Аналитический центр НАФИ. 2021.

[709] URL: https://цифроваяграмотность.рф.

РФ также действуют многочисленные проекты повышения медийной и цифровой грамотности.

Требуется дальнейшее усиление государственной поддержки данного направления общественной активности. Четкое понимание этого имеется на уровне политического руководства России. Заместитель председателя Правительства РФ Д. Чернышенко в ноябре 2021 г. заявил, что «личная цифровая грамотность становится важным условием работы в онлайн-среде».[710] Он отметил угрозы для пользователей от посещения опасных ресурсов и столкновения с мошенниками в цифровом пространстве. Характеризуя меры государственной поддержки, Чернышенко отметил, что в рамках нацпрограммы «Цифровая экономика» уже реализуется несколько проектов по ИТ-образованию и повышению уровня цифровых компетенций. В дополнении к этому Минцифры России разрабатывает проект правил предоставления субсидии на разработку и реализацию программы повышения цифровой грамотности широких слоев населения. По словам Д. Чернышенко, на реализацию просветительских мероприятий в 2022 г. государство выделит 200 млн рублей, всего же до 2024 г. на эти цели будет направлено 600 млн рублей.[711]

Помимо мероприятий программы «Цифровая экономика» комплекс мер по повышению цифровой грамотности и формированию культуры информационной безопасности закреплен в Плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 гг. Среди них заявлены:

а) проведение Единого урока безопасности в сети Интернет;

б) проведение цикла мероприятий для обучающихся, их родителей и работников образовательных организаций «Сетевичок»;

в) организация повышения компетенции родителей (законных представителей) и работников организаций детства в области цифровой грамотности и информационной безопасности на портале «Учеба. онлайн»;

г) разработка и актуализация образовательного контента в рамках проекта «Российская электронная школа», направленного на повышение уровня осведомленности обучающихся в части интернет-безопасности, и др.

Все эти мероприятия могут быть успешно реализованы только на основе частно-государственного партнерства, с привлечением широкого круга общественных объединений и иных НКО.

Помимо обучения (образования) как основной формы повышения уровня цифровой грамотности и культуры информационной безопасности

[710] Дмитрий Чернышенко: Личная цифровая грамотность – важное условие работы в онлайн-среде // Правительство РФ. 15 ноября 2021 г. URL: http://government.ru/news/43803/ (дата обращения: 07.01.2022).

[711] Там же.

важное значение также имеет *информационно-просветительская работа*. Она направлена на развитие критического мышления, повышение осведомленности об угрозах ИПБ (ложных новостях, манипуляции сознанием, мошенничестве и др.) и правилах реагирования на них. Формами ведения информационно-просветительской работы выступают создание и распространение тематических информационных материалов (плакатов, памяток, роликов), интернет-ресурсов, проведение обучающих занятий и иных профилактических мероприятий.

Запрос на получение знаний о правилах обеспечения безопасности в цифровой среде имеется в обществе. Недавнее исследование аналитического центра НАФИ показало, что россияне все сильнее беспокоятся за собственную цифровую безопасность. Более половины опрошенных (57%) хотели бы узнать о том, как лучше защититься от цифровых угроз, а также развить навыки безопасного использования цифровых устройств и технологий. При этом 73% россиян, которые хотели бы больше узнать об инструментах личной цифровой безопасности, испытывают информационный дефицит.[712] Поэтому требуется дальнейшая активизация информационно-просветительской работы институтов гражданского общества в рассматриваемой сфере при широкой государственной поддержке.

[712] Россиянам не хватает информации по защите от киберугроз // Аналитический центр НАФИ. 2 декабря 2021 г. URL: https://nafi.ru/analytics/rossiyanam-ne-khvataet-informatsii-po-zashchite-ot-kiberugroz/ (дата обращения: 03.01.2022).

ЗАКЛЮЧЕНИЕ

Проведенный нами анализ показал, что в современных условиях информационно-психологическая безопасность должна рассматриваться как неотъемлемая часть информационной безопасности, охватывающая вопросы защиты личности и общества от деструктивного информационно-психологического воздействия. Имея древний генезис и длительную историю эволюции, она на непродолжительный период ушла в тень на фоне новых информационно-технологических вызовов эпохи информационной революции.

Однако вследствие бурного развития телевидения, а затем и новых медиа проблема распространения негативной информации и вредоносной коммуникации обрела новую остроту. Основным драйвером роста информационно-психологических угроз стали, на наш взгляд, социальные сети, впервые в истории наделившие отдельно взятого человека возможностями массмедиа. Начавшееся взрывное увеличение количества источников трансляции информации на массовую аудиторию вкупе с широким вовлечением населения в социальные сети и фактором относительной анонимности Интернета коренным образом изменили медиасреду. Этим активно воспользовались многочисленные «инженеры человеческих душ», начиная от сотрудников иностранных спецслужб и террористов и заканчивая мошенниками и сектантами. Все они получили свободный выход на миллионные аудитории, причем невзирая на государственные границы.

Важную роль сыграло также накопление в течение XX в. в психологии и иных гуманитарных науках систематизированного научного знания и четких прикладных рекомендаций по методам оказания влияния на индивидуальное и общественное сознание, многократно апробированным в ходе военных, политических и маркетинговых кампаний. В последнее десятилетие бум интереса к научно-популярной литературе, посвященной манипуляции человеческим сознанием и поведением, наблюдается и среди широких масс населения. Проводятся многочисленные тренинги, мастер-классы и коучинги, где профессиональные и не очень тренеры обучают желающих технологиям оказания воздействия на людей и защите от них. Спрос на такой образовательный контент очень высок.

Еще одним значимым фактором стали технологии сбора и анализа информации о человеке в цифровой среде на основе больших данных и искусственного интеллекта. Оказалось, что, внимательно изучая оставляемый личностью цифровой след, возможно построить ее психологический портрет и подобрать нужные инструменты воздействия. В наибольшей мере такими технологическими возможностями обладают ведущие мировые IT-компании (Big Tech), однако методы анализа поведения человека в сети применяются широким кругом организаций государственного и частного секторов, и этот процесс только нарастает.

Указанные факторы вызвали колоссальный рост информационно-психологических угроз. В Интернете, социальных сетях и мессенджерах возник мощный поток негативного контента, для сдерживания которого государствам пришлось применять экстренные меры. Не меньшую опасность стали представлять и деструктивные формы коммуникации в цифровой среде, исходящие от вербовщиков, террористов, педофилов, агрессивных троллей и мошенников. В работе нами показана чрезвычайно широкая палитра контентных и коммуникационных угроз информационно-психологической безопасности, в основе которых лежат единые механизмы деструктивного информационно-психологического воздействия. Поэтому один из ключевых выводов исследования состоит в необходимости выстраивания комплексного механизма противодействия данным угрозам. Это, в свою очередь, не исключает потребности в задействовании специальных инструментов нейтрализации определенных вызовов, будь то фейки, буллинг или диффамация.

За прошедшие два десятилетия система правового обеспечения информационно-психологической безопасности в целом сформировалась на основе нескольких взаимосвязанных массивов информационного законодательства, касающихся защиты детей от информации, причиняющей вред их здоровью и развитию, ограничения доступа к противоправному контенту, предотвращения злоупотреблений свободой массовой информации и защиты потребителей рекламы. Очень важное значение имело правовое закрепление многочисленных составов преступлений и административных правонарушений в УК РФ и КоАП РФ.

Вместе с тем при высоком уровне нормативной регламентации отдельных групп общественных отношений в рамках общего предмета правового регулирования слаборазвитыми остаются общесистемные начала правового обеспечения информационно-психологической безопасности. Предложенные в настоящей работе поправки в базовый Федеральный закон «Об информации, информационных технологиях и о защите информации» могут послужить лишь первым шагом на пути устранения данного существенного пробела в праве. С учетом признания информационной безопасности стратегическим национальным приоритетом в Стратегии национальной безопасности Российской Федерации мы склонны поддержать мнение профессора Т. А. Поляковой относительно целесообразности разработки и принятия отдельного федерального закона «Об информационной безопасности Российской Федерации». В данном законодательном акте информационная безопасность должна наконец найти целостное воплощение, в котором блок защиты информации будет объединен с блоком информационно-психологической безопасности, как это сделано в модельном законе СНГ «Об информации, информатизации и обеспечении информационной безопасности».

Важным шагом видится нам воплощение в жизнь предложенного в работе проекта Концепции информационно-психологической безопасности.

Полагаем, что данный проект может быть реализован посредством принятия самостоятельного документа стратегического планирования либо включения в качестве составной части в обновленную Доктрину информационной безопасности Российской Федерации, разработка которой, по имеющейся информации, ведется в настоящее время. Убеждены, что, заложив на уровне документа стратегического планирования правильное концептуальное понимание информационно-психологической безопасности, можно создать надежную основу для совершенствования информационного и иного отраслевого законодательства Российской Федерации.

В работе мы попытались также заглянуть за горизонт, определив перспективные направления правового обеспечения информационно-психологической безопасности, связанные с системами виртуальной и дополненной реальности. Еще в монографии 2012 года мы писали о важности формирования перспективных механизмов обеспечения безопасности виртуальной жизнедеятельности человека в связи с развитием процессов виртуализации общества.[713] Хотя тема виртуальной реальности никак не является новой, в прошлом году она получила неожиданный мощный импульс развития со стороны ведущих ИТ-корпораций мира под новым брендом «метавселенных». Это вынуждает всерьез присмотреться к данной проблематике, поскольку сроки внедрения виртуальных миров в жизнь человечества существенно сокращаются. Уже до конца текущего десятилетия можно ожидать запуска нескольких крупных проектов метавселенных, а до конца столетия они, несомненно, получат широкое развитие и станут привычными нишами человеческого существования для миллионов людей по всему миру. В этой связи нами обосновано предложение о разработке и принятии федерального закона «О виртуальной и дополненной реальности».

Вместе с тем протекающие в настоящее время события заставляют нас всерьез обратиться к проблеме совершенствования системы информационного противоборства. Начав специальную военную операцию на территории Украины в феврале 2022 года, Россия вступила в ожесточенную информационную войну, где на стороне противника воюют силы коллективного Запада. Интенсивность применения против нашей страны средств деструктивного информационно-психологического воздействия носит беспрецедентный характер. Причем противоборствующая сторона не сдерживает себя никакими моральными ограничениями, что отчетливо показала чудовищная провокация в Буче в марте 2022 года. В этой связи требуется форсированное наращивание потенциала России в области информационного противоборства, прежде всего по линии пропаганды и контрпропаганды, с широким задействованием институтов гражданского общества.

[713] *Смирнов А. А.* Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского союза: монография. М.: ЮНИТИ: Закон и право, 2012. С. 141.

Приложение 1

Проект

Концепция информационно-психологической безопасности в Российской Федерации

I. Общие положения

1. Настоящая Концепция представляет собой систему взглядов на обеспечение информационно-психологической безопасности как части информационной и национальной безопасности Российской Федерации.

2. Настоящей Концепцией определяются основные угрозы информационно-психологической безопасности в Российской Федерации, цели, задачи, принципы и основные направления деятельности уполномоченных органов публичной власти, организаций и иных субъектов, принимающих участие в обеспечении информационно-психологической безопасности на основании законодательства Российской Федерации.

3. Правовую основу настоящей Концепции составляют Конституция Российской Федерации, Федеральный закон от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации», другие федеральные законы, Стратегия национальной безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации, Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, Основы государственной политики Российской Федерации в области международной информационной безопасности, Концепция информационной безопасности детей, другие документы стратегического планирования, иные нормативные правовые акты Российской Федерации, определяющие направления применения информационных и коммуникационных технологий в Российской Федерации.

4. Настоящая Концепция является основополагающим документом стратегического планирования, определяющим государственную политику в сфере обеспечения информационно-психологической безопасности, а также основой для конструктивного взаимодействия в этой сфере органов публичной власти и институтов гражданского общества, граждан Российской Федерации, иностранных граждан и лиц без гражданства.

5. Обеспечение информационной безопасности является одним из стратегических национальных приоритетов. Информационно-психологическая безопасность является составной частью системы информационной безопасности и представляет собой состояние защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.

6. Российская Федерация при обеспечении информационно-психологической безопасности на долгосрочную перспективу исходит

из необходимости постоянного совершенствования системы обеспечения информационно-психологической безопасности, а также политических, организационных, социально-экономических, информационных, правовых и иных мер:

а) по осуществлению мониторинга информационного пространства, выявлению, прогнозированию и оценке угроз информационно-психологической безопасности;

б) по реализации разработки и применению комплекса оперативных и долговременных мер по предупреждению и устранению угроз информационно-психологической безопасности, их локализации и нейтрализации последствий их проявления;

в) по созданию информационной среды доверия, повышению уровня цифровой грамотности и формированию культуры информационной безопасности;

г) по развитию частно-государственного партнерства и международного сотрудничества в области обеспечения информационно-психологической безопасности.

7. Для целей настоящей Концепции используются следующие основные понятия:

а) обеспечение информационно-психологической безопасности – деятельность по выработке и реализации системы правовых, организационных, информационных и иных мер, направленных на обеспечение защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия;

б) угроза информационно-психологической безопасности – фактор или совокупность факторов, способных причинить вред интересам личности, общества и государства посредством оказания деструктивного информационно-психологического воздействия;

в) деструктивное информационно-психологическое воздействие – негативное влияние на личность, социальные группы и общество деструктивной информации или коммуникации, а также сигналов от технических устройств, дистанционно воздействующих на психику человека через зрительные и слуховые сенсорные системы, создающее опасность причинения вреда интересам личности, общества и государства;

г) система обеспечения информационно-психологической безопасности – совокупность сил обеспечения информационно-психологической безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационно-психологической безопасности, а также правовых норм, регулирующих общественные отношения в сфере обеспечения информационно-психологической безопасности;

д) силы обеспечения информационно-психологической безопасности – государственные органы, а также подразделения и должностные

лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационно-психологической безопасности;

е) средства обеспечения информационной безопасности – правовые, организационные, технические и другие средства, используемые силами обеспечения информационно-психологической безопасности;

ж) правовое обеспечение информационно-психологической безопасности – деятельность по разработке и реализации системы правовых средств, направленных на обеспечение защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.

II. Основные угрозы информационно-психологической безопасности

8. Стремительное развитие информационно-коммуникационных технологий сопровождается ростом угроз безопасности, связанных с оказанием деструктивного информационно-психологического воздействия на личность, социальные группы и обществом в целом.

9. Расширяется использование информационно-коммуникационных технологий для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, что представляет угрозу международному миру и безопасности. Активизируется деятельность специальных служб иностранных государств по проведению информационно-психологических операций в российском информационном пространстве.

10. В целях дестабилизации общественно-политической ситуации в Российской Федерации распространяется недостоверная общественно значимая информация, в том числе заведомо ложные сообщения об угрозе совершения террористических актов. Применяется тактика массовой рассылки ложных сообщений о минировании образовательных организаций и иных мест массового пребывания граждан, реализуемая с использованием современных средств связи и телекоммуникационных сетей. Новый потенциал для дезинформации открывают технологии искусственного интеллекта, в частности позволяющие создавать высококачественные подделки изображения и голоса человека (deepfakes).

11. Российские средства массовой информации и журналисты подвергаются в ряде зарубежных стран неприкрытому политическому давлению и цензуре, что грубо противоречит международно-правовым стандартам свободы массовой информации и демократии. При этом в западных массмедиа развязана мощная скоординированная кампания очернения Российской Федерации, направленная на формирование негативного имиджа России в мире.

12. Доминирование транснациональных корпораций в интернет-секторе создает риски сбора большого массива персональных данных о российских пользователях и его применения для оказания таргетированного деструктивного информационно-психологического воздействия на отдельных людей и социальные группы. Используемые данными корпорациями подходы к модерации контента создают риски широкого распространения в сети Интернет противоправной информации, формирования искаженной картины событий, происходящих в России и в мире, навязывания негативных установок и ценностных ориентаций при одновременном блокировании возможности донесения альтернативных сведений. При этом ими систематически игнорируются законные требования российских властей об удалении или ограничении доступа к противоправному контенту, принятии иных мер по обеспечению информационно-психологической безопасности.

13. Традиционные российские духовно-нравственные и культурно-исторические ценности подвергаются активным нападкам со стороны западных государств и их союзников, транснациональных корпораций, иностранных некоммерческих неправительственных, религиозных, экстремистских и террористических организаций, а также поддерживающих их лиц и организаций внутри страны. При этом ими насаждаются социальные и моральные установки, противоречащие традициям, убеждениям и верованиям народов Российской Федерации.

14. Иностранными государствами и иными международными политическими акторами при поддержке и активном участии определенной внутренней прослойки населения проводится массированная кампания по фальсификации российской и мировой истории, искажению исторической правды и уничтожению исторической памяти, дискредитации российской культуры и русского языка, разжиганию межнациональных и межконфессиональных конфликтов, ослаблению государствообразующего народа.

15. Фактор анонимности в цифровой среде способствует широкому распространению негативного контента и ведению деструктивных коммуникаций, облегчает совершение преступлений и иных противоправных действий. В личностном плане ощущение анонимности обуславливает снятие ряда психологических барьеров в общении и поведении человека в информационном пространстве, что способствует проявлению им своих деструктивных наклонностей и интересов.

16. В сети Интернет размещаются материалы террористических и экстремистских организаций, призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершению самоубийства, осуществляется пропаганда криминального образа жизни, жестокости, насилия и иных антиобщественных действий,

потребления наркотических средств и психотропных веществ, размещается иная противоправная информация. Основными объектами такого деструктивного воздействия являются дети и молодежь.

17. Возрастают масштабы мошенничеств, краж и иных преступлений, совершаемых с использованием информационно-коммуникационных технологий и приемов социальной инженерии. При этом способы и средства совершения таких преступлений становятся все изощреннее.

18. Широкое распространение в цифровой среде получили деструктивные молодежные субкультуры, содержащие негативные идеи, ценностные и поведенческие установки и нормы. Их продвижение осуществляется через многочисленные сообщества и каналы в социальных сетях и мессенджерах, в том числе при содействии спецслужб иностранных государств. Особую опасность представляют деструктивные субкультуры, провоцирующие совершение массовых убийств и применение иных актов насилия, а также суицид и иные формы аутодеструктивного поведения подростков.

19. Негативное воздействие на психику оказывают различные виды речевой агрессии и иной деструктивной коммуникации в социальных сетях и мессенджерах, включая высмеивание (троллинг), травлю в сети (буллинг), доведение до самоубийства (буллицид) и др. Возможности Интернета также активно используются для склонения и иного вовлечения детей и молодежи в террористическую и экстремистскую деятельность, совершение преступлений, потребление и распространение наркотиков, иных антиобщественных действий или действий, представляющих опасность для жизни несовершеннолетнего.

20. Источником угроз информационно-психологической безопасности также выступают коммерческие компании, использующие сочетание продвинутых методов манипуляции сознанием потребителей и анализа их индивидуальной сетевой активности для агрессивного продвижения своих товаров и услуг.

21. Риски причинения вреда психическому и физическому здоровью граждан несут многочисленные «сетевые проповедники» и «учителя», распространяющие сомнительные, а иногда и откровенно ложные знания относительно здорового образа жизни, профилактики и лечения заболеваний, личностного роста, совершения юридически значимых действий и т. п. В период пандемии новой коронавирусной инфекции массированное распространение искаженной и фальсифицированной информации о заболевании, методах его предупреждения и лечения существенно снижает эффективность деятельности национальных систем здравоохранения и биологической безопасности.

22. В традиционных российских средствах массовой информации продолжает в большом объеме присутствовать информационная продукция, не способствующая духовному и моральному развитию личности

и общества. При этом имеется существенный недостаток продукции, пропагандирующей традиционные духовно-нравственные ценности, позитивные ценностные и поведенческие установки, положительный образ настоящего и будущего России.

23. Источником угроз информационно-психологической безопасности для детей и иных уязвимых категорий населения являются компьютерные игры, содержащие натуралистичные сцены жесткого насилия, садизма, порнографии, обучающие потреблению наркотиков, изготовлению и применению в реальной жизни оружия и взрывных устройств, совершению террористических и иных насильственных актов, а также самоубийств и иных аутодеструктивных действий. Особую опасность представляют игры в альтернативной реальности, предполагающие выполнение опасных игровых заданий офлайн.

24. Новые горизонты для деструктивного информационно-психологического воздействия на людей и социальные группы открывают системы виртуальной и дополненной реальности, использующие различные сенсорные каналы и создающие глубокий эффект погружения. Ставка крупных технологических компаний на развитие «метавселенных» позволяет прогнозировать их скорое появление и активное «погружение» в них населения, что создает комплекс новых рисков и вызовов.

25. Значимым фактором уязвимости для деструктивного информационно-психологического воздействия выступает низкий уровень медийной и цифровой грамотности населения и культуры информационной безопасности. Отмечается общественный запрос на усиление информационно-просветительской и образовательной деятельности в данной сфере, особенно среди детей и иных уязвимых слоев населения.

III. Национальные интересы в информационной сфере

26. Развитие глобального информационного общества и процессов цифровой трансформации оказывает влияние на все сферы общественной жизни и международные отношения. Информационно-коммуникационные технологии становятся мощным катализатором социального прогресса и одновременно генератором новых вызовов и угроз. Информационная сфера играет ключевую роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

27. Национальными интересами в информационной сфере (в части обеспечения информационно-психологической безопасности) являются:

а) обеспечение и защита конституционных прав и свобод человека и гражданина, включая право на свободу, неприкосновенность частной жизни, защиту своей чести и доброго имени, свободу мысли и слова, право на информацию и свободу массовой информации;

б) формирование среды доверия в цифровой среде;

в) обеспечение доступа к информации, способствующей развитию личности и общества;

г) защита личности, социальных групп и общества в целом от деструктивного информационно-психологического воздействия;

д) гарантирование психического здоровья и благополучия граждан;

е) сохранение традиционных духовно-нравственных ценностей и национальной идентичности российского общества, повышение культурного потенциала страны;

ж) укрепление национального согласия, политической и социальной стабильности;

з) обеспечение информационного суверенитета России;

и) улучшение имиджа России и повышение ее авторитета на международной арене, усиление политического и культурного влияния России в мире;

к) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам деструктивного ИПВ на личность, социальные группы и общество.

28. Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации, создание условий для реализации прав и свобод человека и гражданина, стабильного социально-экономического развития страны и обеспечения ее национальной безопасности.

IV. Цели, задачи и принципы обеспечения информационно-психологической безопасности

29. Стратегической целью обеспечения информационно-психологической безопасности выступает поддержание состояния защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия, обеспечивающего гарантированную реализацию национальных интересов России.

30. Основными объектами деструктивного информационно-психологического воздействия являются:

- личность, большие и малые социальные группы, общество в целом;
- психика человека, включающая сознание и бессознательное, и групповые психические структуры, состоящие из группового (общественного) сознания и коллективного бессознательного;
- индивидуальные и групповые психические процессы (восприятие, память, мышление, мотивация и т. д.) и психические образования (образы, эмоции, цели, установки, архетипы и т. д.).

Приоритетным объектом правовой защиты от деструктивного информационно-психологического воздействия на макросоциальном уровне выступают дети.

31. Задачами обеспечения информационно-психологической безопасности являются:

а) прогнозирование, выявление, анализ и оценка угроз информационно-психологической безопасности;

б) анализ и оценка уязвимости личности, социальных групп и общества от деструктивного информационно-психологического воздействия;

в) стратегическое планирование в сфере обеспечения информационно-психологической безопасности;

г) правовое регулирование отношений в сфере обеспечения информационно-психологической безопасности;

д) применение комплекса оперативных и долговременных мер по профилактике, предупреждению, пресечению и устранению угроз информационно-психологической безопасности, минимизации и (или) ликвидации последствий их воздействия;

е) применение комплекса оперативных и долговременных мер по повышению способности личности, социальных групп и общества противостоять деструктивному информационно-психологическому воздействию;

ж) организация деятельности системы обеспечения информационно-психологической безопасности;

з) кадровое, информационное, материально-техническое и финансовое обеспечение деятельности субъектов обеспечения информационно-психологической безопасности;

и) международное сотрудничество в области обеспечения информационно-психологической безопасности.

32. Деятельность по обеспечению информационно-психологической безопасности осуществляется на основе следующих принципов:

а) соблюдение прав и свобод человека и гражданина;

б) гарантирование свободы массовой информации и запрет цензуры;

в) законность;

г) 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;

д) суверенитет России в информационном пространстве;

е) создание условий, способствующих всестороннему духовному, нравственному, интеллектуальному и физическому развитию детей, воспитанию в них патриотизма, гражданственности и уважения к старшим;

ж) охрана исторической памяти и защита исторической правды;

з) системность и комплексность применения правовых, организационных, информационных и иных мер обеспечения информационно-психологической безопасности;

и) приоритет предупредительных мер обеспечения информационно-психологической безопасности;

к) частно-государственное партнерство и международное сотрудничество в обеспечении информационно-психологической безопасности.

V. Основные направления деятельности по обеспечению общественной безопасности

33. Деятельность по обеспечению информационно-психологической безопасности включает*:*

а) противодействие источникам угроз информационно-психологической безопасности;

б) блокирование или ослабление деструктивного информационно-психологического воздействия угроз на объекты информационно-психологической безопасности, включая ликвидацию (минимизацию) его последствий;

в) повышение жизнестойкости объектов информационно-психологической безопасности;

г) воздействие на факторы внешней информационной среды.

34. Основными направлениями деятельности по выработке и реализации государственной политики обеспечения информационно-психологической безопасности являются:

а) стратегическое планирование в сфере обеспечения информационно-психологической безопасности;

б) правовое регулирование в сфере обеспечения информационно-психологической безопасности;

в) осуществление государственного контроля (надзора) в сфере обеспечения информационно-психологической безопасности;

г) оказание государственных услуг в сфере обеспечения информационно-психологической безопасности;

д) координация деятельности субъектов обеспечения информационно-психологической безопасности;

е) организация материально-технического, финансового и информационного обеспечения деятельности субъектов обеспечения информационно-психологической безопасности;

ж) проведение научных исследований в области обеспечения информационно-психологической безопасности;

з) подготовка кадров в области обеспечения информационно-психологической безопасности;

и) осуществление международного сотрудничества в области информационно-психологической безопасности.

35. Основными направлениями деятельности по непосредственному обеспечению информационно-психологической безопасности выступают:

а) прогнозирование, выявление, анализ и оценка угроз информационно-психологической безопасности;

б) противодействие распространению негативной информации в средствах массовой информации и сети Интернет;

в) противодействие террористической и экстремистской пропаганде и вербовочной деятельности, разжиганию национальной, расовой, религиозной или социальной ненависти и вражды;

г) противодействие деструктивному информационно-психологическому воздействию со стороны государственных органов и специальных служб иностранных государств, иностранных и международных организаций;

д) обеспечение информационно-психологической безопасности детей;

е) защита чести, достоинства и деловой репутации гражданина, деловой репутации юридического лица;

ж) защита органов публичной власти, должностных лиц от деструктивного информационно-психологического воздействия;

з) противодействие фальсификации отечественной и мировой истории в ущерб интересам России;

и) противодействие распространению деструктивных субкультур и иных форм негативного информационно-психологического воздействия в духовной сфере;

к) противодействие преступлениям и административным правонарушениям, связанным с оказанием деструктивного информационно-психологического воздействия;

л) информирование российской и зарубежной общественности о внутренней и внешней политике Российской Федерации, ее официальной позиции по социально значимым событиям внутренней и международной жизни;

м) ведение контрпропаганды в России и за рубежом;

н) формирование цифровой грамотности граждан и культуры информационной безопасности.

VI. Организационные основы обеспечения информационно-психологической безопасности

36. Система обеспечения информационно-психологической безопасности является частью системы обеспечения информационной и национальной безопасности Российской Федерации.

Обеспечение информационно-психологической безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

37. Система обеспечения информационно-психологической безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом

предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

38. Состав системы обеспечения информационно-психологической безопасности определяется Президентом Российской Федерации.

39. Организационную основу системы обеспечения информационно-психологической безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Генеральная прокуратура Российской Федерации, Следственный комитет Российской Федерации, Центральный банк Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационно-психологической безопасности.

Участниками системы обеспечения информационно-психологической безопасности являются: средства массовой информации и массовых коммуникаций, операторы связи, операторы информационных систем и иные информационные посредники, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационно-психологической безопасности.

40. В целях прогнозирования, мониторинга и контроля ситуации в области информационно-психологической безопасности и координации деятельности органов публичной власти и негосударственных участников системы обеспечения информационно-психологической безопасности создается государственная система реагирования на информационно-психологические угрозы, представляющая собой единый централизованный комплекс, включающий силы и средства обнаружения, предупреждения, нейтрализации и ликвидации последствий воздействия информационно-психологических угроз. Положение о государственной системе реагирования на информационно-психологические угрозы утверждается Президентом Российской Федерации.

41. Реализация настоящей Концепции осуществляется на основе отраслевых документов стратегического планирования Российской Федерации. В целях актуализации таких документов Советом Безопасности Российской Федерации определяется перечень приоритетных направлений обеспечения информационно-психологической безопасности на среднесрочную перспективу с учетом положений стратегического прогноза Российской Федерации.

42. Результаты мониторинга реализации настоящей Концепции отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.

Приложение 2

Проект

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»

Внести в Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующие изменения:

1) часть 1 статьи 1 дополнить пунктом 4 следующего содержания:

«4) обеспечении информационно-психологической безопасности.»;

2) статью 2 дополнить пунктом 23 следующего содержания:

«23. информационно-психологическая безопасность – составная часть системы информационной безопасности, представляющая собой состояние защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.»;

3) дополнить статьей 16.2 следующего содержания:

«16.2. Обеспечение информационно-психологической безопасности.

1. Обеспечение информационно-психологической безопасности представляет собой деятельность по выработке и реализации системы правовых, организационных, информационных и иных мер, направленных на обеспечение защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.

2. Государственное регулирование отношений в сфере обеспечения информационно-психологической безопасности осуществляется путем закрепления запретов и ограничений на распространение информации и ведение коммуникаций, оказывающих деструктивное информационно-психологическое воздействие, установления правил распространения информации и оборота информационной продукции, оказывающих деструктивное информационно-психологическое воздействие, регулирования оснований и порядка удаления и (или) ограничения доступа к информации, распространение которой в Российской Федерации запрещено, закрепления обязанностей лиц и организаций по обеспечению информационно-психологической безопасности, правового регулирования оснований и порядка применения мер информационного противоборства, установления мер ответственности за совершение правонарушений в данной сфере, а также правового стимулирования развития информационной грамотности и формирования культуры информационной безопасности.

3. Принципами обеспечения информационно-психологической безопасности являются:

1) соблюдение прав и свобод человека и гражданина;

2) гарантирование свободы массовой информации и запрет цензуры;

3) законность;

4) 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;

5) суверенитет России в информационном пространстве;

6) создание условий, способствующих всестороннему духовному, нравственному, интеллектуальному и физическому развитию детей, воспитанию в них патриотизма, гражданственности и уважения к старшим;

7) охрана исторической памяти и защита исторической правды;

8) системность и комплексность применения правовых, организационных, информационных и иных мер обеспечения информационно-психологической безопасности;

9) приоритет предупредительных мер обеспечения информационно-психологической безопасности;

10) частно-государственное партнерство и международное сотрудничество в обеспечении информационно-психологической безопасности.

4. Приоритетным объектом правовой защиты от информационных угроз выступают дети. В целях обеспечения информационно-психологической безопасности детей настоящим Федеральным законом, Федеральным законом «О защите детей от информации, причиняющей вред их здоровью и развитию», иными федеральными законами устанавливаются запреты, ограничения и правила оборота информационной продукции, содержащей информацию, причиняющую вред здоровью и развитию детей, возрастная классификация и маркировка информационной продукции, экспертиза информационной продукции, правила удаления и (или) ограничения доступа к информации, распространение которой в Российской Федерации запрещено, осуществляются разработка и реализация перечня мероприятий, направленных на обеспечение информационной безопасности детей, производство информационной продукции для детей. Государство стимулирует применение операторами связи, организаторами распространения информации в сети Интернет, владельцами аудиовизуальных сервисов, операторами поисковых систем и иными информационными посредниками программно-технических и организационных мер, направленных на обеспечение информационно-психологической безопасности детей.

5. Федеральные органы исполнительной власти, иные федеральные государственные органы обеспечивают информационно-психологическую безопасность в соответствии с компетенцией, установленной настоящим Федеральным законом, другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации. Органы исполнительной власти субъектов

Российской Федерации, органы местного самоуправления участвуют в обеспечении информационно-психологической безопасности в соответствии с компетенцией, установленной настоящим Федеральным законом, другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

6. Общественные объединения и иные некоммерческие организации, информационные посредники, граждане могут оказывать содействие органам публичной власти в осуществлении мер по обеспечению информационно-психологической безопасности. Органы публичной власти поддерживают и стимулируют участие общественных объединений и иных некоммерческих организаций, информационных посредников, граждан в обеспечении информационно-психологической безопасности.

7. Органы публичной власти во взаимодействии с общественными объединениями и иными некоммерческими организациями, информационными посредниками, гражданами осуществляют меры, направленные на развитие цифровой грамотности и формирование культуры информационной безопасности».

Президент Российской Федерации

Приложение 3

Закрепление угроз информационно-психологической безопасности в документах стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации

№ п/п	Описание угроз информационно-психологической безопасности	Правовой источник
	В сфере информационной безопасности	
1.	Расширение использования информационно-коммуникационных технологий для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, что представляет угрозу международному миру и безопасности	Стратегия НБ 2021, п. 49
2.	Активизация деятельности специальных служб иностранных государств по проведению разведывательных и иных операций в российском информационном пространстве	Стратегия НБ 2021, п. 51
3.	Распространение недостоверной информации, в том числе заведомо ложных сообщений об угрозе совершения террористических актов, в целях дестабилизации общественно-политической ситуации в РФ	Стратегия НБ 2021, п. 52
4.	Размещение в сети Интернет материалов террористических и экстремистских организаций, призывов к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершению самоубийства, пропаганда криминального образа жизни, потребления наркотических средств и психотропных веществ, размещение иной противоправной информации	Стратегия НБ 2021, п. 52
5.	Стремление транснациональных корпораций закрепить свое монопольное положение в сети Интернет и контролировать все информационные ресурсы, введение такими корпорациями (при отсутствии законных оснований и вопреки нормам международного права) цензуры и блокировка альтернативных интернет-платформ	Стратегия НБ 2021, п. 53
6.	Навязывание по политическим причинам пользователям сети Интернет искаженного взгляда на исторические факты, а также на события, происходящие в РФ и в мире	Стратегия НБ 2021, п. 53
7.	Низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности	Доктрина ИБ 2016, п. 18
	В сфере государственной и общественной безопасности	
8.	Рост числа преступлений, совершаемых с использованием ИКТ	Стратегия НБ 2021, п. 42
9.	Экстремистские проявления, оказывающие дестабилизирующее влияние на общественно-политическую обстановку	Стратегия НБ 2021, п. 42
10.	Попытки деструктивных сил за рубежом и внутри страны использовать объективные социально-экономические трудности в РФ в целях стимулирования негативных социальных процессов, обострения межнациональных и межконфессиональных конфликтов, манипулирования в информационной сфере	Стратегия НБ 2021, п. 44

№ п/п	Описание угроз информационно-психологической безопасности	Правовой источник
11.	Разведывательная и иная деятельность специальных служб и организаций иностранных государств	Стратегия НБ 2021, п. 44
12.	Стремление международных террористических и экстремистских организаций усилить пропагандистскую работу и работу по вербовке российских граждан, созданию на территории России своих законспирированных ячеек, вовлечению в противоправную деятельность российской молодежи	Стратегия НБ 2021, п. 44
13.	Использование возможностей глобальных интернет-компаний для распространения недостоверной информации, организации незаконных публичных акций	Стратегия НБ 2021, п. 44
14.	Возрастание масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере	Доктрина ИБ 2016, п. 14
15.	Масштабное использование сети Интернет для пропаганды незаконного потребления наркотиков	Стратегия ГАП пп. «ж» п. 9
16.	Широкое использование террористическими и экстремистскими организациями механизмов информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников	Доктрина ИБ 2016, п. 13
17.	Деятельность, направленная на насильственное изменение конституционного строя РФ, дестабилизацию внутриполитической и социальной ситуации в стране, дезорганизацию функционирования органов государственной власти, важных государственных, военных объектов и информационной инфраструктуры РФ	Военная доктрина, пп. «а» п. 13
18.	Провоцирование межнациональной и социальной напряженности, экстремизма, разжигание этнической и религиозной ненависти либо вражды	Военная доктрина, пп. «г» п. 13
19.	Экстремистская деятельность националистических, религиозных, этнических и иных организаций и структур, направленная на нарушение единства и территориальной целостности РФ, дестабилизацию внутриполитической и социальной ситуации в стране	Концепция ОБ, п. 11
20.	Распространение экстремистских настроений среди молодежи	Концепция ОБ, п. 11
21.	Активное использование членами экстремистских организаций новых технологий, в том числе информационно-телекоммуникационной сети Интернет, для распространения экстремистских материалов, привлечения в свои ряды новых членов и координации противоправной деятельности	Концепция ОБ, п. 11
22.	Поддержка иностранными государственными органами и организациями экстремистских проявлений в целях дестабилизации общественно-политической обстановки в Российской Федерации	Стратегия ПЭ, п. 7
23.	Участившиеся в иностранных государствах случаи умышленного искажения истории, возрождения идей нацизма и фашизма	Стратегия ПЭ, п. 9
24.	Возбуждение ненависти либо вражды по признакам пола, расовой, национальной, языковой, религиозной принадлежности или принадлежности к какой-либо социальной группе, в том числе путем распространения призывов к насильственным действиям, прежде всего через информационно-телекоммуникационные сети, включая сеть Интернет	Стратегия ПЭ, п. 11

№ п/п	Описание угроз информационно-психологической безопасности	Правовой источник
25.	Экстремистская идеология; распространение экстремистских идей, в частности мнения о приемлемости насильственных действий для достижения поставленных целей	Стратегия ПЭ, п. 14–15
26.	Использование религии как инструмента для вовлечения в свои ряды новых членов, средства для разжигания и обострения межконфессиональных и межэтнических конфликтов	Стратегия ПЭ, п. 17
27.	Деятельность отдельных иностранных некоммерческих неправительственных организаций, ряда общественных и религиозных объединений и их структурных подразделений, связанная с распространением экстремистской идеологии	Стратегия ПЭ, п. 22
	В сфере культуры и межнациональных отношений	
28.	Разрушительное воздействие на базовые моральные и культурные нормы, религиозные устои, институт брака, семейные ценности, абсолютизация свободы личности, активная пропаганда вседозволенности, безнравственности и эгоизма, насаждение культа насилия, потребления и наслаждения, легализация употребления наркотиков, формирование сообществ, отрицающих естественное продолжение жизни	Стратегия НБ 2021, п. 85
29.	Использование проблемы межнациональных и межконфессиональных отношений в качестве предмета геополитических игр и спекуляций, порождающих вражду и ненависть	Стратегия НБ 2021, п. 85
30.	Насаждение чуждых идеалов и ценностей, пересмотр базовых норм морали, психологическое манипулирование	Стратегия НБ 2021, п. 86
31.	Нарастание проявлений агрессивного национализма, ксенофобии, религиозного экстремизма и терроризма	Стратегия НБ 2021, п. 86
32.	Активные нападки на традиционные российские духовно-нравственные и культурно-исторические ценности со стороны США и их союзников, а также со стороны транснациональных корпораций, иностранных некоммерческих неправительственных, религиозных, экстремистских и террористических организаций, оказание ими информационно-психологического воздействия на индивидуальное, групповое и общественное сознание путем распространения социальных и моральных установок, противоречащих традициям, убеждениям и верованиям народов РФ	Стратегия НБ 2021, п. 87
33.	Информационно-психологические диверсии и «вестернизация» культуры; попытки фальсификации российской и мировой истории, искажения исторической правды и уничтожения исторической памяти, разжигания межнациональных и межконфессиональных конфликтов, ослабления государствообразующего народа	Стратегия НБ 2021, п. 88
34.	Дискредитация традиционных для России конфессий, культуры, русского языка как государственного языка РФ	Стратегия НБ 2021, п. 89
35.	Формирование новой модели восприятия – так называемого клипового мышления, характерной особенностью которого является массовое поверхностное восприятие информации	Стратегия РИО, п. 16
36.	Размывание традиционных нравственных ценностей народов РФ	Стратегия ГНП, пп. «б» п. 13
37.	Правовой нигилизм	Стратегия ГНП, пп. «в» п. 13
38.	Распространенность негативных стереотипов в отношении некоторых народов	Стратегия ГНП, пп. «е» п. 13

№ п/п	Описание угроз информационно-психологической безопасности	Правовой источник
	В сфере обороны страны и международных отношений	
39.	Расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств	Доктрина ИБ 2016, п. 12, 15
40.	Увеличение в зарубежных СМИ объема материалов, содержащих предвзятую оценку государственной политики РФ	Доктрина ИБ 2016, п. 12
41.	Наращивание информационного воздействия на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей	Доктрина ИБ 2016, п. 12
42.	Использование для решения внешнеполитических задач инструментов «мягкой силы», прежде всего возможностей гражданского общества, информационно-коммуникационных, гуманитарных и других методов и технологий, в дополнение к традиционным дипломатическим методам	Концепция ВП, п. 9
43.	Использование информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности	Военная доктрина, пп. «м» п. 12
44.	Подрывная деятельность специальных служб и организаций иностранных государств и их коалиций против РФ	Военная доктрина, пп. «о» п. 12
45.	Деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющая целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества	Военная доктрина, пп. «в» п. 13

Приложение 4

Виды негативного контента в международно-правовых актах

№ п/п	Описание негативного контента	Правовой источник
Информация, подстрекающая к войне, геноциду, апартеиду, разжигающая ненависть или вражду		
1.	Пропаганда войны	Международный пакт о гражданских и политических правах (ст. 20)
2.	Выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию	Международный пакт о гражданских и политических правах (ст. 20)
3.	Прямое и публичное подстрекательство к совершению геноцида	Конвенция о предупреждении преступления геноцида и наказании за него от 9 декабря 1948 г. (п. «с» ст. III)
4.	Поощрение преступления апартеида	Международная конвенция о пресечении преступления апартеида и наказании за него от 30 ноября 1973 г. (п. «б» ст. III)
5.	Поощрение расовой дискриминации	Международная конвенция о ликвидации всех форм расовой дискриминации от 30 ноября 1973 г. (ст. 4)
6.	Расистские и ксенофобские материалы, мотивированная угроза расизма и ксенофобии; расистское и ксенофобское мотивированное оскорбление	Дополнительный протокол к Конвенции о киберпреступности в отношении криминализации деяний расистского и ксенофобского характера, совершаемых при помощи компьютерных систем, от 28 января 2003 г. (ст. 3–5)
7.	Отрицание, чрезвычайная минимизация, одобрение или оправдание геноцида или преступлений против человечества	Дополнительный протокол к Конвенции о киберпреступности в отношении криминализации деяний расистского и ксенофобского характера, совершаемых при помощи компьютерных систем, от 28 января 2003 г. (ст. 6)
8.	Программы, способствующие расовой ненависти	Европейская конвенция о трансграничном телевидении от 5 мая 1989 г. (пп. «б» ч. 1 ст. 7)
Контент террористического характера		
9.	Публичное подстрекательство к совершению террористического преступления	Конвенция Совета Европы о предупреждении терроризма от 16 мая 2005 г. (ст. 5)
10.	Шокирующие фотографии или изображения террористических актов, которые нарушают принципы неприкосновенности частной жизни и человеческого достоинства жертв либо усиливают терроризирующее воздействие таких актов на население, а также на жертв и их родных	Рекомендация Парламентской ассамблеи Совета Европы № 1706 (2005) «СМИ и терроризм» (пп. «v» п. 8), Декларация о свободе выражения мнений и информации в СМИ в контексте борьбы с терроризмом от 2 марта 2005 г.

№ п/п	Описание негативного контента	Правовой источник
11.	Новостная информация и комментарии, усиливающие социальную напряженность, лежащую в основе терроризма, в частности высказывания, разжигающие ненависть	Рекомендация Парламентской ассамблеи Совета Европы № 1706 (2005) «СМИ и терроризм» (пп. «vi» п. 8), Декларация о свободе выражения мнений и информации в СМИ в контексте борьбы с терроризмом от 2 марта 2005 г.
12.	Распространяемые террористами через Интернет незаконные сообщения и изображения	Рекомендация Парламентской ассамблеи Совета Европы № 1706 (2005) «СМИ и терроризм» (пп. «v» п. 10)
13.	Информация, создающая угрозы для безопасности людей и проведения антитеррористических операций или судебного расследования террористической деятельности	Декларация о свободе выражения мнений и информации в СМИ в контексте борьбы с терроризмом от 2 марта 2005 г.
Контент, содержащий жестокость и насилие, иная социально опасная информация		
14.	Программы, чрезмерно выделяющие насилие	Европейская конвенция о трансграничном телевидении от 5 мая 1989 г. (пп. «б» ч. 1 ст. 7)
15.	Видеозаписи, содержащие насилие, жестокость	Рекомендация Комитета министров Совета Европы № R (89) 7 от 27 апреля 1989 г. относительно принципов распространения видеозаписей, содержащих насилие, жестокость или имеющих порнографическое содержание
16.	Ничем не оправданное изображение насилия (сообщения, слова и изображения, содержащие насилие или символизирующие насилие, которое занимает первостепенное положение и при этом не находит оправдывающих обстоятельств в контексте)	Рекомендация Комитета министров Совета Европы № R (97) 19 от 20 октября 1997 г. о демонстрации насилия в электронных средствах массовой информации
17.	Сообщения, побуждающие к мысли восхищаться теми или подражать тем, кто потребляет табак, алкогольные напитки или наркотические вещества	Рекомендация Комитета министров Совета Европы № R (86) 14 от 16 октября 1986 г. о подготовке стратегии борьбы с курением, злоупотреблением алкогольными напитками и наркоманией в сотрудничестве с органами, проводящими опросы населения, и средствами массовой информации (ст. 7)
Порнографические материалы, непристойная информация		
18.	Детская порнография	Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии, принятый Генеральной ассамблеей ООН 25 мая 2000 г. (ст. 2, 3), Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г. (ст. 9) и др.

№ п/п	Описание негативного контента	Правовой источник
19.	Материалы, пропагандирующие преступления, связанные с торговлей детьми, эксплуатацией детей, детской порнографией, сексуальными злоупотреблениями в отношении детей	Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии, принятый Генеральной ассамблеей ООН 25 мая 2000 г. (ст. 9), Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений от 25 октября 2007 г. (ст. 8)
20.	Непристойные программы	Европейская конвенция о трансграничном телевидении от 5 мая 1989 г. (ст. 7)
Контент, содержащий клевету и оскорбления		
21.	Клеветнические утверждения	Декларация о средствах массовой информации и правах человека от 23 января 1970 г.
Опасная для детей информация		
22.	Информация и материалы, причиняющие вред благополучию ребенка	Конвенция о правах ребенка от 20 ноября 1989 г. (п. «е» ст. 17)
23.	Программы, которые могут нанести вред физическому, умственному или нравственному развитию детей и подростков	Европейская конвенция о трансграничном телевидении от 5 мая 1989 г. (ч. 1 ст. 7)
Запрещенные или ограничиваемые виды рекламы		
24.	Реклама и телеторговля: - вводящая в заблуждение или наносящая ущерб интересам потребителей; - способная причинить вред интересам детям; - призывающая несовершеннолетних совершать сделки по покупке либо аренде товаров и услуг; - воздействующая на подсознание человека; - скрытая	Европейская конвенция о трансграничном телевидении от 5 мая 1989 г. (ч. 2–4 ст. 11)
25.	Реклама и телеторговля определенными видами товаров (табачными изделиями, алкогольными напитками; лекарствами и способами лечения, которые в транслирующем государстве-участнике можно получать только по рецепту врача)	Европейская конвенция о трансграничном телевидении от 5 мая 1989 г. (ч. 1, 3 и 5 ст. 13)

Приложение 5

Закрепление угроз информационно-психологической безопасности в уголовном и административно-деликтном законодательстве Российской Федерации

Виды негативной (противоправной) информации

№ п/п	Уголовно наказуемые виды информации в соответствии с УК РФ	Административно наказуемые виды информации в соответствии с КоАП РФ
	Порочащие сведения и иная информация, оскорбляющая достоинство или подрывающая репутацию лица	
1.	Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию (ст. 128.1, 298.1)	Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию (ст. 5.61.1)
2.	Публичное оскорбление (ст. 297, 319, 336)	Оскорбление, то есть унижение чести и достоинства другого лица, выраженное в неприличной или иной противоречащей общепринятым нормам морали и нравственности форме (ст. 5.61)
3.	Информация, оскорбляющая религиозные чувства верующих (ст. 148 УК РФ)	
4.		Нецензурная брань (ст. 6.26, 6.27, 13.21)
5.		Дискредитирующая информация как способ недобросовестной конкуренции (ст. 14.33)
	Ложная информация	
6.	Заведомо ложные сведения различных типов, в том числе сфальсифицированные[1] (ст. 142, 142.1, 159.1, 170, 170.1, 170.2, 172.2, 185, 185.3, 185.5, 195, 197–199, 200.6, 207, 207.1, 207.2, 217.2, 303, 306, 307, 322.2, 322.3, 327–327.2, 354.1)	[Заведомо][2] ложные (недостоверные) сведения различных типов, в том числе сфальсифицированные (ст. 7.32.6, 8.32.1, 8.32.2, 12.2, 13.15, 13.19.2, 13.22, 14.5, 14.28, 14.44, 15.19, 15.30, 16.2, 16.7, 17.9, 19.7.1, 19.7.2, 19.7.2–1, 19.7.3, 19.7.7–19.7.14, 19.8, 19.8.1, 19.8.2, 19.8.3, 19.13, 19.18, 19.27, 19.23, 19.26)
7.		Неполные или искаженные сведения (ст. 8.5, 11.30, 13.19.2, 14.28, 14.33, 14.34, 14.46, 15.6, 15.11, 15.13, 15.15.16, 15.19, 15.32.2, 15.33, 19.7, 19.7.3, 19.7.5–2–19.7.5–4, 19.7.7–19.7.14, 19.8, 19.8.3, 19.30, 20.2)

[714] Следует отметить, что во многих из перечисленных статей преступное деяние состоит в действиях по изготовлению таких заведомо ложных сведений путем фальсификации документов и иными способами, тогда как распространение указанных сведений выступает преступным деянием в меньшей части составов (ст. 185.3, 207–207.2, 307 УК РФ и др.). Однако принципиально это не меняет сути данного вида контента.

[715] Здесь и далее в таблице квадратные скобки означают, что содержащийся в них признак обозначен не во всех перечисленных ниже статьях закона.

№ п/п	Уголовно наказуемые виды информации в соответствии с УК РФ	Административно наказуемые виды информации в соответствии с КоАП РФ
8.		Сведения, не содержащие необходимых реквизитов/данных либо содержащие ложные (неправомерные) реквизиты (ст. 6.26, 13.15, 13.21, 13.22, 14.3, 14.24, 14.46.1, 15.12, 15.26.1, 15.29, 17.8.1, 17.11, 17.12, 19.34)
Информация, содержащая публичные призывы или иные формы стимулирования противоправных и общественно опасных действий		
9.	[Публичные] призывы: - к совершению самоубийства (ст. 110.2); - к осуществлению террористической деятельности (ст. 205.2); - к массовым беспорядкам или к участию в них (ст. 212); - к насилию над гражданами (ст. 213); - к осуществлению экстремистской деятельности (ст. 280); - к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 280.1); - к развязыванию агрессивной войны (ст. 354)	Публичные призывы: - к осуществлению террористической или экстремистской деятельности (ст. 13.15, 13.37); - к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 20.3.2)
10.	Публичное оправдание терроризма (ст. 205.2)	Материалы, публично оправдывающие терроризм, или другие материалы… обосновывающие или оправдывающие необходимость осуществления такой деятельности (ст. 13.15, 13.37)
11.	Пропаганда терроризма (ст. 205.2)	Пропаганда: - наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ (6.13); - закиси азота (ст. 6.13.1); - нетрадиционных сексуальных отношений среди несовершеннолетних (ст. 6.21); - нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами (ст. 20.3)
12.		Публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами (ст. 20.3)

№ п/п	Уголовно наказуемые виды информации в соответствии с УК РФ	Административно наказуемые виды информации в соответствии с КоАП РФ
13.	Информация, доводящая до самоубийства путем угроз или систематического унижения человеческого достоинства потерпевшего в рамках доведения до самоубийства (ст. 110)	
14.	Информация, склоняющая к совершению самоубийства путем уговоров, предложений, подкупа, обмана или иным способом (ст. 110.1)	
15.	Информация, содействующая совершению самоубийства советами, указаниями, предоставлением информации… или обещанием скрыть средства или орудия совершения самоубийства (ст. 110.1)	
16.	Информация о способах совершения самоубийства (ст. 110.2)	
17.	Информация, склоняющая или иным образом вовлекающая несовершеннолетнего в совершение противоправных действий, заведомо для виновного представляющих опасность для жизни несовершеннолетнего, путем уговоров, предложений, обещаний, обмана, угроз или иным способом (ст. 151.2)[1]	
18.		Реклама табака, табачной продукции, табачных изделий, никотинсодержащей продукции, курительных принадлежностей, устройств для потребления никотинсодержащей продукции или кальянов (ст. 14.3.1)
19.		Демонстрация табачных изделий, никотинсодержащей продукции, курительных принадлежностей, устройств для потребления никотинсодержащей продукции или кальянов либо процесса потребления табака или потребления никотинсодержащей продукции (ст. 14.3.1)

[1] Отметим, что в УК РФ содержится и ряд иных схожих статей, связанных с вовлечением несовершеннолетних в совершение противоправных и иных общественно опасных действий, в частности в совершение преступлений (ст. 150) и антиобщественных действий (ст. 151). Однако они в основном связаны именно с личной коммуникацией, как, впрочем, и сам состав ст. 151.2 УК РФ. Но для последнего установлен квалифицирующий признак: «то же деяние, совершенное в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет)», что однозначно указывает на возможность «контентной» формы проявления данной угрозы. По той же причине в настоящий перечень включены составы ст. 110, 110.1 и 110.2.

№ п/п	Уголовно наказуемые виды информации в соответствии с УК РФ	Административно наказуемые виды информации в соответствии с КоАП РФ
20.		Информация, содержащая предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена (ст. 13.15)
Информация, разжигающая ненависть или вражду		
21.	Информация, возбуждающая ненависть либо вражду, унижающая достоинство человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе (ст. 282)	Информация, возбуждающая ненависть либо вражду, унижающая достоинство человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе (ст. 20.3.1)
22.		Экстремистские материалы (ст. 20.29)
Сведения, связанные с фальсификацией истории или осквернением исторической памяти		
23.	Заведомо ложные сведения о деятельности СССР в годы Второй мировой войны (ст. 354.1)	
24.	Информация, реабилитирующая нацизм, выражающаяся в отрицании фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси, одобрении преступлений, установленных указанным приговором (ст. 354.1)	
25.	Выражающие явное неуважение к обществу сведения о днях воинской славы и памятных датах России, связанных с защитой Отечества (ст. 354.1)	Выражающие явное неуважение к обществу сведения о днях воинской славы и памятных датах России, связанных с защитой Отечества (ст. 13.15)
26.	Информация, оскверняющая символы воинской славы России (ст. 354.1)	Информация, оскверняющая символы воинской славы России (ст. 13.15)
27.	Информация, оскорбляющая память защитников Отечества либо унижающая честь и достоинство ветерана Великой Отечественной войны (ст. 354.1)	
Порнографический контент		
28.	Порнографические материалы или предметы, включая материалы или предметы с порнографическими изображениями несовершеннолетних (ст. 242.1)	Объявление о привлечении детей к участию в создании информационной продукции, причиняющей вред их здоровью и (или) развитию (ст. 6.17)
29.	Материалы или предметы с порнографическими изображениями несовершеннолетних (ст. 242.1)	Материалы или предметы с порнографическими изображениями несовершеннолетних (ст. 6.20)
30.	Зрелищное мероприятие порнографического характера (ст. 242.1)	
Информация, создающая угрозу общественной и транспортной безопасности		

№ п/п	Уголовно наказуемые виды информации в соответствии с УК РФ	Административно наказуемые виды информации в соответствии с КоАП РФ
31.		Знаки и устройства, сходные с маркировочными знаками и устройствами, принятыми для опознавания аэродромов, вертодромов или посадочных площадок, при условии размещения их в районе аэродрома, вертодрома или посадочной площадки (ст. 11.3)
32.		Сведения, содержащие инструкции по самодельному изготовлению взрывчатых веществ и взрывных устройств (ст. 13.15)
33.		Реклама, имеющая сходство с дорожными знаками (ст. 14.38)
34.		Информация, нарушающая установленные законодательством о средствах массовой информации условия освещения контртеррористической операции (ст. 20.27)
Вредная для детей информация		
35.		Информация, причиняющая вред здоровью и (или) развитию детей (ст. 13.21, 13.36)
36.		Информация о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия) (ст. 13.15)
Информация, воздействующая на бессознательное		
37.		Теле-, видео-, кинопрограммы, документальные и художественные фильмы, а также относящиеся к специальным средствам массовой информации информационные компьютерные файлы и программы обработки информационных текстов, содержащие скрытые вставки, воздействующие на подсознание людей и (или) оказывающие вредное влияние на их здоровье (ст. 13.15)

Виды деструктивной (противоправной) коммуникации

№ п/п	Уголовно наказуемые виды коммуникации в соответствии с УК РФ	Административно наказуемые виды коммуникации в соответствии с КоАП РФ
Коммуникация, связанная с оскорблением и иными формами унижения человеческого достоинства		
1.	Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию (ст. 128.1, 298.1)	Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию (ст. 5.61.1)
2.		Дискредитация как способ недобросовестной конкуренции (ст. 14.33)

№ п/п	Уголовно наказуемые виды коммуникации в соответствии с УК РФ	Административно наказуемые виды коммуникации в соответствии с КоАП РФ
3.	Публичное оскорбление (ст. 297, 319, 336)	Оскорбление, то есть унижение чести и достоинства другого лица, выраженное в неприличной или иной противоречащей общепринятым нормам морали и нравственности форме (ст. 5.61)
4.		Мелкое хулиганство, то есть нарушение общественного порядка, выражающее явное неуважение к обществу, сопровождающееся нецензурной бранью в общественных местах, оскорбительным приставанием к гражданам, а равно уничтожением или повреждением чужого имущества (ст. 20.1)
5.		Появление… в… общественных местах в состоянии опьянения, оскорбляющем человеческое достоинство и общественную нравственность (ст. 20.21)
	Обман и манипулирование сознанием	
6.	Заведомо ложный донос о совершении преступления (ст. 306)	
7.	Обман или злоупотребление доверием как способ совершения преступлений (ст. 110.1, 150, 159–159.5, 165)	
8.		Использование в коммуникации разных форм обмана (ст. 16.2, 16.7, 17.9, 19.18, 19.27 и др.)
9.		Распространение в информационно-телекоммуникационных сетях заведомо недостоверной общественно значимой информации под видом достоверных сообщений (ст. 13.15)
10.		Распространение ложных, неточных или искаженных сведений как форма недобросовестной конкуренции (ст. 14.33)
11.	Манипулирование рынком (ст. 185.3)	Манипулирование рынком (ст. 15.30)
12.	Умышленное использование инсайдерской информации (ст. 185.6)	
13.	Фиктивное банкротство, то есть заведомо ложное публичное объявление руководителем или учредителем (участником) юридического лица о несостоятельности данного юридического лица, а равно гражданином, в том числе индивидуальным предпринимателем, о своей несостоятельности (ст. 197)	
14.	Заведомо ложное сообщение об акте терроризма (ст. 207)	Заведомо ложный вызов специализированных служб (ст. 19.13)
15.	Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 207.1)	

№ п/п	Уголовно наказуемые виды коммуникации в соответствии с УК РФ	Административно наказуемые виды коммуникации в соответствии с КоАП РФ
16.	Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия (ст. 207.2)	
17.	Обман как способ уклонения военнослужащего от исполнения обязанностей военной службы (ст. 339)	
	Публичные призывы или иные формы стимулирования противоправных и иных общественно опасных действий	
18.	Публичные призывы: - к осуществлению террористической деятельности (ст. 205.2); - к массовым беспорядкам или к участию в них (ст. 212); - к насилию над гражданами (ст. 213); - к осуществлению экстремистской деятельности (ст. 280); - к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 280.1); - к развязыванию агрессивной войны (ст. 354)	[Публичные] призывы: - к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 20.3.2); - к совершению самоубийства (ст. 110.2)
19.	Публичное оправдание терроризма (ст. 205.2)	
20.	Пропаганда терроризма (ст. 205.2)	Пропаганда: - наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ (ст. 6.13); - закиси азота (ст. 6.13.1); - нетрадиционных сексуальных отношений среди несовершеннолетних (ст. 6.21); - нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами (ст. 20.3)
21.	Доведение до самоубийства или до покушения на самоубийство путем угроз… или систематического унижения человеческого достоинства потерпевшего (ст. 110)	
22.	Склонение к совершению самоубийства путем уговоров, предложений, подкупа, обмана или иным способом (ст. 110.1)	

№ п/п	Уголовно наказуемые виды коммуникации в соответствии с УК РФ	Административно наказуемые виды коммуникации в соответствии с КоАП РФ
23.	Содействие совершению самоубийства советами, указаниями, предоставлением информации… или обещанием скрыть средства или орудия совершения самоубийства (ст. 110.1)	
24.	[Склонение], [вербовка] или [иное вовлечение] лица: - в совершение преступления (ст. 150); - в совершение антиобщественных действий (ст. 151); - в совершение действий, представляющих опасность для жизни несовершеннолетнего (ст. 151.2); - в совершение хотя бы одного из преступлений террористического характера (ст. 205.1); - в совершение действий, связанных с организацией массовых беспорядков (ст. 212); - к потреблению наркотических средств, психотропных веществ или их аналогов (ст. 230); - спортсмена к использованию субстанций и (или) методов, запрещенных для использования в спорте (ст. 230.1); - в занятие проституцией или принуждение к продолжению занятия проституцией (ст. 240); - в деятельность экстремистского сообщества (ст. 282.1)	Вовлечение несовершеннолетнего: - в употребление алкогольной и спиртосодержащей продукции, новых потенциально опасных психоактивных веществ или одурманивающих веществ (ст. 6.10); - в процесс потребления табака или потребления никотинсодержащей продукции (ст. 6.23); - в участие в несанкционированных собрании, митинге, демонстрации, шествии или пикетировании, если это действие не содержит уголовно наказуемого деяния (ст. 20.2)
25.	Побуждение граждан к отказу от исполнения гражданских обязанностей или к совершению иных противоправных деяний (ст. 239)	
26.	Обещание или предложение посредничества в коммерческом подкупе (ст. 204.1)	
27.	Обещание или предложение посредничества во взяточничестве (ст. 291.1)	Незаконные… предложение или обещание от имени или в интересах юридического лица либо в интересах связанного с ним юридического лица… денег, ценных бумаг или иного имущества, оказание ему услуг имущественного характера либо предоставление ему имущественных прав… (ст. 19.28)
28.	Провокация взятки, коммерческого подкупа либо подкупа в сфере закупок товаров, работ, услуг для обеспечения государственных или муниципальных нужд (ст. 304)	

№ п/п	Уголовно наказуемые виды коммуникации в соответствии с УК РФ	Административно наказуемые виды коммуникации в соответствии с КоАП РФ
	Коммуникация, разжигающая ненависть или вражду	
29.	Действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично (ст. 282)	Действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично (ст. 20.3.1)
30.	Публичные действия, выражающие явное неуважение к обществу и совершенные в целях оскорбления религиозных чувств верующих (ст. 148)	
	Угрозы и принуждение	
31.	Угрозы как способ доведения до самоубийства (ст. 110)	
32.	Угроза убийством или причинением тяжкого вреда здоровью (ст. 119)	
33.	Угроза убийством, причинением вреда здоровью, уничтожением или повреждением имущества в отношении участников правосудия или предварительного расследования (ст. 296)	
34.	Вымогательство, то есть требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких (ст. 163)	
35.	Принуждения журналистов к распространению либо к отказу от распространения информации (ст. 144)	Принуждение: - к участию в собрании, митинге, демонстрации, шествии или пикетировании (ст. 5.38); - к участию или к отказу от участия в забастовке путем… угроз применения насилия либо с использованием зависимого положения принуждаемого (ст. 5.40)
36.	Принуждение к совершению сделки или к отказу от ее совершения под угрозой применения насилия, уничтожения или повреждения чужого имущества, а равно распространения сведений, которые могут причинить существенный вред правам и законным интересам потерпевшего или его близких (ст. 179)	Понуждение хозяйствующим субъектом, осуществляющим торговую деятельность, или хозяйствующим субъектом, осуществляющим поставки продовольственных товаров, к заключению и (или) исполнению договора возмездного оказания услуг (в том числе с третьими лицами)… (ст. 14.42)
37.	Принуждение к даче показаний (ст. 302, 309)	

№ п/п	Уголовно наказуемые виды коммуникации в соответствии с УК РФ	Административно наказуемые виды коммуникации в соответствии с КоАП РФ
38.	Принуждение к даче показаний или уклонению от дачи показаний либо к неправильному переводу (ст. 309)	
Негативная сексуальная коммуникация		
39.	Развратные действия (ст. 135)	
40.	Привлечение несовершеннолетнего в качестве исполнителя для участия в зрелищном мероприятии порнографического характера (ст. 242.2)	
Коммуникация, связанная с фальсификацией истории или оскорблением исторической памяти		
41.	Вандализм, то есть осквернение зданий или иных сооружений (ст. 214)	
42.	Реабилитация нацизма, выражающаяся в отрицании фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси, одобрении преступлений, установленных указанным приговором, а равно распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны (ст. 354.1)	
43.	Надругательство над Государственным гербом Российской Федерации или Государственным флагом Российской Федерации (ст. 329)	
44.	Публичное осквернение символов воинской славы России (ст. 354.1)	Публичное осквернение символов воинской славы России (ст. 13.15)

Смирнов А. А.

Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации

Дизайн, верстка: В. Матвеев
Корректор: О. Гриднева

ООО «Издательство «Русь»
194362, Санкт-Петербург,
п. Парголово, ул. Ломоносова, д. 113, лит. А
Подписано в печать 22.08.2022

Тираж 500 экз. Заказ 218
Отпечатано в типографии «РИП СПБ»
194295, г. Санкт-Петербург,
Поэтический бульвар, д. 2, лит. А

ISBN 978-5-8090-0109-0