

Федеральное государственное автономное образовательное учреждение  
высшего образования  
«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ  
ИМЕНИ ПАТРИСА ЛУМУМБЫ» (РУДН)

*На правах рукописи*

**СЕИДОВ Рафаэль Закирович**

**АДМИНИСТРАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ  
В СЕТИ «ИНТЕРНЕТ»**

5.1.2 Публично-правовые (государственно-правовые) науки

**ДИССЕРТАЦИЯ**

на соискание ученой степени кандидата юридических наук

**Научный руководитель:**

кандидат юридических наук, доцент

Иванский Валерий Прокопьевич

Москва – 2025

## ОГЛАВЛЕНИЕ

<b>ВВЕДЕНИЕ</b> .....	4
<b>Глава 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ «ИНТЕРНЕТ»</b> .....	24
1.1. Понятие «несовершеннолетний» в юридической науке, законодательстве России и зарубежных государствах.....	24
1.2. Правовая характеристика информации, причиняющей вред здоровью и развитию несовершеннолетних с помощью сети «Интернет», в российском законодательстве.....	49
1.3. Правовая характеристика деструктивного контента для несовершеннолетних в сети «Интернет» в зарубежном законодательстве.....	65
1.4. Концептуальные подходы к пониманию категории «информационная безопасность» в законодательстве и юридической науке.....	84
<b>Глава 2. ПРАВОВОЙ СТАТУС ОРГАНОВ ПУБЛИЧНОЙ ВЛАСТИ И ЧАСТНЫХ ЛИЦ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ «ИНТЕРНЕТ»</b> .....	110
2.1. Публичные властные субъекты по обеспечению информационной безопасности несовершеннолетних в зарубежных государствах.....	110
2.2. Органы публичной власти в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в России.....	138
2.3. Частные лица в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в России и зарубежных государствах.....	162
<b>Глава 3. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТВЕТСТВЕННОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ «ИНТЕРНЕТ»</b>	

<b>ПО ЗАКОНОДАТЕЛЬСТВУ РОССИИ И ЗАРУБЕЖНЫХ ГОСУДАРСТВ.....</b>	<b>188</b>
3.1. Меры административного принуждения в сфере информационной безопасности несовершеннолетних в сети «Интернет» по законодательству зарубежных государств.....	188
3.2. Общая характеристика административной ответственности за правонарушения в области информационной безопасности несовершеннолетних в российском сегменте сети «Интернет» .....	205
<b>ЗАКЛЮЧЕНИЕ.....</b>	<b>235</b>
<b>СПИСОК ЛИТЕРАТУРЫ .....</b>	<b>246</b>
<b>Приложение А. Виды деструктивного контента в сети «Интернет» для несовершеннолетних лиц.....</b>	<b>312</b>
<b>Приложение Б. Полномочия «Управления по информационной безопасности несовершеннолетних» в составе структуры Роскомнадзора.....</b>	<b>315</b>
<b>Приложение В. Законопроект статьи 10.8. Обязанности владельца социальных сетей в информационно-телекоммуникационной сети «Интернет».....</b>	<b>317</b>
<b>Приложение Г. Составы административных правонарушений по КоАП РФ в сфере информационной безопасности несовершеннолетних в сети «Интернет».....</b>	<b>318</b>
<b>Приложение Д. Законопроект статьи 6.17.1. Регистрация пользователя социальной сети в информационно-телекоммуникационной сети «Интернет» без идентификации и (или) без аутентификации возраста пользователя.....</b>	<b>321</b>
<b>Приложение Е. Статистика размеров административных штрафов, налагаемых на граждан в сфере информационной безопасности несовершеннолетних в сети «Интернет».....</b>	<b>322</b>

## ВВЕДЕНИЕ

**Актуальность темы исследования.** В современных условиях информационно-телекоммуникационная сеть «Интернет» представляет собой неотъемлемую часть жизни почти каждого человека. Значительное распространение информации в сети «Интернет» оказывает как положительное влияние на участников интернет-пространства, так и деструктивное, в особенности на несовершеннолетних лиц, которые попадают под воздействие информации, причиняющей им вред, – моральный, психологический, материальный, физический.

По данным МВД России, за первые семь месяцев 2025 года число правонарушений, совершенных с использованием сети «Интернет» против несовершеннолетних в России, увеличилось на 25 % по сравнению с аналогичным периодом 2024 года. Жертвами киберпреступников стали около 5 тысяч несовершеннолетних<sup>1</sup>. При этом наиболее часто интернет-средой совершения преступлений в отношении несовершеннолетних выступают социальные сети (70 %), в основном «ВКонтакте» и «Одноклассники»<sup>2</sup>.

Административно-правовое обеспечение информационной безопасности несовершеннолетних в сети «Интернет» становится одной из первоочередных задач любого государства и в особенности России: в ч. 4 ст. 67.1 Конституции РФ указано, что «дети – важнейший приоритет государственной политики России»<sup>3</sup>. Следовательно, в целях совершенствования административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет» проводится исследование нормативно-правовых актов российского и зарубежных государств и особенно их правоприменения, научных трудов.

На основании вышесказанного диссертационное исследование содержит анализ законодательства и правоприменительного опыта России с такими

---

<sup>1</sup> Информационное агентство ТАСС. URL: <https://tass.ru/obschestvo/24919635> (дата обращения: 21.08.2025).

<sup>2</sup> Сетевое издание «Интерфакс-Россия». URL: <https://www.interfax-russia.ru/northwest/main/kazhdoe-pyatoe-kiberprestuplenie-v-rf-soversheno-podrostkami-statistika-skr> (дата обращения: 21.08.2025).

<sup>3</sup> Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 06.10.2022.

государствами, как Австралия, Великобритания, Франция (национального и наднационального законодательств ЕС). Выбор этих государств для исследования обусловлено следующими авторскими критериями: 1) наличие национального закона о безопасности в сети «Интернет»; 2) наличие законодательно закреплённого положения или законопроекта о возрастных ограничениях в сети «Интернет», в том числе непосредственно идентификации несовершеннолетних в социальных сетях. Австралия полностью удовлетворяет своим законодательством обоим критериям и представляет собой первое в мире государство, законодательно ограничившее доступ к социальным сетям по возрастному признаку. Великобритания также имеет закон о безопасности в сети «Интернет», в котором, в том числе, есть нормы, которые обязывают онлайн-платформы принимать меры по определению возраста и проверке возраста пользователя. Великобритания очень много внимания уделила возможным вариантам проверки возраста пользователей цифровыми платформами, что представляет научный интерес в рамках диссертационного исследования. Франция имеет профильный закон о безопасности в сети «Интернет» и имеет законодательно закреплённые положения о верификации возраста несовершеннолетних в сети «Интернет».

Поэтому законодательный и правоприменительный опыт этих государств предоставляет для нас научный интерес. Также считаем возможным рассмотреть в рамках исследования и законодательства иных государств, например:

- при определении правового содержания понятий «несовершеннолетний», «подросток», «малолетний» – в этом случае для нас наибольший интерес, с правовой точки зрения, будет представлять законодательство Германии, в котором есть исследуемые понятия, легально закреплённые;

- исследовательский фокус также направлен на законодательство Ирландии, у которой есть и профильный закон, и законопроект в этой сфере, который был снят в 2025 году с рассмотрения в силу исключительно политических причин (ропуском Нижней палаты ирландского парламента);

- также в работе имеются упоминания законов США как правового родоначальника этой сферы: первая социальная сеть появились именно в США в

1995 году – Classmates.com, а также именно в США зарегистрированы основные цифровые платформы (Facebook, X, Instagram – запрещенные на территории РФ на данный момент). То есть первое правило о возрастном ограничении самих цифровых платформ как раз связано именно с Законом США о защите конфиденциальности детей в Интернете 1998 года<sup>4</sup>, который запрещает веб-сайтам собирать информацию о детях младше 13 лет без их согласия, и, по общему правилу, которое законодательно не закреплено, текущий минимальный возраст доступа во всех основных социальных сетях составляет 13 лет.

Изучить большее количество государств также не позволяет ограниченный объем диссертационного исследования. Однако с увеличением правового сотрудничества России и Китая, Индии, Бразилии считаем важным уточнить следующее. Нами не рассматриваются эти государства в связи с тем, что в Бразилии и Индии отсутствует законодательно закрепленное положение или законопроект о возрастных ограничениях в сети «Интернет», в том числе идентификация несовершеннолетних в социальных сетях; в Китае разработано детальное законодательство в исследуемой сфере, но оно регламентирует иные правовые аспекты в отличие от российского и европейского, австралийского законодательств, направленных на: 1) идентификацию всех пользователей вне зависимости от возраста; 2) ограничение не в рамках доступа (регистрации) несовершеннолетнего в сети «Интернет», а в части ограничения времени, которое проводит в сети «Интернет» несовершеннолетний. Можно сказать, что, с одной стороны, Китай, а с другой стороны, например, Австралия и некоторые государства Евросоюза образуют две абсолютно разные модели по обеспечению информационной безопасности несовершеннолетних в сети «Интернет», так как в Китае изначально обеспечивается информационная безопасность лиц по единым стандартам независимо от возрастных критериев, то есть это полная идентификация (аутентификации) при регистрации на цифровых платформах (с указанием документа, подтверждающего личность). Таким образом, социальные сети Китая

---

<sup>4</sup> Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (дата обращения: 30.03.2025).

достаточно «прозрачны». В Австралии, США, ЕС – более гибкий подход. Постепенно большинство государств приходят к выводу, что необходимо вводить ограничения по возрасту при регистрации и использовании социальных сетей. Причем эти ограничения вводятся, в отличие от Китая, именно на момент регистрации пользователя, а не во время, проведенное им в социальной сети. У России сегодня есть возможность выбора модели по обеспечению информационной безопасности несовершеннолетних в сети «Интернет»: либо более жесткая регламентация (как в Китае), либо более гибкий подход (как уже сделали, например, Австралия, Франция, Великобритания).

Несомненно, административно-правовое обеспечение информационной безопасности лиц любого возраста и непосредственно несовершеннолетних лиц имеет отличия из-за большей уязвимости последних в части особенностей их развития – психического, умственного, физиологического, паттернов поведения – ввиду отсутствия у несовершеннолетних лиц развитого критического мышления и жизненного опыта. По этой причине требуется разработка особенностей административно-правового обеспечения их информационной безопасности в сети «Интернет», что послужило основой для более детального изучения в данном диссертационном исследовании понятия «несовершеннолетние» и его классификаций.

**Степень разработанности темы исследования.** Исследуемая тема достаточно широко рассмотрена учеными-юристами, но в контексте административной ответственности несовершеннолетних и правовых аспектов информационной безопасности граждан не подлежали обстоятельному научному анализу научно-правовые проблемы, связанные с административно-правовым обеспечением информационной безопасности несовершеннолетних в сети «Интернет». Имеются следующие диссертационные исследования правовых аспектов информационной безопасности несовершеннолетних в сети «Интернет»: С. Л. Банщикова («Административная ответственность за неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по их содержанию и воспитанию», 2017), С. А. Буданов («Правовое

обеспечение информационной безопасности несовершеннолетних», 2006), В. А. Гирис («Правовое регулирование деятельности Европейского союза в области обеспечения кибербезопасности», 2023), Е. В. Горбачева («Административно-правовое обеспечение информационной безопасности несовершеннолетних», 2011), Е. В. Кузнецова («Предупреждение делинквентного поведения несовершеннолетних, продуцируемого контентом сети Интернет», 2019), С. Л. Липатовой («Защита конституционных прав человека на честь и достоинство от посягательств в компьютерной сети «Интернет», 2006), С. В. Молчанова («Административно-правовые основания ограничения конституционного права человека на распространение информации через Интернет в Российской Федерации», 2005), А. В. Польшикова («Уголовно-правовые и криминологические меры борьбы с изготовлением и оборотом материалов с порнографическими изображениями несовершеннолетних в сети «Интернет», 2009), Т. И. Сустина («Правовое обеспечение информационной безопасности несовершеннолетних в условиях цифровой трансформации общества», 2023), К. А. Шуликова («Административно-правовые основы противодействия распространению деструктивного контента в сети «Интернет», 2024).

Отметим, что вопросу социальных сетей посвящено исследование М. А. Болвачева («Использование социальных сетей при расследовании преступлений экстремистской направленности», 2022), однако тема исследования лишь незначительно коррелирует с тематикой нашего исследования.

Правовые исследования понятий «несовершеннолетний», «ребенок» и «подросток» в юридической науке представлены в научных трудах В. И. Абрамова, Д. К. Амировой, Т. Н. Балашова, И. Бандурка, А. Р. Бахман, Д. Н. Бахрах, С. А. Ветошкина, Л. Н. Дегтярева, Е. А. Капитонова, Н. В. Комбарова, Е. А. Лактюнкина, Т. В. Обыденова, Г. Ф. Ручкина, О. В. Садина, А. П. Солдатова, А. В. Токарева, Е. О. Тулупова, Е. А. Усачева, Н. М. Хромова, И. В. Черненко, К. Б. Ярошенко и др. А также в научных работах зарубежных авторов-правоведов: S. C. Aitken, A. Daly, E. Desmet, R. T. Dias, J. Eekelaar, M. Freeman, R. M. Galvão, K. Hanson, K. Hollingsworth, N. Pardhey, N. Peleg, A. Rabe, S. Rap, R. Ribeiro,



H. Stalford, E. K. M. Tisdall, J. Tobin, M. Varela и др.

Вопросы понятия информации, информационных прав и ограничений представлены в трудах таких авторов, как С. С. Алексеев, И. Л. Бачило, Е. Г. Белякова, А. И. Березенцева, Л. А. Букалерева, И. Ю., Гольяпина, М. С. Дадаева, И. А. Демидова, В. П. Иванский, С. В. Кобзева, А. В. Корнев, С. П. Матвеев, В. С. Маурин, Н. Н. Моисеев, Д. Ф. Мухаметова, О. В. Танимов, Р. Ш. Шарофзода, Г. А. Шокиров, С. А. Anderson, L. A. Bygrave, L. A. Bygrave, N. L. Carnagey, K. E. Dill, J. Eubanks, R. Gellert, D. Hallinan, C. Violato, K. Yeung и др.

Проблематику отнесения информации к «деструктивной», «вредоносной», «вредной» для несовершеннолетнего рассматривают такие авторы, как П. А. Астафичев, К. М. Беликова, Е. Л. Болотова, К. В. Бородин, М. С. Власенко, К. Э. Геляхов, Г. А. Грищенко, Ю. Н. Кириченко, К. К. Крупенникова, Е. В. Кузнецова, И. В. Медведева, В. Д. Никишин, С. А. Осипов, Р. Е. Ренжигло, К. Д. Рыдченко, Ю. Б. Савва, Е. Н. Тогузаева, М. Ю. Толстых, В. Н. Цимбал, К. А. Шуликов и др.

Разные аспекты правовых категорий «информационная безопасность» и «кибербезопасность» изучены и отражены в трудах таких авторов, как С. А. Авакьян, Н. А. Аникина, М. М. Ащепкова, А. В. Борисенко, Е. А. Брылева, Н. С. Виноградова, Н. С. Волкова, С. Т. Гаврилов, Х. И. Гаджиев, Е. В. Горбачева, В. В. Горлова, Н. В. Гришина, Д. И. Дедов, М. К. Дзанагова, Н. Диакун-Тибо, В. А. Довгаль, А. С. Дугенец, С. В. Иванов, В. Я. Ищейнов, А. В. Кубышкин, А. А. Кузнецов, Д. В. Куц, В. А. Лаврухин, Ю. А. Ланчева, Т. Г. Маглинова, Д. С. Малец, А. С. Митрясов, А. А. Нечай, Н. В. Новикова, Т. А. Полякова, Д. И. Правиков, О. А. Пучков, А. А. Смирнов, А. И. Смирнов, В. Ю. Статъев, А. П. Стельмах, В. Н. Стрельникова, Э. В. Талапина, Л. К. Терещенко, В. А. Тиньков, А. В. Тонконогов, Н. В. Третьяк, О. М. Хохлова, В. А. Цвык, Я. А. Чувашова, B. Corcoran, G. G. Fuster, M. Kaljurand, N. Kshetri, K. R. Ludvigsen, G. Szpor и др.

Правовые аспекты органов публичной власти и организаций обеспечения информационной безопасности несовершеннолетних в сети «Интернет» отражены в трудах таких авторов, как А. Н. Акимова, Л. И. Афанасьева, С. Л. Банщикова,

Л. Л. Бошаева, О. Н. Булаков, С. В. Венцель, В. Э. Гацолати, И. Ю. Гольяпина, А. З. Динисламова, А. Б. Зеленцов, В. А. Зоз, А. С. Лагуточкина, Е. И. Лукина, О. В. Маскальцова, А. К. Полянина, О. А. Федотова, В. А. Чистяков, Л. В. Шварц, А. М. Шитов, К. А. Шуликов; зарубежных ученых-правоведов: P. Crofts, M. A. P. Dinis, H. Dong, J. Gaffey, B. Gengler, W. Hao, W. Hartzog, T. Hu, Y. Jang, C. Jarvie, C. Libor, O. Likhota, P. Lindskoug, X. Lu, Z. Martin, H. van Rijswijk, A. I. Sani, M. Smith, D. J. Solove, D. Svantesson, M. Vara, K. Virgin, F. Yang и др.

Административно-правовая ответственность за нарушение законодательства РФ и зарубежных государств в сфере информационной безопасности несовершеннолетних в сети «Интернет» рассмотрена в научных трудах таких авторов, как Е. В. Абраменко, М. В. Бондаренко, Л. В. Гаврилова, А. В. Голикова, П. В. Головненков, А. А. Ефремов, И. А. Зайцев, Н. С. Зорина, Г. Ю. Каримова, Н. Е. Краснова, Р. А. Леонов, Е. В. Муратова, Д. А. Новгородов, Е. А. Перепелова, В. Н. Плигина, Е. Ю. Политова, А. И. Сметанникова, А. К. Соловьева, С. В. Соловьева, О. А. Строева, А. П. Стуканов, Э. В. Талапина, Л. К. Терещенко, Л. В. Чистякова, К. О. Шкатулов, W. Bateman, L. McDonald и др.

На основании вышесказанного можно сделать вывод, что, несмотря на достаточное количество диссертационных исследований и иных научно-правовых трудов, которые посвящены информационной безопасности в целом и непосредственно несовершеннолетних, особенностям обеспечения информационной безопасности в сети «Интернет», непосредственно административно-правовое обеспечение информационной безопасности несовершеннолетних в сети «Интернет» на диссертационном и монографическом уровне ранее не исследовалось, что делает данное диссертационное исследование новаторским, особенно с учетом компаративного анализа российского и зарубежного законодательства в исследуемой сфере правоотношений.

**Объектом исследования** является совокупность общественных отношений, складывающихся в связи с административно-правовым обеспечением информационной безопасности несовершеннолетних в сети «Интернет», а также система сформировавшихся в правоведении научных представлений в этой

области.

**Предметом исследования** выступает совокупность правовых норм, регламентирующих административно-правовое обеспечение информационной безопасности несовершеннолетних в сети «Интернет», зарубежный опыт в этой сфере, судебная и правоприменительная практика, полномочия публичных властных субъектов в сфере административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет», в том числе по регламентированию доступа несовершеннолетних в социальные сети, доктринальные конструкции и понятия.

**Цель исследования** заключается в формировании целостного научного представления об административно-правовых средствах обеспечения информационной безопасности несовершеннолетних в сети «Интернет» на основе анализа научных теорий и актуального законодательства в этой сфере; а также разработка научно обоснованных предложений по совершенствованию действующего российского законодательства в этой сфере.

**Задачи диссертационного исследования:**

- определение понятия «несовершеннолетний» в юридической науке, законодательстве РФ и зарубежных государств; сравнительный анализ понятия «несовершеннолетний» с терминами «ребенок» и «подросток»;
- изучение правовых характеристик информации, причиняющей вред здоровью и развитию несовершеннолетних с помощью сети «Интернет», в российском и зарубежных законодательствах;
- определение концептуальных подходов к пониманию категории «информационная безопасность» в юридической науке и законодательстве;
- изучение правового статуса публичных властных субъектов в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в Российской Федерации и зарубежных государствах;
- раскрытие особенностей участия частных лиц в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в Российской Федерации и зарубежных государствах;

- изучение мер административного принуждения в сфере информационной безопасности несовершеннолетних в сети «Интернет» по законодательству зарубежных государств;
- раскрытие общей характеристики административной ответственности за правонарушения в области информационной безопасности несовершеннолетних в российском сегменте сети «Интернет»;
- разработка предложений по совершенствованию норм российского законодательства, связанного с информационной безопасностью несовершеннолетних в сети «Интернет».

**Методология и методы исследования.** Для достижения цели и задач диссертационного исследования были использованы различные методы познания, а именно: философские методы (диалектический, историзм); общенаучные методы исследования – методы эмпирического исследования (сравнение, описание и измерение); теоретические и общелогические методы (дедукция, индукция, системный подход, методы анализа, синтеза, структурно-функциональный, сравнение, классификация); частнонаучный метод (сравнительно-правовой); специально-юридические методы (формально-юридический, метод юридической аналогии, метод толкования юридических норм).

Диалектический метод использовался для изучения отличительных правовых характеристик объекта исследования, в том числе для изучения правовых характеристик информации, причиняющей вред здоровью и развитию несовершеннолетних с помощью сети «Интернет» в российском и зарубежных законодательствах. С использованием диалектического метода исследования была раскрыта правовая природа понятий «несовершеннолетний», «малолетний» и «подросток», «информационная безопасность» и «информационная безопасность непосредственно несовершеннолетних в сети «Интернет».

Историко-правовой метод был использован для анализа становления (развития) административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет», трансформации законодательства в этой сфере с учетом современных реалий.

Для анализа правовых норм и изучения закономерностей развития права в сфере административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет», выявления взаимосвязей между правом и другими социальными явлениями (в частности, влияния деструктивного контента на несовершеннолетних, их развития и нравственности), а также для прогнозирования изменений в правовой системе были использованы общенаучные методы исследования. Системный анализ позволил выявить внутренние взаимосвязи между нормативными конструкциями, субъектами правоотношений в исследуемой теме. Применение системно-структурного метода позволило раскрыть информационную безопасность несовершеннолетних в сети «Интернет» как элемент общей системы административно-правового регулирования информационной безопасности; этот метод был использован при изучении условий и порядка привлечения к ответственности за административные правонарушения в исследуемой сфере правоотношений. Функциональный метод применен для определения ключевых направлений развития законодательства об административной ответственности в рамках применения идентификации возраста пользователей социальных сетей.

Сравнительный (сравнительно-правовой) подход использовался для анализа понятийного аппарата и источников права, научно-правовых трудов в области административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет», а также для сопоставления российского законодательства и зарубежных стран. Применение формально-юридического метода в диссертационном исследовании позволило провести анализ административно-правовых норм и понятийного аппарата в сфере административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет» и обосновать основные и предложенные авторские дефиниции; проанализировать нормативно-правовые источники, судебную практику. Метод толкования норм права использовался при изучении норм, регулирующих вопросы правонарушений в области информационной безопасности несовершеннолетних в российском и зарубежном сегментах сети

«Интернет».

Применение в диссертационной работе комплекса методов обеспечило всестороннее изучение объекта и предмета исследования, позволило обосновать теоретические положения и выработать практические рекомендации.

**Теоретическую основу исследования составили** идеи и концепции, разработанные отечественными и зарубежными учеными в области административного и информационного права, а также в сфере государственного контроля и надзора. В процессе работы над диссертацией использовалась научная литература, посвященная различным аспектам и проблемам как административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в целом, так и административному и информационному праву в частности:

– исследование коллективом авторов (С. Е. Титор, Ф. Г. Мышко, В.В. Попов, Т. Н. Каменева, М. А. Горбунов), посвященное правовому регулированию защиты несовершеннолетних от деструктивной информационной среды, послужило основой для анализа характеристик деструктивного контента, компаративному анализу российского и зарубежного законодательства, определение механизмов имплементации положительного опыта в российское законодательство;

– коллективная монография Л. К. Терещенко, Н. С. Волкова, А. А. Ефремова, С. М. Зырянова «Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере» позволила провести детальный анализ понятий и содержаний информационной безопасности несовершеннолетних, в том числе в сети «Интернет».

– научные труды К. А. Шуликова, посвященные административно-правовым основам противодействия распространения деструктивного контента в сети «Интернет», послужили основой для анализа правовых конструкций «деструктивный контент», особенностей вопросов ответственности в изучаемой сфере правоотношений;

– научные труды И. А. Зайцева, раскрывающие разные аспекты административной ответственности в исследуемой диссертантом теме, в частности

некоторые научные выводы И. А. Зайцева, послужили основой для анализа и дискурса в части изменения возраста лиц, привлекаемых к административной ответственности в исследуемой сфере правоотношений.

**Нормативную основу диссертационного исследования** составили: Конституция РФ, российские правовые акты, зарубежное и международное законодательство в рассматриваемой области правоотношений.

**Эмпирическая основа диссертационного исследования** состоит из информационно-аналитических данных и судебной практики, российского, зарубежного и международного правового опыта и материалов официальных информационных источников российских и зарубежных органов публичной власти в сфере административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет», а также различных теоретических научных источников по исследуемой области общественных отношений, включая монографии, диссертации, научные публикации в периодических изданиях и материалы научных конференций.

**Научная новизна исследования** определяется тем, что исследование фундировано проведенным правовым анализом административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в России и зарубежных государствах. К элементам научной новизны относятся следующие теоретические и прикладные результаты диссертационного исследования:

- сформулированы авторские понятия «подросток», «информационная безопасность несовершеннолетних», «информационная безопасность несовершеннолетних в сети «Интернет»;
- выявлен правовой пробел в Федеральном законе от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»<sup>5</sup> в части отсутствия причинения вреда жизни несовершеннолетнего;
- проведен сравнительно-правовой анализ терминов «информационная

---

<sup>5</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

безопасность» и «кибербезопасность» в законодательствах и научных трудах; предложено авторское определение непосредственно в части информационной безопасности несовершеннолетних лиц и использования сети «Интернет»;

- установлены критерии участников информационной безопасности несовершеннолетних лиц в сети «Интернет» в русле предложенного авторского понятия «информационная безопасность несовершеннолетних в сети «Интернет»;

- обоснована авторская классификация деструктивного контента для несовершеннолетних в сети «Интернет»;

- выявлено, что перечень субъектов (административных органов публичной власти), которые уполномочены осуществлять контроль (надзор) за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию несовершеннолетним согласно ст. 20 Федерального закона № 436-ФЗ, является неполным;

- установлено, что в России отсутствует специализированная структура в составе Роскомнадзора, направленная на обеспечение информационной безопасности несовершеннолетних в сети «Интернет»;

- установлено, что отсутствует правовой механизм подтверждения при регистрации в социальных сетях в сети «Интернет» несовершеннолетних граждан и административная ответственность в этой сфере;

- обоснована правовая позиция, что с учетом значимости и значительного развития добровольчества (волонтерства) в сфере обеспечения информационной безопасности в сети «Интернет» следует дополнить ч. 1 ст. 2. Федерального закона от 11.08.1995 № 135-ФЗ<sup>6</sup> еще одной целью, связанной именно с этой деятельностью добровольцев (волонтеров).

### **Основные положения, выносимые на защиту**

**1.** Предложены авторские определения понятий «подросток» и «малолетний ребенок» в российском праве, которые определяют термин «несовершеннолетний».

---

<sup>6</sup> Федеральный закон от 11.08.1995 № 135-ФЗ (ред. от 28.12.2024) «О благотворительной деятельности и добровольчестве (волонтерстве)» // СЗ РФ. 1995. № 33. Ст. 3340; СЗ РФ. 2024. № 53 (часть I). Ст. 8564.



Проведен анализ правовых понятий «несовершеннолетний», «ребенок», «малолетний», «подросток» и их соотношений в юридической науке и в законодательстве. Использование термина «подросток» отражает динамичное правовое положение «несовершеннолетних», которых, по нашему мнению, следует подразделить на «малолетний ребенок» и «подросток». Предлагается авторское определение:

*«Малолетний ребенок – гражданин или лицо без гражданства в возрасте до 14 лет, правовой статус которого определяется дееспособностью малолетних и полным отсутствием деликтоспособности»;*

*«Подросток – это гражданин или лицо без гражданства в возрасте от 14 до 18 лет, правовой статус которого определяется частичной дееспособностью и деликтоспособностью».*

Внесение понятий «малолетний ребенок» и «подросток» во второй абзац статьи 1 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»<sup>7</sup> будет способствовать унификации указанной терминологии в законодательстве.

2. Разработана авторская классификация контента, наносящего вред жизни, здоровью и развитию несовершеннолетнего (деструктивного контента) в сети «Интернет», согласно которой выделен:

1) *незаконный (запрещенный) контент международного уровня*, представленный общепринятым противоправным контентом;

2) *незаконный (запрещенный или ограниченный) контент национального, наднационального уровня*, представленный противоправной информацией, распространение которой, в том числе в сети «Интернет», запрещено согласно национальным законодательствам и (или) наднациональным законодательствам. Этот вид контента в значительной мере обусловлен историко-культурными особенностям государств, действующими нормативными актами. Незаконный контент национального (наднационального) уровня может быть запрещен к

---

<sup>7</sup> Федеральный закон от 24.07.1998 № 124-ФЗ (ред. от 30.11.2024) «Об основных гарантиях прав ребенка в Российской Федерации» // СЗ РФ. 1998. № 31. Ст. 3802; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

распространению или же иметь ограничения по возрастным критериям (откровенный контент или содержащий сцены жестокости);

3) *нежелательный (вредоносный) контент* – контент, который не указан в законодательно закреплённых перечнях деструктивного контента государств, но из оценки которого выявляется, что этот контент представляет опасность причинения значительного вреда несовершеннолетним.

3. Предложено авторское определение: «информационная безопасность несовершеннолетних представляет собой состояние защищённости физических лиц (граждан и лиц без гражданства), не достигших возраста 18 лет, обеспечиваемое комплексом правовых средств, направленных на защиту несовершеннолетних лиц и их прав от воздействия на них информации, причиняющей вред их жизни, здоровью или развитию».

4. Предложено и обосновано авторское определение: «информационная безопасность несовершеннолетних в сети «Интернет» представляет собой состояние защищённости лиц, не достигших возраста 18 лет, от информации, обращение которой в сети «Интернет» правовыми актами признаётся запрещённым». Обеспечение информационной безопасности несовершеннолетних в сети «Интернет» – это деятельность административных органов публичной власти и частных лиц, связанная с применением:

- административными органами публичной власти мер государственного принуждения;

- частными лицами мер, направленных на мониторинг контента, правовое воспитание несовершеннолетних; повышение родительских компетенций в сфере безопасного поведения детей в сети «Интернет»; проведение мероприятий, направленных на повышение грамотности детей по вопросам информационной безопасности в сети «Интернет».

5. Установлено, что в России отсутствует административный орган публичной власти или его структурное подразделение, основное направление деятельности которых было бы направлено непосредственно на обеспечение информационной безопасности несовершеннолетних в сети «Интернет».

Обоснована целесообразность в структуре Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) создания Управления по информационной безопасности несовершеннолетних, полномочия которого предложены в диссертационном исследовании.

6. Предложен правовой механизм подтверждения возраста лиц при регистрации в социальных сетях несовершеннолетних граждан и меры административной ответственности в этой сфере. Данный правовой механизм и административная ответственность фундируются на обязанностях владельца социальных сетей в информационно-телекоммуникационной сети «Интернет» при регистрации пользователя провести идентификацию и (или) аутентификацию его возраста и удостовериться, что физическое лицо достигло подросткового возраста (четырнадцати лет), за исключением случаев регистрации в государственных и (или) муниципальных образовательных социальных сетях, регистрация в которых разрешена с 6,6 лет с согласия родителей (законных представителей) регистрируемого лица; также для целей регистрации пользователя в социальной сети владелец социальной сети принимает разумные меры для подтверждения возраста физического лица; нарушение владельцем социальных сетей в сети «Интернет» требований настоящей статьи влечет за собой административную ответственность.

7. Обосновано, что в целях обеспечения информационной безопасности несовершеннолетних в сети «Интернет», а именно защиты от информации, причиняющей вред их жизни, здоровью и развитию, законодательно необходимо ввести административную ответственность за неисполнение владельцем социальной сети обязанности по идентификации и (или) аутентификации достижения пользователем 14 лет при регистрации (за исключением случаев регистрации в государственных и (или) муниципальных образовательных социальных сетях, регистрация в которых разрешена с 6,6 лет с согласия родителей (законных представителей) регистрируемого несовершеннолетнего лица)).

**8.** Обосновано, что регистрация малолетнего ребенка (то есть лица, не достигшего четырнадцатилетнего возраста) в социальной сети в информационно-телекоммуникационной сети «Интернет» (не являющейся государственной и (или) муниципальной образовательной социальной сетью), с использованием недостоверных, заведомо ложных или не принадлежащих малолетнему лицу персональных (в том числе биометрических) данных – влечет меры административной ответственности.

**Теоретическая значимость исследования** заключается в следующем:

– настоящее диссертационное исследование является одной из первых комплексных системных научных работ в сфере административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет»;

– предложен новый объект правовой охраны – «жизнь», которому может быть причинен вред от информации наравне со здоровьем и развитием несовершеннолетнего лица – в текст, в том числе в название Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

– представлена авторская классификация контента, наносящего вред жизни, здоровью и развитию несовершеннолетнему (деструктивного контента) в сети «Интернет», разработанная на основе анализа российского и зарубежного законодательства в этой сфере;

– в расширение теоретико-правовых представлений в исследуемой сфере предложены авторские определения понятий «малолетний ребенок», «подросток»; «информационная безопасность несовершеннолетних», «информационная безопасность несовершеннолетних в сети «Интернет».

**Практическая значимость исследования** обусловлена следующим:

– предложен правовой механизм подтверждения возраста пользователя при регистрации в социальных сетях в сети «Интернет» и меры административной ответственности в этой сфере;

– предложено учредить специализированную структуру в составе

Роскомнадзора, полномочия которой были бы направлены на обеспечение информационной безопасности несовершеннолетних в сети «Интернет»;

– выводы диссертанта могут быть использованы органами публичной власти в нормативно-правовом регулировании сферы информационных технологий и массовых коммуникаций;

– разработаны и обоснованы предложения по совершенствованию российского законодательства в сфере административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет».

По результатам проведенного диссертационного исследования разработаны предложения по внесению изменений в административное и информационное законодательство, а именно:

– предложено законодательно закрепить авторские определения «малолетний (ребенок)» и «подросток» во втором абзаце статьи 1 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

– предложен новый объект правовой охраны – «жизнь», которому может быть причинен вред от информации наравне со здоровьем и развитием несовершеннолетнего лица. Обоснована целесообразность изложения названия Федерального закона от 29.12.2010 № 436-ФЗ в следующем виде: «О защите детей от информации, причиняющей вред их *жизни*, здоровью и развитию»;

– дополнить Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» статьей «10.8. Обязанности владельца социальных сетей в информационно-телекоммуникационной сети «Интернет»;

– дополнить КоАП РФ<sup>8</sup> следующей статьей: «Статья 6.17.1. Регистрация пользователя социальной сети в информационно-телекоммуникационной сети «Интернет» без идентификации и (или) без аутентификации возраста пользователя;

---

<sup>8</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404

– дополнить частями 4 и 5 ст. 5.35 «Неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по содержанию и воспитанию несовершеннолетних» КоАП РФ.

Результаты диссертационного исследования могут быть использованы в образовательном процессе при преподавании учебных дисциплин «Административное право», «Правовое обеспечение информационной безопасности» и в научной деятельности при подготовке научных работ по научной специальности «Публично-правовые (государственно-правовые) науки». Значимость результатов диссертационного исследования состоит также в дальнейшем совершенствовании законодательства, регулирующего обеспечение информационной безопасности несовершеннолетних в сети «Интернет».

**Степень достоверности и апробация результатов исследования.** Диссертация подготовлена и предназначена для обсуждения на кафедре административного и финансового права юридического института ФГАОУ ВО «Российский университет дружбы народов имени Патриса Лумумбы». Достоверность исследования подтверждается использованием актуальных и многочисленных нормативных правовых актов, теоретических трудов российских и зарубежных исследователей, материалов судебной практики. По теме диссертации опубликовано 8 научных статей в научных журналах, входящих в перечень ведущих научных изданий, рекомендованных ВАК при Министерстве науки и высшего образования РФ. Основные положения и результаты исследования были представлены и обсуждались в рамках следующих научных конференций: XII Международная научно-практическая конференция «Глобализация, деглобализация и публичное право» (Москва, РУДН, 2023); XIII Международная научно-практическая конференция «Глобализация, деглобализация и публичное право» (Москва, РУДН, 2024); международная научная конференция студентов и молодых ученых «Право на пути к устойчивому развитию» (Москва, РУДН, 2025).

**Соответствие паспорту научной специальности.** Тема исследования и разработанные научные положения, охватывающие вопросы административно-правового обеспечения информационной безопасности несовершеннолетних в сети

«Интернет», соответствуют пунктам 13, 19, 25 направления исследований специальности 5.1.2. «Публично-правовые (государственно-правовые) науки».

**Структура диссертации** обусловлена целью и задачами исследования. Диссертационное исследование состоит из введения, трех глав, в состав которых входят девять параграфов, заключения, списка литературы и приложений.

# **Глава 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ «ИНТЕРНЕТ»**

## **1.1. Понятие «несовершеннолетний» в юридической науке, российском и зарубежном законодательстве**

Трансформация, актуализация и унификация понятийного аппарата в современной правовой науке является необходимой составляющей развития и совершенствования как юридической науки в целом, так и в частности непосредственно правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в России и зарубежных государствах. Несомненно, что в понятийно-терминологическом аппарате юридической науки в настоящее время существует множество проблем, в особенности это отсутствие общепринятых определений и «проблема синонимии»<sup>9</sup>; наличие смысловых (ментальных) архаизмов, которые в том числе были ранее заимствованы из норм международного права; возникновение сложностей и субъективизма правоприменения. Рассмотрим более детально плюрализм понятий «ребенок», «несовершеннолетний» и «подросток» в правовых нормах. Так, в нормах частного и публичного российского права несовершеннолетние являются «носителями особого правового статуса ввиду возрастных и психофизических особенностей»<sup>10</sup>. Разумеется, специфика отрасли права формирует различные правовые механизмы регулирования правоотношений с участием несовершеннолетних<sup>11</sup>.

---

<sup>9</sup> Бурдин К. К. Понятийный аппарат как точка роста юридической науки и практики // Теория и практика общественного развития. 2024. № 7 (195). С. 175-180.

<sup>10</sup> Хромова Н. М. Правовой статус несовершеннолетних: частный и публичный аспекты // Российская юстиция. 2024. № 8. С. 23-34.

<sup>11</sup> Хромова Н. М. Трансформация правового статуса несовершеннолетних с древнейших времен до наших дней // Черные дыры в российском законодательстве. 2020. № 2. С. 36-39.



Правовые основы статуса несовершеннолетнего отдельно не закреплены в Конституции РФ<sup>12</sup>, а устанавливаются исходя из основных положений конституционно-правового статуса личности<sup>13</sup>. Конституция РФ не дает определения несовершеннолетним лицам, только указывая в ст. 67.1, ст. 38, 39, что таким лицом считается «ребенок» или «дети». Руководствуясь конституционными нормами (ч. 4 ст. 15), рассмотрим статью 1 Конвенции о правах ребенка, в которой дано общее понятие «ребенок» для всех категорий лиц, «не достигших совершеннолетнего возраста, то есть до достижения 18-летнего возраста, если законом он не достигает совершеннолетия ранее»<sup>14</sup>. Аналогичный подход представлен и в более ранних декларациях, таких как Женевская Декларация прав ребенка 1924 года<sup>15</sup>, которая зафиксировала положения о правах ребенка, и Декларация прав ребенка 1959<sup>16</sup> года: отсутствует четкая терминология, понятие «ребенок» не уточняется и не разделяется на отдельные категории. Таким образом, эти акты нормативно только закрепляют само понятие «ребенок».

Вернемся к нормам национального законодательства. Так, нормотворческий подход, который использован в Конституции РФ и в Конвенции о правах ребенка, заключающийся в том, что к исследуемой категории относятся лица до 18 лет и применение термина «ребенок» (как единственное число) и «дети» (как множественное число) также использовано и в иных актах, составляющих правовую систему России. Так, в ст. 1 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» дано общее понятие, что «ребенок – лицо до достижения им возраста 18 лет

<sup>12</sup> Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 06.10.2022.

<sup>13</sup> Дегтярева Л. Н. Конституционно-правовая защита несовершеннолетних в современной России (на примере Центрального федерального округа) : дис. ... канд. юрид. наук : 12.00.02. Елец, 2010. С. 24.

<sup>14</sup> Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989, вступила в силу для СССР 15.09.1990) // Сборник международных договоров СССР. Выпуск XLVI, 1993 (в дополнение к документу приняты Факультативные протоколы от 25.05.2000, вступившие в силу для России).

<sup>15</sup> Geneva Declaration of the Rights of the Child of 1924. URL: <https://www.humanium.org/en/text-2> (дата обращения: 01.05.2025) (не ратифицирована).

<sup>16</sup> Декларация прав ребенка (Принята 20.11.1959 Резолюцией 1386 (XIV) на 841-м пленарном заседании Генеральной Ассамблеи ООН) // Международная защита прав и свобод человека. Сборник документов. М. : Юридическая литература, 1990. С. 385-388 (не ратифицирована).

(совершеннолетия)»<sup>17</sup>. При этом, в дальнейших определениях, например, в законодательно закреплённых понятиях торговли детьми и эксплуатации детей (ст. 1 ФЗ № 124-ФЗ от 24.07.1998) понятия «ребенок (дети)» синонимичны понятию «несовершеннолетний». Несомненно, что дефинитивная конструкция фундирована конвенционным определением 1989 года<sup>18</sup>. В Федеральном законе от 29.12.2010 № 436-ФЗ исследуемые нами понятия используются, но не раскрываются<sup>19</sup>. В Федеральном законе от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» представлено понятие «несовершеннолетний» как лицо, не достигшее возраста 18 лет (ст. 1)<sup>20</sup>.

Можно сказать, что коррелирующим признаком в вышеуказанных понятиях выступает именно момент достижения совершеннолетия, то есть возраста 18 лет.

Семейный кодекс РФ в ч. 1 ст. 54 закрепляет, что «ребенком признается лицо, не достигшее возраста восемнадцати лет (совершеннолетия)»<sup>21</sup>. Таким образом, можно сделать вывод, что и Федеральный закон № 124-ФЗ, и СК РФ лишь только приняли уже существующее понятие из международного законодательства.

Считаем важным уточнить, что семейная отрасль права рассматривает понятие «ребенок» как двухаспектное правовое понятие: 1) непосредственно как лицо, соответствующее возрастной градации (0–18 лет) – то есть как специального субъекта семейного права, что отражено в ст. 54–60, 67–79 СК РФ; 2) обозначение генетической (биологической), иными словами, родственной связи (ст. 85, 87–88 СК РФ). При этом следует уточнить, что второй аспект не получил отражения в законодательном определении понятия «ребенок». Как точно отметила Е. А. Усачева, «в рамках одного нормативного акта один и тот же термин используется многовариантно. Статьи 85, 87, 88 СК РФ, употребляя понятие

<sup>17</sup> Федеральный закон от 24.07.1998 № 124-ФЗ (ред. от 30.11.2024) «Об основных гарантиях прав ребенка в Российской Федерации» // СЗ РФ. 1998. № 31. Ст. 3802; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>18</sup> Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989, вступила в силу для СССР 15.09.1990) // Сборник международных договоров СССР. Выпуск XLVI, 1993.

<sup>19</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>20</sup> Федеральный закон от 24.06.1999 № 120-ФЗ (ред. от 08.08.2024) «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» // СЗ РФ. 1998. № 31. Ст. 3802; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>21</sup> Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ (ред. от 23.11.2024) // СЗ РФ. 1996. № 1. Ст. 16; Российская газета. 27.11.2024. № 269.

«дети», уточняют, что это дети совершеннолетние. Такая комбинация сама по себе делает невозможным применение при толковании указанных норм дефиниции п. 1 ст. 54 СК РФ»<sup>22</sup>. На наш взгляд, понятие «ребенок (дети)» с акцентированием именно на биологическое родство (а не по факту достижения определенного возраста) обозначено в статье в п. «ж. 1)» ч. 1 ст. 72 Конституции РФ, устанавливающей совместное ведение РФ и субъектов РФ создания условий для достойного воспитания семьями детей, а также обязанность совершеннолетних детей заботиться о своих родителях. Иными словами, законодатель использует в этом случае понятие «совершеннолетние дети», что, по нашему мнению, по возрастному критерию противоречит при буквальном трактовании нормы (дефиниции) ст. 54 СК РФ. Аналогичная конструкция имеется и в ч. 3 ст. 38 Конституции РФ, которая устанавливает, что трудоспособные дети, достигшие 18 лет, должны заботиться о нетрудоспособных родителях.

Приведем и иные примеры подобных правовых конструкций в российском законодательстве: 1) в ч. 3, ч. 4, ч. 5 ст. 1.1 и далее по тексту (ст. 4, 5, 9, 9.1) Закона РФ № 4301-1 от 15.01.1993 используются следующие понятия: «дети в возрасте до 18 лет, дети старше 18 лет, ставшие инвалидами до достижения ими возраста 18 лет, и дети в возрасте до 23 лет, обучающиеся в организациях, осуществляющих образовательную деятельность, по очной форме обучения)»<sup>23</sup>; 2) согласно п. «а» ч. 2 Указа Президента РФ от 11.03.2020 № 180 установленные указом выплаты получают «дети в возрасте до 18 лет, дети старше 18 лет, ставшие инвалидами до достижения ими возраста 18 лет, и дети в возрасте до 23 лет, обучающиеся по очной форме обучения в организациях, осуществляющих образовательную деятельность)»<sup>24</sup>; 3) пункт «ж) ежемесячная выплата на каждого ребенка в возрасте

<sup>22</sup> Усачева Е. А. Понятие «ребенок» в категориальном аппарате семейно-правового регулирования // Законы России: опыт, анализ, практика. 2016. № 8. С. 40-43.

<sup>23</sup> Закон РФ от 15.01.1993 № 4301-1 (ред. от 29.05.2024) «О статусе Героев Советского Союза, Героев Российской Федерации и полных кавалеров ордена Славы» // Российская газета. 10.02.1993. № 27; СЗ РФ. 2024. № 23 (часть I). Ст. 3055.

<sup>24</sup> Указ Президента РФ от 11.03.2020 № 180 «О дополнительных мерах социальной защиты некоторых категорий граждан Российской Федерации» // Собрание законодательства РФ. 2020. № 11. Ст. 1530.

до 18 лет или до 23 лет (при условии обучения по очной форме)» части 2 Постановления Правительства РФ от 02.09.2022 № 1547<sup>25</sup>.

Таким образом, несмотря на законодательно закреплённую дефиницию «ребёнок – лицо до достижения им возраста 18 лет (совершеннолетия)»<sup>26</sup>, законодательно используется и иные возрастные признаки «ребёнка (детей), такие как «дети старше 18 лет, ставшие инвалидами до достижения ими возраста 18 лет» и «дети в возрасте до 23 лет, обучающиеся по очной форме обучения в организациях, осуществляющих образовательную деятельность».

В ГК РФ законодатель уже вводит категории несовершеннолетних: 1) малолетние, не достигшие 14 лет; 2) несовершеннолетние в возрасте от 14 до 18 лет<sup>27</sup>. Иными словами, вводя разграничение по возрастному критерию, законодатель акцентирует внимание на возникновении прав и обязанностей отдельных категорий по мере их взросления (ст. 26 и 28 ГК РФ).

Обратимся к нормам трудового права, а именно возникновению трудовой дееспособности у лиц, достигших возраста шестнадцати лет (ст. 63 ТК РФ<sup>28</sup>); в то же время ст. 20 ТК РФ и ст. 63 ТК РФ предусматривают и снижение указанного возраста. С учётом наличия у несовершеннолетнего трудовой правосубъектности, имеется и процессуальная дееспособность для защиты интересов в суде<sup>29</sup>. Однако ст. 391 ТК РФ предоставляет право обращения работника в суд, но не определяет возраст несовершеннолетних работников, которые могут обратиться в суд за разрешением споров.

На основании вышеизложенного анализа норм частного права можно сделать вывод, что правовой статус субъектов гражданского процессуального права (в том

---

<sup>25</sup> Постановление Правительства РФ от 02.09.2022 № 1547 «О порядке предоставления выплат гражданам Донецкой Народной Республики, Луганской Народной Республики, Украины и лицам без гражданства, вынужденно покинувшим территории Донецкой Народной Республики, Луганской Народной Республики, Украины и прибывшим на территорию Российской Федерации» // СЗ РФ. 2022. № 37. Ст. 6343.

<sup>26</sup> Федеральный закон от 24.07.1998 № 124-ФЗ (ред. от 30.11.2024) «Об основных гарантиях прав ребёнка в Российской Федерации» // СЗ РФ. 1998. № 31. Ст. 3802; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>27</sup> Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024, с изм. от 31.10.2024) // СЗ РФ. 1994. № 32. Ст. 3301; СЗ РФ. 2024. № 33 (Часть I). Ст. 4933.

<sup>28</sup> Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 28.12.2024) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 3; СЗ РФ. 2024. № 53 (Часть I). Ст. 8551.

<sup>29</sup> Гражданский процесс: учебник для студентов высших юридических учебных заведений / Отв. ред. В. В. Ярков. 10-е изд., перераб. и доп. М. : Статут, 2017. С. 70.

числе и несовершеннолетних) связывается с наличием гражданской процессуальной правоспособности, которая возникает с момента рождения и прекращается в момент смерти, и гражданской процессуальной дееспособностью, принадлежащей в полном объеме гражданам, достигшим возраста 18 лет (ч. 1 ст. 37 ГПК РФ)<sup>30</sup>. Однако ч. 4 ст. 37 ГПК РФ устанавливает исключение, так как лица в возрасте от 14 до 18 лет вправе лично защищать в суде свои права, свободы и законные интересы по делам, возникающим из гражданских, семейных, трудовых и иных правоотношений (суд вправе привлекать к участию в подобных делах законных представителей несовершеннолетних).

Рассмотрим публичный аспект правового статуса несовершеннолетних в российском законодательстве. Так, УК РФ в ч. 1 ст. 87 признает лиц, которым ко времени совершения преступления исполнилось 14, но не исполнилось 18 лет – несовершеннолетними<sup>31</sup>. Частью 1 ст. 20 УК РФ обозначено, что понятие «несовершеннолетний» подразделяется на две категории, в зависимости от наступления последствий по преступлению: 1) лицо, достигшее на момент совершения преступления 16 лет; 2) лицо в возрасте от 14 лет до момента совершеннолетия. По аналогии с гражданской правоспособностью уголовная возникает с рождения лица и заканчивается его смертью, а также реализуется через положения УПК РФ<sup>32</sup>, регламентирующие случаи, когда потерпевшим (ч. 2 ст. 45 УПК РФ с учетом положений п. 8 Постановления Пленума ВС РФ № 17 от 29.06.2010<sup>33</sup>) или подозреваемым и обвиняемым (ст. 48, 426 и 428 УПК РФ) является несовершеннолетнее лицо, а именно устанавливает необходимость обязательного привлечения законных представителей данного несовершеннолетнего лица. Иными словами, можно сделать вывод, что нормы УПК

<sup>30</sup> Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 28.12.2024) // СЗ РФ. 2002. № 46. Ст. 4532; СЗ РФ. 2024. № 53 (Часть I). Ст. 8531.

<sup>31</sup> Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025) // СЗ РФ. 1996. № 25. Ст. 2954; СЗ РФ. 2025. № 9. Ст. 860.

<sup>32</sup> Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 28.02.2025) // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921; СЗ РФ. 2025. № 9. Ст. 842.

<sup>33</sup> Постановление Пленума Верховного Суда РФ от 29.06.2010 № 17 (ред. от 16.05.2017) «О практике применения судами норм, регламентирующих участие потерпевшего в уголовном судопроизводстве» // Российская газета. 07.07.2010. № 147; Российская газета. 24.05.2017. № 110.

РФ не предусматривают в уголовном процессе самостоятельного участия несовершеннолетнего лица.

Российское законодательство имеет дифференцированный подход к установлению уголовно-правовой деликтоспособности: 1) лица до 14 лет не подлежат уголовной ответственности; 2) по общему правилу привлекаются к уголовной ответственности лица с 16 лет (ч. 1 ст. 20 УК РФ); 3) устанавливается исключение из общего правила согласно ч. 2 ст. 20 УК РФ: при совершении преступления согласно исчерпывающему перечню, лицо привлекается к ответственности от 14 до 16 лет. Следует отметить, что недостижение установленного законом возраста на момент совершения преступления полностью исключает уголовную ответственность (ч. 2 ст. 9 УК РФ и п. 5 Постановления Пленума ВС РФ № 1 от 01.02.2011)<sup>34</sup>.

Нормы уголовного законодательства о возрасте, с которого наступает уголовная ответственность, полностью коррелируются с п. 4.1 Минимальных стандартных правил ООН, касающихся отправления правосудия в отношении несовершеннолетних<sup>35</sup>, согласно которым установление минимального возраста лиц, привлекающихся к уголовной ответственности, должно учитывать аспекты эмоциональной, духовной и интеллектуальной зрелости. Как отмечает З. А. Астемиров, «...несовершеннолетние в возрасте от 14 до 18 лет, с одной стороны, достигают уже достаточно высокого уровня социализации (у них появляется самостоятельность, настойчивость, умение контролировать своё поведение, владеть собой), с другой – происходит дальнейшая социализация личности»<sup>36</sup>. Можно сказать, что именно вышеуказанные аспекты обусловили дифференцированный подход к установлению уголовно-правовой деликтоспособности в российском праве.

---

<sup>34</sup> Постановление Пленума Верховного Суда РФ от 01.02.2011 № 1 (ред. от 28.10.2021) «О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних» // Российская газета. 11.02.2011. № 29; Российская газета. 12.11.2021. № 257.

<sup>35</sup> Минимальные стандартные правила Организации Объединенных Наций, касающиеся отправления правосудия в отношении несовершеннолетних («Пекинские правила») (приняты 29 ноября 1985 г. Резолюцией 40/33 на 96-м пленарном заседании Генеральной Ассамблеи ООН) // Советская юстиция. 1991. №№ 12-14; Сайт ООН. URL: [https://www.un.org/ru/documents/decl\\_conv/conventions/beijing\\_rules.shtml](https://www.un.org/ru/documents/decl_conv/conventions/beijing_rules.shtml) (дата обращения: 27.03.2025).

<sup>36</sup> Астемиров З. А. Уголовная ответственность и наказание несовершеннолетних. М., 1970. С. 20.

Административное право, как и уголовное, также относится к публичному праву и обладает схожими с уголовным правом задачами (ст. 1.2 КоАП РФ<sup>37</sup>). Административная правоспособность, идентичная с уголовной и гражданской, возникает с рождения и заканчивается со смертью. В административном праве, как и в уголовном, не предусмотрено самостоятельного участия несовершеннолетних в административно-юрисдикционном производстве.

В отношении лиц, не достигших совершеннолетия, предусмотрен особый порядок рассмотрения дел об административных правонарушениях и применения административных санкций: возникает особая подведомственность – дела рассматриваются комиссией по делам несовершеннолетних и защите их прав (ч. 3 ст. 1.3 КоАП РФ). Впрочем, имеется, как отмечает В. М. Емельянов, «существенный недостаток действующего административного законодательства. Этим недостатком является отсутствие достаточно четко регламентированного отличия правового статуса несовершеннолетнего от правового статуса совершеннолетних лиц, при производстве по делу об административном правонарушении. Это, в свою очередь, затрудняет обеспечение их законных прав и интересов в должной мере»<sup>38</sup>.

Рассмотрим деликтоспособность несовершеннолетних в административном праве. Так, согласно ч. 1 ст. 2.3 КоАП РФ административной ответственности подлежит лицо, достигшее к моменту совершения административного правонарушения возраста 16 лет. Иными словами, согласно нормам административного права несовершеннолетним признается физическое лицо в возрасте от 16 до 18 лет.

Административная деликтоспособность возникает с 16 лет, так как привлекаться к административной ответственности может только лицо, которое на момент совершения правонарушения достигло 16 лет. В ином случае производство по делу об административном правонарушении в отношении указанного лица не

---

<sup>37</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404.

<sup>38</sup> Емельянов В. М. Правовое положение несовершеннолетнего в административно-юрисдикционном производстве // Правопорядок: история, теория, практика. 2019. № 3 (22). С. 6-11.

может быть начато, а начатое производство подлежит прекращению на основании п. 2 ч. 1 ст. 24.5 КоАП РФ. Как в этом контексте отмечает Н. М. Хромова, «...до наступления указанного возраста лицо, совершившее административное правонарушение, считается малолетним»<sup>39</sup>. Для нас в приведенной цитате вызывает особый интерес использованный в рамках публичного права автором термин «малолетний», так как этот термин закреплен и используется, как правило, в рамках частного права.

Следует различать административную ответственность и ответственность в административном праве, так как «административная ответственность» – это юридическая ответственность в соответствии с КоАП РФ, а ответственность в административном праве – юридическая ответственность как по КоАП РФ, так и дисциплинарная ответственность в публичных учреждениях.

Рассмотрим вопрос о дисциплинарной ответственности несовершеннолетних в публичных учреждениях РФ.

Так, в ч. 4 ст. 43 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»<sup>40</sup> установлено, что за нарушение (неисполнение) положений устава и правил внутреннего распорядка образовательного учреждения, правил проживания в общежитиях и интернатах и иных локальных нормативных актов по вопросам организации и осуществления образовательной деятельности к обучающимся могут быть применены меры дисциплинарного взыскания – замечание, выговор, отчисление из организации, осуществляющей образовательную деятельность.

Согласно ч. 5 ст. 43 федерального закона № 273-ФЗ меры дисциплинарного взыскания не применяются к обучающимся по образовательным программам дошкольного, начального общего образования, а также к обучающимся с ограниченными возможностями здоровья (с задержкой психического развития или нарушением интеллекта). То есть, иными словами, меры дисциплинарного

---

<sup>39</sup> Хромова Н. М. Правовой статус несовершеннолетних: частный и публичный аспекты // Российская юстиция. 2024. № 8. С. 23-34.

<sup>40</sup> Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 28.02.2025) «Об образовании в Российской Федерации» // СЗ РФ. 2012. № 53 (ч. 1). Ст. 7598; СЗ РФ. 2025. № 9. Ст. 859.



взыскания применяются к обучающимся по образовательным программам начиная с основного общего образования (5–9 классы, что примерно соответствует 10–12 годам, в зависимости от года поступления в школу (6–8 лет). Согласно ст. 67 Федерального закона от 29.12.2012 №273-ФЗ (ред. от 28.02.2025) «Об образовании в Российской Федерации» в первый класс принимают детей от 6,6 до 8 лет. В порядке исключения могут принять детей другого возраста, для чего понадобится разрешение учредителя школы. Применение мер дисциплинарного взыскания к несовершеннолетнему обучающемуся по образовательным программам, начиная с основного общего образования (от 10 лет), является одним из видов административно-правового принуждения.

Дисциплинарное принуждение по административному праву – это отраслевой вид административно-правового принуждения, а дисциплинарное принуждение в целом (в широком смысле) – межотраслевой вид государственного принуждения. Меры дисциплинарного воздействия применяются на основе, в том числе, норм административного права – к членам административных коллективов (военнослужащим, сотрудникам полиции, учащимся, студентам и др.)<sup>41</sup>. Дисциплинарное принуждение по административному праву можно определить как совокупность предусмотренных административным и административно-процессуальным законодательством приемов, средств и способов организационного, психического, физического, материального, процессуального воздействия на сознание и поведение членов организованных коллективов в случаях нарушения ими социальных норм с целью их понуждения к должному поведению, обеспечения применения дисциплинарных взысканий либо соблюдения установленных запретов и ограничений<sup>42</sup>.

Согласно толкованию норм п. 2 ст. 1074 ГК РФ, ст. 32.2 КоАП РФ, ч. 2 ст. 88 УК РФ, ст. 399 УПК РФ и п. 21 Постановления Пленума Верховного Суда РФ № 1

---

<sup>41</sup> Бахрах Д. Н. Дисциплинарно-правовое принуждение в Российской Федерации // Государство и право. 2006. № 6. С. 46.

<sup>42</sup> Лещина Э. Л. Дисциплинарное принуждение по административному праву: понятие, признаки, структура // Вестник Нижегородского университета им. Н. И. Лобачевского. 2018. № 1. С. 87-95.

от 01.02.2011<sup>43</sup> штраф (возмещение материального вреда), назначенный несовершеннолетнему лицу, у которого отсутствует самостоятельный доход, может быть взыскан с его родителей или иных законных представителей. При этом существует мнение И. В. Черненко<sup>44</sup>, А. В. Бриллиантова<sup>45</sup>, О. Н. Петровой<sup>46</sup>, что подобные нормы нарушают принцип личной ответственности лица, совершившего правонарушение. Однако правило о субсидиарной ответственности несовершеннолетних лиц и их законных представителей обосновано ч. 2 ст. 38 Конституции РФ<sup>47</sup>, в которой обозначена конституционная обязанность родителей по воспитанию детей.

В региональном законодательстве, как правило, исследуемые понятия либо не раскрываются, либо повторяют дефиницию федерального законодательства. Рассмотрим несколько примеров. Так, например, Закон г. Москвы от 23.11.2005 № 60 применяет, но не раскрывает понятий «ребенок», «дети», «несовершеннолетний»<sup>48</sup>. Интересным уточнением отличался утративший уже юридическую силу Закон Республики Коми от 19 ноября 1996 г. № 36-РЗ, в ст. 2 которого было указано, что «дети (ребенок) – лица (лицо) в возрасте до 18 лет» (ст. 2)<sup>49</sup>. Отметим, что в законе как раз было зафиксировано общепринятое трактование<sup>50</sup>, что «дети» и «ребенок» – тождественные понятия, отличающиеся

<sup>43</sup> Постановление Пленума Верховного Суда РФ от 01.02.2011 № 1 (ред. от 28.10.2021) «О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних» // Российская газета. 11.02.2011. № 29; Российская газета. 12.11.2021. № 257.

<sup>44</sup> Черненко И. В. Особенности лишения свободы на определенный срок для несовершеннолетних // Вестник Кемеровского государственного университета. 2006. № 1. С. 17.

<sup>45</sup> Бриллиантов А. В. Новые особенности уголовной ответственности и наказания несовершеннолетних // Российский судья. 2004. № 2. С. 13.

<sup>46</sup> Петрова О. Н. Роль наказания в превенции преступности несовершеннолетних в свете изменений Уголовного кодекса Российской Федерации // Преступность как она есть и направления антикриминальной политики. М., 2004. С. 155-160.

<sup>47</sup> Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 06.10.2022.

<sup>48</sup> Закон г. Москвы от 23.11.2005 № 60 «О социальной поддержке семей с детьми в городе Москве» (ред. от 20.10.2021) // Ведомости Московской городской Думы. 29.12.2005. № 12(2). Ст. 293; URL: <https://base.garant.ru/384375/> (дата обращения: 01.05.2025).

<sup>49</sup> Закон Республики Коми от 19 ноября 1996 г. № 36-РЗ «О защите прав детей в Республике Коми». URL: <https://base.garant.ru/27300328/> (дата обращения: 01.05.2025).

<sup>50</sup> Балашова Т. Н. Соотношение понятий «ребенок» и «несовершеннолетний» в законодательстве Российской Федерации / Закон и право. 2019. № 11. С. 32-36; Жукова Т. А., Сайфуллина Н. А. Соотношение понятий «ребёнок», «несовершеннолетний», «малолетний», «подросток», «дети» в юридической науке // Наука и инновации в современном мире : сб. научных статей. М., 2018. С. 249-254; Яхина Н. Д., Тулупова Е. О. Понятие «несовершеннолетний» в законодательстве Российской Федерации. Соотношение с понятием «ребенок» // E-Scio. 2022. № 10 (73). С. 635-641 и др.

лишь количественным признаком. Аналогичные определения «детство» и «дети (ребенок)» указаны и в Законе Приморского края от 29.12.2004 № 217-КЗ «О защите прав ребёнка в Приморском крае»<sup>51</sup>. Таким образом, можно сделать вывод о том, что и на региональном уровне нет четких и унифицированных границ в понятиях «дети», «ребенок», «малолетний», «несовершеннолетний».

В русле нашего правового исследования интересным является тот факт, что не только понятия «ребенок (дети)» и «несовершеннолетние» на федеральном и региональном уровнях не имеют однозначных понятий, но также применяется и понятие «подросток». Так, в Законе РФ № 1244-1 от 15.05.1991 имеется статья 25, которая уже своим названием – «Меры социальной поддержки детей и подростков» – вводит на законодательном уровне разграничение понятий «дети» и «подростки»<sup>52</sup>. Отметим, что в абз. 1 ст. 1 указано: «и подростков в возрасте до 18 лет» – то есть имеется возрастной критерий (аналогично указано и в ст. 4, ст. 27.1); далее в абз. 5 ст. 1 обозначено: «Детям и подросткам, страдающим болезнями вследствие чернобыльской катастрофы» – то есть уже без уточнения возрастных ограничений до 18 лет. Также разграничение терминов «дети» и «подростки» указаны в Письме Роспотребнадзора от 16.05.2007 № 0100/4960-07-32 «О действующих нормативных и методических документах по гигиене детей и подростков»<sup>53</sup>, в Решении Коллегии Евразийской экономической комиссии от 13.12.2022 № 195 «О порядке введения в действие изменений в технический регламент Таможенного союза «О безопасности продукции, предназначенной для детей и подростков» (ТР ТС 007/2011)»<sup>54</sup>.

---

<sup>51</sup> Закон Приморского края от 29.12.2004 № 217-КЗ «О защите прав ребенка в Приморском крае» (в ред. 1 марта 2023) // Ведомости Законодательного Собрания Приморского края. 29.12.2004. № 84.

<sup>52</sup> Закон РФ от 15.05.1991 № 1244-1 (ред. от 25.12.2023) «О социальной защите граждан, подвергшихся воздействию радиации вследствие катастрофы на Чернобыльской АЭС» // Ведомости СНД и ВС РСФСР. 1991. № 21. Ст. 699; СЗ. 2024. № 1 (часть I). Ст. 3.

<sup>53</sup> Письмо Роспотребнадзора от 16.05.2007 № 0100/4960-07-32 «О действующих нормативных и методических документах по гигиене детей и подростков». М. : Федеральный центр гигиены и эпидемиологии Роспотребнадзора, 2007; СПС «КонсультантПлюс».

<sup>54</sup> Решение Коллегии Евразийской экономической комиссии от 13.12.2022 № 195 «О порядке введения в действие изменений в технический регламент Таможенного союза «О безопасности продукции, предназначенной для детей и подростков» (ТР ТС 007/2011)» // Официальный сайт ЕЭС. URL: <https://docs.eaeunion.org/documents/399/7129/> (дата обращения: 03.03.2025).

В ч. 1 Распоряжения Правительства РФ от 28.04.2023 № 1105-р используется термин «дети», а в самой Концепции информационной безопасности детей в РФ, которая утверждена распоряжением Правительства РФ от 28.04.2023 № 1105-р, уже имеется разграничение «дети» и «подростки». Так, в абз. 4–5 раздела I указано: «...нестабильность эмоциональной сферы и низкий уровень критичности восприятия и обработки информационного потока детьми и подростками свидетельствуют о том, что именно дети и подростки находятся в группе потенциального риска для негативного воздействия»<sup>55</sup>.

Проанализируем далее мнения ученых-правоведов по вопросу исследования этого параграфа. Ряд авторов (например, Н. В. Комбаров<sup>56</sup>, А. В. Токарева<sup>57</sup>) утверждают, что «дети» – всего лишь множественное число понятия «ребенок», не относя его к отдельному термину.

В юридической науке принято считать, что «ребенок» – понятие универсальное, то есть общее, которое применяется к несовершеннолетнему лицу. Так, А. Р. Бахман<sup>58</sup>, В. В. Белозерцева<sup>59</sup>, С. А. Ветошкин<sup>60</sup> рассматривают это понятие как общее и утверждают, что дети являются самостоятельными субъектами права, не достигшими совершеннолетнего возраста. Заслуживает внимания двухаспектное понимание термина «ребенок» И. Бандурка: первым признаком понятия выступает возрастная характеристика и юридически признанные и значимые кровные связи с родителями; вторым признаком выступает «повышенная защищенность», которая выражается в том, что в нормативно-правовых актах уже совершеннолетнее лицо может быть названо «ребенком»<sup>61</sup>. По нашему мнению,

<sup>55</sup> Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СЗ РФ. 2023. № 19. Ст. 3481.

<sup>56</sup> Комбаров Н. В. Институт прав и свобод ребенка: понятие, содержание, признаки. СПб. // Ленинградский юридический журнал, 2009. С. 87.

<sup>57</sup> Токарева А. В. Подходы к трактовке понятий «несовершеннолетний» и «ребенок» в конституционном праве Российской Федерации // Наука и мир. 2015. № 9. С. 171-173.

<sup>58</sup> Бахман А. Р. Об актуальности создания детского кодекса в России // Вестник Томского государственного университета. 2011. № 352. С. 120-122.

<sup>59</sup> Белозерцева В. В. Доступ несовершеннолетнего к правосудию, как неотъемлемое право человека // Вестник Восточно-Сибирского института МВД России. 2024. № 3 (110). С. 9-18.

<sup>60</sup> Ветошкин С. А. Ювенальное право : уч. пос. Екатеринбург : ГОУ ВПО, 2009. С. 229.

<sup>61</sup> Бандурка И. Понятие ребенка в национальном законодательстве и международно-правовых документах // Закон и жизнь. 2015. № 8. С. 36.

такое понятие «ребенка» свойственно именно отрасли семейного права. По мнению Д. К. Амировой, термин «несовершеннолетний» является менее широким понятием, чем универсальный термин «ребенок», так как является отраслевым понятием и непосредственно возрастным критерием; также понятия («несовершеннолетний» и «малолетний») могут быть основой для фундирования самостоятельных видов правового статуса»<sup>62</sup>. В. И. Абрамова указывает, что правовое понятие «ребенок» является не просто более широким по отношению к понятиям «малолетний», «подросток», «несовершеннолетний», но и включает их в себя<sup>63</sup>. Однако в научных трудах достаточно часто понятия «ребенок» и «несовершеннолетний» являются тождественными<sup>64</sup>. К примеру, А. В. Токарева отождествляет понятия «ребенок» и «несовершеннолетний», но при этом отмечает, что термин «несовершеннолетний» относится именно к правовым терминам, а термин «ребенок» используется в основном в семейном праве, но в то же время активно используется и в других областях знаний, помимо юридической науки<sup>65</sup>. Аналогичного подхода придерживается и Г. А. Трофимова<sup>66</sup>.

По мнению Н. М. Хромовой, по объему предоставленной законом дееспособности несовершеннолетних можно разделить на три группы: 1) малолетние до 6 лет (полностью недееспособные); 2) малолетние от 6 до 14 лет («недееспособности с исключениями» (наличие отдельных элементов дееспособности и неделиктоспособности); 3) несовершеннолетние от 14 до 18 лет<sup>67</sup>. Интересной является позиция Е. А. Усачевой, предлагающей отказаться от использования для обозначения специального правового статуса термина «ребенок» в чистом виде в пользу категории «несовершеннолетний ребенок», под

<sup>62</sup> Амирова Д. К. Понятие «ребёнок» в категориальном аппарате уголовно-правового регулирования: проблемы законодательной регламентации и совершенствования // Вестник Казанского юридического института МВД России. 2022. № 4 (50). С. 40–46.

<sup>63</sup> Абрамов В. И. Права ребенка в России (теоретический аспект) / Под ред. Н. И. Матузова. Саратов : СГАП, 2005. 324 с.

<sup>64</sup> Капитонова Е. А. Конституционные обязанности ребенка в Российской Федерации : автореф. дис. ...канд. юрид. наук. Пенза, 2010. 26 с.; Токарева А. В. Подходы к трактовке понятий «несовершеннолетний» и «ребенок» в конституционном праве Российской Федерации // Наука и мир. 2015. № 9. С. 171-173.

<sup>65</sup> Токарева А. В. Подходы к трактовке понятий «несовершеннолетний» и «ребенок» в конституционном праве Российской Федерации // Наука и мир. 2015. № 9. С. 171-173.

<sup>66</sup> Трофимова Г. А. Совершеннолетний ребенок: пробелы в правовом статусе // Адвокат. 2014. № 8. С. 67-72

<sup>67</sup> Хромова Н. М. Правовой статус несовершеннолетних: частный и публичный аспекты // Российская юстиция. 2024. № 8. С. 23-34.

которым Е. А. Усачева понимает «лицо, не достигшее возраста восемнадцати лет и не приобретшее полной гражданской дееспособности по иным основаниям»<sup>68</sup>. К правоведам, которые обосновывают термин «подросток», можно отнести О. В. Садину, по мнению которой малолетним считается лицо в возрасте до 14 лет, а подросток – в возрасте от 14 до 18 лет<sup>69</sup>. А. П. Солдатов указывает конкретные возрастные критерии разграничения понятий «малолетний» и «подросток»: к первой категории относятся несовершеннолетние лица до 10 лет, а ко второй – несовершеннолетние лица в возрасте от 10 до 14 лет. Основным критерием в этом случае выступает возраст, так как по мере взросления у человека возникают новые права и обязанности<sup>70</sup>. Нам ближе подход О. В. Садиной, поскольку и в ее авторской терминологии, и в положениях ст. 26 и 28 ГК РФ выделяется дееспособность малолетних (лиц, не достигших 14 лет) и дееспособность несовершеннолетних в возрасте от 14 до 18 лет, таким образом, не указывая точную формулировку определения термина для лиц от 14 до 18 лет. Часто встречается позиция авторов научных работ, которые разделяют понятия «дети (ребенок)» и «подростки», «молодежь», но не конкретизируют их и не приводят авторских понятий (Т. В. Обыденова<sup>71</sup>).

На наш взгляд, на основании приведенного анализа законодательства и различных мнений правоведов, понятия «малолетний (ребенок)» и «подросток» входят в состав понятия «несовершеннолетний». Можно сделать вывод, что единообразный подход к изучаемой терминологии в доктрине российского права отсутствует, несмотря на то, что определения употребляемых понятий играют важную роль в определении прав и обязанностей, которыми обладают несовершеннолетние определенного возраста.

<sup>68</sup> Усачева Е. А. Понятие «ребенок» в категориальном аппарате семейно-правового регулирования // Законы России: опыт, анализ, практика. 2016. № 8. С. 40-43.

<sup>69</sup> Садина О. В. Правовой статус несовершеннолетнего в российском законодательстве: теоретико-правовой. Мытищи, 2010. С. 20.

<sup>70</sup> Солдатов А. П. Гарантии и обеспечение прав в границах местного самоуправления. Славянск-на-Кубани : СГПИ, 2015. 387 с.

<sup>71</sup> Обыденова Т. В. Правовое регулирование административной ответственности несовершеннолетних // Административное и муниципальное право. 2012. № 6. С. 67-69.

Рассмотрим законодательство зарубежных государств (Австралии и Великобритании, Франции и иных некоторых государств ЕС, начиная с надгосударственных европейских норм и постепенно переходя к анализу наиболее интересных в рамках изучаемой темы правовых актов).

Законодательно в Австралии совершеннолетним считается лицо после достижения 18 лет (ст. 5 Закона 1974 «О достижении совершеннолетия»<sup>72</sup> в редакции 2011 года), при этом закон понятий «несовершеннолетний» или «совершеннолетний» не раскрывает, обозначая лишь возрастной критерий. Кроме того, согласно (2) ст. 6 вышеуказанного закона имеется уточнение, что с учетом положений раздела (2) 7 выражения «совершеннолетие» («majority»), «достижение совершеннолетия» («full age»), «sui juris», «несовершеннолетний» («minor»), «несовершеннолетие» («minority»), «младенец» («infant»), «младенчество» («infancy»), «несовершеннолетний» («nonage») и любые подобные выражения, используемые в законе, должны толковаться в соответствии со ст. 5. Таким образом, аналогично с российским законодательством, в австралийском «ребенком» считается лицо, не достигшее 18 лет, согласно ратифицированной Австралией в 1990 году Конвенции ООН о правах ребенка 1989 года. Данный нормотворческий подход отражен в отраслевых законах: к примеру, законы Нового Южного Уэльса иллюстрируют вышесказанное ст. 3 Закона о детях (уголовное судопроизводство) 1987 г.<sup>73</sup>, Законом о залоге 2013 г. (ст. 4)<sup>74</sup>. Интересно, что в двух законах 1987 года (ст. 3 закона о детях (общественные работы) и ст. 3 закона о детских центрах содержания под стражей)<sup>75</sup> имеется определение ребенка как лица, не достигшего 18-летнего возраста, однако, по единому законодательству о

<sup>72</sup> Age of Majority Act 1974 (amendments A2011-3 of 1 March 2011) // The Age of Majority Ordinance 1974 was notified in the Commonwealth Gazette on 24 October 1974 (Cwlth Gaz 1974 No 87A). URL: <https://www.legislation.act.gov.au/a/1974-46/Default.asp?show=full> (дата обращения: 21.07.2025).

<sup>73</sup> Children (Criminal Proceedings) Act 1987 No 55 (NSW). URL: <https://www.legislation.nsw.gov.au/view/pdf/asmade/act-1987-55> (дата обращения: 21.07.2025).

<sup>74</sup> The Bail Act 2013 No 26 (NSW). URL: <https://legislation.nsw.gov.au/view/pdf/asmade/act-2013-26> (дата обращения: 21.07.2025).

<sup>75</sup> Children (Community Service Orders) Act 1987 No 56. URL: <https://legislation.nsw.gov.au/view/whole/html/inforce/2016-01-15/act-1987-056> (дата обращения: 21.07.2025); Children (Detention Centres) Act 1987 No 57. URL: <https://legislation.nsw.gov.au/view/html/inforce/2023-07-14/act-1987-057> (дата обращения: 21.07.2025).

доказательствах, «ребенок» определяется как «ребенок любого возраста» (ст. 3, словарь, часть 1 Закона о доказательствах 1995 года)<sup>76</sup>.

При этом присутствует и дифференцированный возрастной критерий при определении несовершеннолетнего лица: в ст. 4 Закона Нового Южного Уэльса о несовершеннолетних правонарушителях 1997 года определено, что «ребенком» считается «лицо, достигшее возраста 10 лет (возраст наступления уголовной ответственности) или превышающее его, но не достигшее 18 лет»<sup>77</sup>.

Понятие «подросток» в австралийском законодательстве не получило четкого определения, но закреплено в примечании к ст. 3 Закона о детях и подростках (опеке и защите) 1998 г., в которой разграничены понятия «ребенок» («лицо, не достигшее 16 лет») и «подросток» («лицо в возрасте от 16 лет до 18 лет»)<sup>78</sup>. Аналогичный подход представлен и в Законе о преступлениях (домашнее и личное насилие) 2007 г., согласно которому «ребенком» считается лицо в возрасте до 16 лет<sup>79</sup>.

Также в ряде законов, посвященных несовершеннолетним, предусмотрены особые условия судопроизводства для лиц, не достигших 21-летнего возраста: 1) если преступление совершено лицом до 21 года, то рассматривается дело Судом по делам детей (ст. 28 Act 2007)<sup>80</sup>; если обвинительное решение вынесено лицу до 21 года, но достигшему 18 лет на момент совершения им преступления, то такое лицо может быть приговорено к отбыванию любого срока тюремного заключения в исправительном учреждении для несовершеннолетних, а не во взрослой тюрьме (ст. 19 Act 2007); 2) лицу, которому на момент совершения правонарушения не исполнилось 21 года, предусмотрен альтернативный судебный процесс (вынесение предупреждений и предостережений) (ст. 7A Закона о несовершеннолетних

<sup>76</sup> Evidence Act 1995 No 25 (NSW). URL: <https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1995-025> (дата обращения: 21.07.2025).

<sup>77</sup> Young Offenders Act 1997 No 54 (NSW). URL: <https://legislation.nsw.gov.au/view/pdf/asmade/act-1997-54> (дата обращения: 21.07.2025).

<sup>78</sup> Children and Young Persons (Care and Protection) Act 1998 No 157 (NSW). URL: <https://legislation.nsw.gov.au/view/whole/whole/html/inforce/2014-07-04/act-1998-157> (дата обращения: 21.07.2025).

<sup>79</sup> Crimes (Domestic and Personal Violence) Act 2007 No 80 (NSW). URL: <https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2007-080> (дата обращения: 21.07.2025).

<sup>80</sup> Children (Criminal Proceedings) Act 1987 No 55 (NSW). URL: <https://www.legislation.nsw.gov.au/view/pdf/asmade/act-1987-55> (дата обращения: 21.07.2025).



правонарушителях<sup>81</sup>). Таким образом, в австралийском законодательстве достаточно часто используется сочетание понятий «дети и подростки» или «ребенок и подросток».

В Великобритании возраст совершеннолетия составляет также 18 лет согласно ст. 1 (1) Family Law Reform Act 1969<sup>82</sup>. При этом отметим, что возраст уголовной ответственности в Англии, Уэльсе составляет 10 лет. Дети в возрасте до 11 лет могут быть направлены к социальному работнику и в комиссию по делам несовершеннолетних. Непосредственно возрастной градации понятие «несовершеннолетний» законодательство Великобритании не содержит. В законе, регламентирующем обеспечение информационной безопасности в сети «Интернет» (Online Safety Act<sup>83</sup>), в части (1) ст. 236 указано, что «ребенок означает лицо, не достигшее 18-летнего возраста».

Институты ЕС, в том числе Европейская комиссия, в своих сообщениях о правах ребенка часто ссылаются на Конвенцию ООН как на основу стандартов для всех государств – членов ЕС, так как все они являются участниками Конвенции ООН о правах ребенка. Следовательно, можно сделать вывод, что ЕС определяет ребенка согласно нормам Конвенции ООН о правах ребенка<sup>84</sup>, рассмотренной нами ранее. Так, под совершеннолетием понимается достижение лицом возраста, в котором ребенок (подросток) становится взрослым и приобретает полную дееспособность, то есть может заниматься юридической деятельностью и нести ответственность по любым договорным обязательствам. Во всех государствах – членах ЕС совершеннолетие наступает в 18 лет<sup>85</sup>.

<sup>81</sup> Young Offenders Act 1997 No 54. URL: <https://legislation.nsw.gov.au/view/whole/html/inforce/2020-10-27/act-1997-054> (дата обращения: 21.07.2025).

<sup>82</sup> Family Law Reform Act 1969. URL: <https://www.legislation.gov.uk/ukpga/1969/46/section/1> (дата обращения: 21.07.2025).

<sup>83</sup> Online Safety Act 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50> (дата обращения: 21.07.2025).

<sup>84</sup> Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989, вступила в силу для СССР 15.09.1990) // Сборник международных договоров СССР. Выпуск XLVI, 1993 (в дополнение к документу приняты Факультативные протоколы от 25.05.2000, вступившие в силу для России).

<sup>85</sup> Age of Majority by Country 2025. URL: <https://worldpopulationreview.com/country-rankings/age-of-majority-by-country> (дата обращения 30.03.2025); Письмо ФНП от 22.07.2016 № 2668/03-16-3 «О Методических рекомендациях по удостоверению доверенностей» (вместе с «Методическими рекомендациями по удостоверению доверенностей», утв. решением Правления ФНП от 18.07.2016, протокол N 07/16) // СПС «КонсультантПлюс».

Если несовершеннолетний становится родителем или вступает в брак до достижения совершеннолетия, в некоторых государствах – членах ЕС он получает полную дееспособность. В других государствах – членах ЕС дети, вступившие в брак, получают лишь частичную дееспособность<sup>86</sup>. Например, они больше не подчиняются родительскому контролю и могут действовать в соответствии со своими личными потребностями, но им может быть запрещено распоряжаться недвижимым имуществом или брать займы. В некоторых государствах – членах ЕС для детей, ставших родителями, назначается опекун<sup>87</sup>.

Правовую проблему, выраженную в отсутствии единообразного подхода к понятиям «ребенок» и «несовершеннолетний» в правовых актах в ЕС, отметил в научной работе S. Trotter (С. Троттер). Так, в различных актах, как национальных, так и наднациональных, используется множество понятий, таких как «ребенок», «несовершеннолетний», «подросток», «юный взрослый», «молодой человек», «молодежь», «лицо, не достигшее возраста уголовной ответственности», «лицо, условно подлежащее уголовной ответственности» и т. д.<sup>88</sup> Ряд зарубежных авторов отмечают, что несомненными недостатками Конвенции ООН о правах ребенка<sup>89</sup>, во-первых, является «напряженность в рамках такой расплывчатой и открытой нормы, которая является гибкой, но трудной для интерпретации и применения на практике в настоящее время» в отношении презумпции, что дети являются независимыми правообладателями и что в силу своего развития, особой зависимости и уязвимости они нуждаются в особых правах, гарантирующих гуманное обращение и уважение человеческого достоинства с учетом их возраста и зрелости<sup>90</sup>. Во-вторых, в Концепции придания должного значения взглядам ребенка в соответствии с его возрастом и зрелостью (ст. 12(1)) и развивающимися способностями ребенка (ст. 5) допускаются разные толкования и подвергаются

<sup>86</sup> Aitken S. C. Global Crises of Childhood: rights, justice and the unchildlike child // *Area*. 2001. № 33(2). P. 119-127.

<sup>87</sup> Age of majority. FRA: the EU's Rights Agency. URL: <https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/age-majority> (дата обращения 30.03.2025)

<sup>88</sup> Trotter S. The Child in European Human Rights Law // *Modern Law Review*. 2018. № 81(3). P. 452-479.

<sup>89</sup> Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989, вступила в силу для СССР 15.09.1990) // Сборник международных договоров СССР. Выпуск XLVI, 1993 (в дополнение к документу приняты Факультативные протоколы от 25.05.2000, вступившие в силу для России).

<sup>90</sup> Freeman M. A Commentary on the United Nations Convention on the Rights of the Child, Article 3: The Best Interests of the Child. Martinus Nijhoff, First Edition (February 23, 2007). 79 p.

рассмотрению такими авторами, как А. Дейли (A. Daly), К. Хансон (K. Hanson), Е. К. М. Тисдалл (E. K. M. Tisdall), Э. Десмет (E. Desmet), Д. Рейнаерт (D. Reynaert), С. Лембрехтс (S. Lembrechts), Т. Лифаард (T. Liefwaard), критике за то, что они дают мало ориентиров для государства и реализации на практике<sup>91</sup>. В связи с этим Тобин указывает на отсутствие консенсуса относительно значения конкретных прав детей и баланса между защитой и автономией, который необходимо установить<sup>92</sup>. К. Hollingsworth (К. Холлингсуорт) объясняет, что закон должен быть направлен на обеспечение развития ребенка, который будет постепенно становиться самостоятельным субъектом правоотношений – способствовать становлению детей как полностью автономных правообладателей<sup>93</sup>. По мнению Ст. Рэп (Stephanie Rap), дети рассматриваются как «развивающиеся человеческие существа, что отличает их от взрослых и заслуживает особого отношения к ним со стороны закона», а при этом «рекомендации Комитета ООН по правам ребенка не всегда ясны и последовательны»<sup>94</sup>; также отметим, что сама рассматриваемая Концепция, по мнению ряда зарубежных правоведов<sup>95</sup>, не имеет основательной теоретической основы и не в полной мере отражает динамичное правовое положение несовершеннолетних.

<sup>91</sup> Daly A. No Weight for “Due Weight”? A Children’s Autonomy Principle in Best Interest Proceedings // 26 The International Journal of Children’s Rights 61. 2018; Hanson K. Children’s Participation and Agency When They Don’t “Do the Right Thing”, 23 // Child-hood 471. 2016; Tisdall E. K. M. Children and Young People’s Participation: A Critical Consideration of Article 12’ // W. Vandenhoe, E. Desmet, D. Reynaert and S. Lembrechts (eds.). Routledge International Handbook of Children’s Rights Studies. 2015. P. 185; Liefwaard T. Juvenile Justice from an International Children’s Rights Perspective // W. Vandenhoe, E. Desmet, D. Reynaert and S. Lembrechts (eds.). Routledge International Handbook of Children’s Rights Studies. 2015. P. 234.

<sup>92</sup> Tobin J. Understanding a Human Rights Based Approach to Matters Involving Children: Conceptual Foundations and Strategic Considerations // A. Invernizzi and J. Williams (eds.), The Human Rights of Children: From Visions to Implementation. 2011. 61, at 78; а также схожая точка зрения отражена у Hanson, Schools of Thought in Children’s Rights // M. Liebel, K. Hanson, I. Saadi and W. Vandenhoe (eds.). Children’s Rights from Below: Cross-Cultural Perspectives. 2012. 63, at 70.

<sup>93</sup> Hollingsworth K. Theorising Children’s Rights in Youth Justice: The Significance of Autonomy and Foundational Rights // The Modern Law Review. 2013. 1046 (76), at 1060.

<sup>94</sup> Rap S. Safeguarding the Dynamic Legal Position of Children: A Matter of Age Limits? // Erasmus Law Review. 2020. Vol. 1. P. 4-12.

<sup>95</sup> Tobin J. Seeking to Persuade: A Constructive Approach to Human Rights Treaty Interpretation // Harvard Human Rights Journal. 2010. Vol. 23. P. 1 (1-50 p.); Freeman M. Why It Remains Important to Take Children’s Rights Seriously // The International Journal of Children’s Rights. 2007. Vol. 15(1). P. 5-23; Freeman M. Taking Children’s Rights More Seriously // International Journal of Law and the Family. 1992. Vol. 6 (52). P. 59; Eekelaar J. The Emergence of Children’s Rights // Oxford Journal of Legal Studies. 1986. Vol. 6(161). P. 170-171; Hanson K., Peleg N. Waiting for Children’s Rights Theory // International Journal of Children’s Rights. 2020. Vol. 28 (15). P. 1-28; Hanson K., Peleg N. Waiting for Children’s Rights Theory // International Journal of Children’s Rights. 2020. Vol. 28 (1). P. 15-35.

Статья 24 Хартии ЕС об основных правах<sup>96</sup> закрепляет «права ребенка», декларирует право несовершеннолетних на защиту и заботу, приоритетность непосредственно интересов несовершеннолетних органами публичной власти или частными учреждениями, равнозначность родителей ребенка в вопросе взаимоотношений с ним. Статья 32 обозначенной Хартии фиксирует трудовые права несовершеннолетних (отметим, что в названии статьи использованы понятия «детский труд» и «молодые люди»), запрещая детский труд и устанавливая особые условия труда для молодых людей. Отметим, что при употреблении понятия «молодые люди» используется такой условный возрастной критерий, как «минимальный возраст приема на работу не может быть ниже того возраста, когда заканчивается период обязательного школьного образования». Этот возраст конкретизируется в ч. 3 ст. 2 Конвенции № 138 МОТ<sup>97</sup>, согласно которой возраст не должен быть ниже 15 лет. Отметим, что в этой Конвенции в ст. 1 и далее используется термин «подросток», без конкретизации дефиниций.

В национальных законодательствах государств – членов ЕС также в большинстве случаев не представлено универсального определения исследуемых терминов. Применение этих терминов варьируется в зависимости от нормативно-правового контекста и часто эти термины не определяются явно, но используются в разных положениях, которые устанавливают конкретный возрастной предел. Комитет по правам ребенка, который контролирует выполнение соглашения в соответствии с конвенцией подписавших соглашение государств, изложил «руководящие принципы» (недискриминация (ст. 2); наилучшее обеспечение интересов ребенка (ст. 3); обеспечение права на жизнь, выживание и развитие (ст. 6); уважение и учет взглядов и мнения ребенка (ст. 12))<sup>98</sup> того, как молодежь, подростки и дети младшего возраста должны быть защищены с помощью мер

<sup>96</sup> Хартия Европейского Союза об основных правах (Страсбург, 12 декабря 2007 г.) (2016/C 202/02) // СПС «Гарант». URL: <https://base.garant.ru/71672404/> (дата обращения: 21.07.2025).

<sup>97</sup> Конвенция № 138 Международной организации труда «О минимальном возрасте для приема на работу» [рус., англ.] (Заключена в г. Женеве 26.06.1973). URL: <https://base.garant.ru/2540542/> (дата обращения: 21.07.2025).

<sup>98</sup> Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989, вступила в силу для СССР 15.09.1990) // Сборник международных договоров СССР. Выпуск XLVI, 1993.

предосторожности в цифровом (электронном) мире, и каким образом должны быть защищены права этих лиц.

Термин «ребенок» широко используется во всех законодательных актах, начиная от законов о детях, уголовных кодексов, законов о социальном обеспечении, законов о защите детей, трудового законодательства и т. д. В большинстве законодательных актов это понятие относится ко всем детям младше 18 лет. Однако он также может использоваться для того, чтобы отличать детей младшего возраста от подростков, как в некоторых уголовных законах.

В научных работах используются термины «ребенок»<sup>99</sup>, «дети», «подростки», «несовершеннолетние» то как синонимы, то выделяя чаще всего оборот «дети и подростки» (Н. Пардей (N. Pardhey), Р. Т. Диас (R. T. Dias), М. Ирфан (M. Irfan), Р. М. Гальван (R. M. Galvão), М. Варела (M. Varela), Р. Рибейро (R. Ribeiro))<sup>100</sup>.

Четырнадцать государств – членов ЕС определяют «несовершеннолетний» в своих гражданских кодексах (ГК) как лицо в возрасте от 0 до 18 лет: Всеобщий гражданский кодекс Австрии (абз. 2 § 21 Австрии Allgemeines bürgerliches Gesetzbuch, ABGB<sup>101</sup>); Франция (ст. 388 ГК Франции (Code civil des Français), Люксембург (ст. 388 ГК; Code Civil. TITLE X.-Minority, guardianship and emancipation); ст. 233 раздел 13 Книги 1 ГК Нидерландов (Boek 1 van het Nederlandse Burgerlijk Wetboek Titel 13 Artikel 233). Согласно § 30 ГК Чешской Республики (Nr. 40/1964 GBl.) абзац 1 § 30 устанавливает, что дееспособность лица возникает в полном объеме с наступлением совершеннолетия, то есть 18 лет.

Понятие «молодежь» в законодательстве ЕС используется исключительно для обозначения лиц, которые старше 18 лет и, как правило, до 30 лет. Впрочем, в этом

<sup>99</sup> Stalford H. Introduction: The EU as a Children's Rights Actor: Law, Policy and Structural. The EU as a Children's Rights Actor. Publisher: Barbara Budrich publisher. 2015. 11 Pages.

<sup>100</sup> Pardhey N., Dias R. T., Irfan M., Galvão R. M., Varela M., Ribeiro R. 3.3 Children and youth rights in the digital era and environmental development through binding legal instruments / Insight Into Child and Youth Safety Online Via International Laws Edges // Revista de Gestão Social e Ambiental. 2024. № 18(9). P. 1-20.

<sup>101</sup> «Minderjährige sind Personen, die das achtzehnte Lebensjahr noch nicht vollendet haben; haben sie das vierzehnte Lebensjahr noch nicht vollendet, so sind sie unmündig» – Несовершеннолетними считаются лица, не достигшие восемнадцатилетнего возраста; если они не достигли четырнадцатилетнего возраста, то они малолетние. – Allgemeines bürgerliches Gesetzbuch or ABGB on 1 June 1811. URL: <https://www.jusline.at/gesetz/abgb/paragraf/21> (дата обращения: 01.05.2025).

вопросе также имеются правовые коллизии, а именно: согласно Декларации ООН<sup>102</sup> «молодежь» обозначает лиц от 15 до 24 лет, но из этого определения следует, что тогда понятие «ребенок» («дети») обозначает лиц до 15 лет, что не соответствует ст. 1 Конвенции ООН о правах ребенка, согласно которой «ребенок» («дети») обозначает лиц до 18 лет. Уточним, что понятие «молодежь» представлено и в Стратегии ЕС, согласно которой к молодежи относятся лица в возрасте от 13 до 30 лет<sup>103</sup>, а в официальной статистике Евростата используется возрастной критерий категории «молодежь» в рамках от 15 до 29 лет<sup>104</sup>.

В правовых актах рассматриваемых зарубежных государств понятие «подросток» применяется (без четкого определения) в общем комментарии № 20 о подростках<sup>105</sup>, в котором Комитет по правам ребенка фокусируется на возрастном периоде с 10 до 18 лет. Понятие «подросток» используется и в национальном законодательстве нескольких государств ЕС (Дания, Германия, Италия, Люксембург, Нидерланды). Например, в ряде нормативных документов и стратегии молодежной политики<sup>106</sup> Австрии используются термины «подростки» (с 14 до 18 лет) и «молодые взрослые» (с 18 до 30 лет). При этом в разных федеральных землях Австрии могут быть свои определения этих понятий. Например, в законах о защите молодежи земель Штирия, Каринтия, Зальцбург, Тироль и Форарльберг общее понятие «молодежь» делится на «детей» (лиц, не достигших 14 лет) и «подростков» (с 14 до 18 лет), а в законе Верхней Австрии понятие «дети» отсутствует<sup>107</sup>.

<sup>102</sup> Декларация о распространении среди молодежи идеалов мира, взаимного уважения и взаимопонимания между народами (принята резолюцией 2037 (XX) Генеральной Ассамблеи от 7 декабря 1965 года). URL: [https://www.un.org/ru/documents/decl\\_conv/declarations/youth\\_peace\\_ideals.shtml](https://www.un.org/ru/documents/decl_conv/declarations/youth_peace_ideals.shtml) (дата обращения: 30.03.2025).

<sup>103</sup> Молодежная политика: европейский опыт. Доклады ИЕ РАН № 163 / Отв. ред. А. Ю. Борка. М.: ИЕ РАН, 2005. 65 с.

<sup>104</sup> Children and youth. EU youth dashboard. URL: <https://ec.europa.eu/eurostat/web/children-youth/database/eu-youth-dashboard> (дата обращения: 30.03.2025).

<sup>105</sup> Замечание общего порядка №20 об осуществлении прав ребенка в подростковом возрасте. Конвенция о правах ребенка ООН. URL: <https://docs.un.org/ru/CRC/C/GC/20> (дата обращения: 30.03.2025).

<sup>106</sup> Österreichische Jugendziele 30. September 2020 wurden 28 (aller Bundesministerien beschlossen). URL: <https://www.bundeskanzleramt.gv.at/agenda/jugend/oesterreichische-jugendstrategie/jugendziele.html> (дата обращения: 01.05.2025).

<sup>107</sup> Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Bundes-Jugendvertretungsgesetz, Fassung vom 05.05.2025 / Bundesgesetz über die Vertretung der Anliegen der Jugend (Bundes-Jugendvertretungsgesetz) StF: BGBl. I Nr. 127/2000 (NR: GP XXI IA 270/A AB 351 S. 46. BR: 6253 und 6254 AB 6264 S. 670.), BGBl. I Nr. 136/2001. URL: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001059> (дата обращения: 01.05.2025).

Так, в Дании и Германии к подросткам относятся лица в возрасте от 14 до 18 лет, в Люксембурге и Италии – лица в возрасте от 15 до 18 лет (статья 1 Закона № 977/67 «О безопасности труда детей и подростков»<sup>108</sup>), в Нидерландах – лица в возрасте от 12 до 18 лет. В «Замечании общего порядка № 20 от 06.12.2016 об осуществлении прав ребенка в подростковом возрасте»<sup>109</sup> (условное обозначение: CRC/C/GC/20) ООН Комитет по правам ребенка признаёт, что подростковый возраст нелегко определить и что дети могут достигать зрелости в разном возрасте. Созревание мальчиков и девочек происходит в разном возрасте; в разное время развиваются и разные функции мозга. Процесс перехода от детства к взрослой жизни зависит от контекста и условий, что нашло свое отражение в значительных различиях культурных стереотипов подростков в национальных законодательствах, которые обеспечивают разные пороговые уровни для вступления во взрослую деятельность, а также во многих международных органах, которые используют разные возрастные категории для определения подросткового возраста.

Подростки в возрасте до 18 лет имеют все права, закрепленные в Конвенции; они имеют право на особые меры защиты и в соответствии со своими развивающимися способностями могут в прогрессивном порядке пользоваться своими правами (ст. 5). Подростковый возраст представляет собой уникальный определяющий этап в развитии человека, характеризующийся быстрым умственным развитием, что влияет на принятие рискованных решений, определенные процессы принятия решений и способность контролировать импульсы. По мнению Э. Десмет, возникает неоднозначная связь между Конвенцией о правах ребенка и молодежью. Учитывая пересечение целевых групп в области прав детей и молодежной политики, мы изучаем существующие и потенциальные связи между этими двумя направлениями политики, чтобы оценить, может ли (дальнейшее) объединение этих направлений политики (в области детей и в области подростков) способствовать реализации прав молодежи. В Концепции

<sup>108</sup> Legge 17 ottobre 1967, n. 977 Tutela del lavoro dei ((bambini)) e degli adolescent (Ultimo aggiornamento all'atto pubblicato il 14/03/2016) (GU n.276 del 06-11-1967). URL: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1967-10-17;977> (дата обращения: 30.03.2025).

<sup>109</sup> Замечание общего порядка № 20 (2016) об осуществлении прав ребенка в подростковом возрасте. URL: [https://fgbu-ac.ru/international\\_obligations/2/1/2\\_52.G1640448.pdf](https://fgbu-ac.ru/international_obligations/2/1/2_52.G1640448.pdf) (дата обращения: 30.03.2025).

есть верхний возрастной предел понятия «дети», что является предметом споров<sup>110</sup>. Можно сделать вывод, что в рамках усилий по реализации Конвенции о правах ребенка права и проблемы детей старшего возраста, также называемых «подростками», не получили такого же внимания, как права и проблемы детей младшего возраста<sup>111</sup>. Кроме того, в своем докладе «Положение детей в мире» детский фонд ООН (ЮНИСЕФ) за 2011 год переключил свое внимание с детей младшего возраста (0–9 лет) на подростков (10–19 лет)<sup>112</sup>. Несмотря на то, что конкретный возраст детей и подростков отличается, они подпадают под действие «молодежной политики». Как минимум, эта «пересекающаяся» группа» включает подростков в возрасте от 10–15 до 18 лет.

Рассмотрим соотношение понятий «ребенок» и «подросток», «несовершеннолетний» на примере национального немецкого законодательства как, по нашему мнению, наиболее полный и регламентированный пример в этой сфере правоотношений. Согласно § 1 Закона о защите молодежи (Jugendschutzgesetz (JuSchG))<sup>113</sup> детьми являются лица в возрасте до 14 лет, а подростками – лица в возрасте от 14 лет, но моложе 18 лет.

Согласно абз. (1) § 7 Восьмой книги Социального кодекса (SGB VIII)<sup>114</sup> представлены следующие определения: 1) «ребенок» – лицо до 14 лет; 2) «подросток» – лицо от 14 до 18 лет; 3) «молодой взрослый» – лицо, достигшее 18 лет, но до 27 лет; 4) «молодой человек» – лицо до момента достижения 27 лет. Уточним, что вышеуказанная терминология представлена в официальной русифицированной версии Международной молодежной службы ФРГ (International Youth Service of the Federal Republic of Germany (IJAB))<sup>115</sup>. Также уточним, что в

<sup>110</sup> Desmet E. Implementing the Convention on the Rights of the Child for ‘youth’: who and how? // International Journal of Children’s Rights. 2012. № 20. P. 3–23.

<sup>111</sup> Замечание общего порядка № 4 (2003) «Здоровье и развитие подростков в контексте Конвенции о правах ребенка» CRC/GC/2003/4 от 1 июля 2003 года. URL: <https://european-court-help.ru/zamechanie-obshhego-porjadka-4-2003-god-zdorove-i-razvitie-podrostkov-v-kontekste-konvencii-o-pravah-rebenka/> (дата обращения: 01.05.2025).

<sup>112</sup> The State of the World’s Children 2011. United Nations Children’s Fund (UNICEF). URL: <https://www.unicef.org/media/84876/file/SOWC-2011.pdf> (дата обращения: 01.05.2025).

<sup>113</sup> Jugendschutzgesetz vom 23. Juli 2002 (BGBl. I S. 2730), das zuletzt durch Artikel 12 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist. URL: <https://www.buzer.de/JuSchG.htm> (дата обращения: 28.03.2025).

<sup>114</sup> Sozialgesetzbuch (SGB VIII). URL: <https://www.sozialgesetzbuch-sgb.de/sgbviii/7.html> (дата обращения: 28.03.2025).

<sup>115</sup> International Youth Service of the Federal Republic of Germany. URL: <https://www.kinder-jugendhilfe.info/ru/obshchie-ramochnye-uslovia/obshchestvo/deti-podrostki-i-molodye-vzroslye> (дата обращения: 28.03.2025).



Законе Германии о защите молодежи от 23 июля 2002 г. (Jugendschutzgesetz)<sup>116</sup> в (1) § 1 есть два определения: 1) дети – это лица, которым еще не исполнилось 14 лет; 2) подростки – лица, которым уже исполнилось 14 лет, но еще не исполнилось 18 лет. Таким образом, в Германии существуют разные правовые основы для определения детей и подростков.

## **1.2. Правовая характеристика информации, причиняющей вред здоровью и развитию несовершеннолетних с помощью сети «Интернет», в российском законодательстве**

В современном мире информационных технологий, характеризующихся чрезвычайно интенсивным развитием цифровых правоотношений, информация приобретает статус жизненно необходимого ресурса как для общества, так и для государства и становится «ключевым понятием при исследовании явлений государственно-правовой жизни»<sup>117</sup>. В условиях продолжающейся в мировом масштабе информационной революции особую актуальность приобретает проблема правового регулирования общественных отношений в сфере информационных технологий<sup>118</sup>, в том числе с учетом правовых особенностей участников данных правоотношений. Создание, распространение и доступ к информации в настоящее время происходит в значительной степени посредством сети «Интернет». Стоит отметить, что вовлеченность несовершеннолетних в онлайн-среду достаточно высока. Так, по данным ООН по состоянию на 2023 г., 79 % несовершеннолетних активно пользовались сетью «Интернет» в целях получения различной информации<sup>119</sup>. Использование информационных ресурсов сети «Интернет» несовершеннолетними с каждым годом только возрастает, каждые

<sup>116</sup> Jugendschutzgesetz vom 23. Juli 2002 (BGBl. I S. 2730), das zuletzt durch Artikel 12 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist. URL: <https://www.buzer.de/JuSchG.htm> (дата обращения: 01.05.2025).

<sup>117</sup> Шарофода Р. Ш., Шокиров Г. А. Информация как объект юридического научного познания и правового воздействия // Правовая жизнь. 2021. № 3 (35). С. 5-22.

<sup>118</sup> Матвеев С. П. Актуальные проблемы реализации информационных прав граждан // Административное право и процесс. 2024. № 12. С. 29-33.

<sup>119</sup> Сайт ООН. Новые данные об использовании интернета в мире: прогресс есть, но различия сохраняются. URL: <https://www.ungeneva.org/ru/news-media/news/2023/11/87882/novye-dannye-ob-ispolzovanii-interneta-v-mire-progress-est-no> (дата обращения: 01.05.2025).

полсекунды в мире один малолетний или подросток выходит в сеть «Интернет»<sup>120</sup>.

На этом фоне международное сообщество и государства обеспокоены регламентацией того, какую именно информацию следует относить к деструктивно влияющей на развитие несовершеннолетних. Это действительно необходимо, так как в 30 государствах более трети подростков подвергаются оскорблениям и травле (кибербуллинг). Также в сети «Интернет» наличествует информация экстремистского и террористического характера (в том числе сопряженная с вербовкой школьников для подобных деяний), а также подстрекательство к самоубийству или членовредительству. Кроме того, приблизительно 80 % подростков в 25 государствах мира подвергаются сексуальному насилию или эксплуатации в сети «Интернет»<sup>121</sup>. Следовательно, государства уделяют повышенное внимание защите детства, ведь оно является важнейшим периодом в жизни каждого человека, в который начинает формироваться личность, поскольку внешние факторы в это время оказывают сильное влияние на несовершеннолетнего. Детство оказывает влияние на всю дальнейшую жизнь, поэтому значимо обеспечить людям такое детство, чтобы в будущем они стали здоровыми членами общества. Таким образом, при глобальном и публичном распространении различного контента в сети «Интернет» возникают риски для несовершеннолетних пользователей, так как их здоровью и развитию может причинить вред информация, содержащая чрезмерную жестокость, пропаганду насилия, порнографический контент в силу нестабильной эмоциональной сферы несовершеннолетних лиц, а также их еще низкого уровня ментального, критичного восприятия и анализа информации.

В истоке нашего исследования, посвященного характеристике информации, причиняющей вред здоровью и развитию несовершеннолетних в сети «Интернет», в российском и зарубежном законодательствах, следует кратко рассмотреть понятия «информация», «информационные права несовершеннолетних» и непосредственно «информация, наносящая вред развитию несовершеннолетних». Н. Н. Моисеев,

---

<sup>120</sup> Официальный сайт ООН. Безопасность детей и молодежи в Интернете. URL: <https://www.un.org/ru/global-issues/child-and-youth-safety-online> (дата обращения: 01.05.2025).

<sup>121</sup> Там же.

учитывая великое множество вариантов понимания информации, сделал вывод о том, что «в силу широты этого понятия нет и не может быть строгого и достаточно универсального определения информации»<sup>122</sup>. Тем не менее, обобщая имеющиеся в научных источниках дефиниции информации, можно выделить два сложившихся подхода к ее пониманию: в широком и узком смысле. В широком смысле информация – это весь окружающий человека мир во всем его многообразии. В узком смысле этого слова информация представляет собой сведения, получаемые индивидом посредством информационной связи. Для того чтобы информация стала объектом общественного правоотношения, необходимо соответствие ее определенным критериям: 1) информация должна быть не элементарным отражением окружающего нас мира (т.е. не информацией в широком понимании этого термина), а смысловым сигналом, предназначенным для других субъектов. Как справедливо отмечается в литературе, она «должна быть конкретизирована, «привязана» к ситуации...»<sup>123</sup>; 2) информация как объект правоотношений должна относиться к таким ее видам, которые «по своей природе могут поддаваться нормативно-организационному воздействию и в существующих условиях требуют такого воздействия»<sup>124</sup>.

Так, в российском законодательстве, а именно в п. 1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ обозначено, что «информация – сведения (сообщения, данные) независимо от формы их представления»<sup>125</sup>.

В ст. 2 Модельного закона «Об информации, информатизации и обеспечении информационной безопасности» государств – участников СНГ указано, что «информация – сведения или данные о фактах, событиях, явлениях, процессах независимо от способа их представления»<sup>126</sup>. На универсальном международном

<sup>122</sup> Моисеев Н. Н. Человек, наука и общество. М. : Наука, 1982. С. 74.

<sup>123</sup> Корнев А. В., Танимов О. В. Информационное право в условиях цифровой трансформации российского права : монография. М. : Проспект, 2024. С. 8.

<sup>124</sup> Алексеев С. С. Теория права. М. : Бек, 1995. С. 211.

<sup>125</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; СЗ РФ. 2024. № 48. Ст. 7218.

<sup>126</sup> Постановление № 41-15 Межпарламентской Ассамблеи государств-участников СНГ «О модельном законе «Об информации, информатизации и обеспечении информационной безопасности» (Принято в г. Санкт-Петербурге 28.11.2014) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. 2015. № 62 (часть 2).

уровне, в таких актах, как Всеобщая декларация прав человека 1948 г.<sup>127</sup>, Международный пакт о гражданских и политических правах 1966 г.<sup>128</sup>, Международный пакт о социальных, экономических и культурных правах 1966 г.<sup>129</sup>, используется понятие «информация» в контексте прав и свобод человека на получение и распространение информации без легальной трактовки самого понятия. Поэтому можно только согласиться с утверждением В. П. Иванского, что «до сих пор ни в юридической доктрине, ни в законодательстве, ни в международном праве не сложилось единого представления, что такое информация»<sup>130</sup>. Так, в законодательстве не дается описание отличительных признаков информации, но законодатель попытался ее охарактеризовать посредством других, по его мнению, однородных названий, используемых в правовых актах: сведения, данные, сообщение. Между тем найти в правовых актах обозначенные выше равнозначные термину «информация» названия не представляется возможным. Также имеется и иная проблема, заключающаяся в том, что с повсеместным внедрением применения технических вычислительных средств обработки и распространения данных, представленных в электронном виде, обнажились трудности в разграничении материального носителя и зафиксированных на нем физических знаков (символов), содержащих информацию. Иначе говоря, в юридической науке некоторыми учеными отождествляется носитель сведений как хранилище символов, выражающих информацию, с самой информацией<sup>131</sup>. Кроме того, как справедливо отмечает И. А. Демидова, отсутствие однозначности в определении понятия «информация»

<sup>127</sup> Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета 05.04.1995. № 67.

<sup>128</sup> Международный пакт о гражданских и политических правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-м пленарном заседании Генеральной Ассамблеи ООН) // Ведомости Верховного Совета СССР. 1976. № 17. Ст. 291; Бюллетень Верховного Суда РФ. 1994. № 12 (вступил в силу для СССР 23.03.1976).

<sup>129</sup> Международный пакт об экономических, социальных и культурных правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-м пленарном заседании Генеральной Ассамблеи ООН) // Ведомости Верховного Совета СССР. 1976. № 17. Ст. 291 (ратифицирован Указом Президиума ВС СССР от 18.09.1973 N 4812-VIII).

<sup>130</sup> Иванский В. П. Правовая сущность информации в условиях использования цифровых технологий // RUDN Journal of Law. 2025. Т. 29. № 1. С. 221–234.

<sup>131</sup> Там же.

мешает плодотворному развитию междисциплинарных связей и сдерживает развитие новых научных направлений<sup>132</sup>.

Считаем важным пояснить, что в нашем исследовании не будет представлен детальный анализ понятия «информация» ввиду ограниченного объема диссертационного исследования и многогранности, дискуссионности самого понятия «информация» в сфере правовых отношений.

В российском законодательстве право на информацию закреплено в ч. 4 ст. 29 Конституции РФ: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Тем не менее термин «право на информацию» не закреплен на уровне отраслевого законодательства (Закон об информации №149-ФЗ), поэтому судить о его содержании возможно только благодаря различным авторским трактовкам. Таким образом, на норме ст. 29 Конституции РФ фундируются и информационные права несовершеннолетних, которые являются субъективными и закрепляются в различных нормативно-правовых актах.

По мнению Л. А. Букалеровой, информационные права несовершеннолетних можно разделить на три группы: 1) возникающие из конституционных прав на информацию, например, из права получения информации, ее передачи; 2) право на защиту информации о несовершеннолетнем либо же информации у несовершеннолетнего лица; 3) права, которые связаны с защитой от воздействия деструктивного контента<sup>133</sup>. Целесообразно согласиться с мнением А. С. Пиголкина о назревшей потребности дополнить право на информацию рядом присущих информационному обществу конституционных прав, такими как свободой доступа гражданина к информационным технологиям и глобальному информационному пространству, права на защиту личной и иной конфиденциальной информации<sup>134</sup>.

---

<sup>132</sup> Демидова И. А. Понятие информации: теоретико-прикладной аспект // Актуальные вопросы развития правовой информатизации в условиях формирования информационного общества. Сборник научных статей / Под общей редакцией Е. И. Коваленко. Минск, 2017. С. 342-349.

<sup>133</sup> Букалерова Л. А. Защита прав и интересов детей в информационной сфере требует внимания // Вестник Московского университета им. С. Ю. Витте. Серия 2: Юридические науки. 2019. № 4 (22). С. 58.

<sup>134</sup> Глобализация и развитие законодательства. Очерки / Отв. ред. А. С. Пиголкин, Ю. А. Тихомиров. М. : Городец, 2004. 464 с.

Однако информационные права несовершеннолетних влекут за собой и вопросы как защиты этих прав, так и их ограничений. Например, согласно ч. 2 ст. 10 Европейской конвенции о защите прав человека и основных свобод<sup>135</sup> допускается в целях охраны здоровья, репутации, нравственности и т. д. установление ограничений свободы слова и (или) массового распространения информации. Аналогичное исключение из презумпции содержится и в ч. 2 ст. 29 и ст. 55 Конституции РФ.

Анализ интернет-угроз, проведенный «Лабораторией Касперского» показал, что в России каждый шестой пользователь модуля «Родительский контроль» сталкивался с порносайтами, четверть пользователей – с сайтами, посвященными азартным играм<sup>136</sup>. Отметим, что в отчете 2024 года при опросах и анализе участвовали в том числе дети от 3-х лет, в связи с чем возрастает опасность того, с какой информацией дети сталкиваются в сети и ее влияние на интеллектуальное развитие подрастающего поколения. Анализ «Лаборатории Касперского» показал, что популярные короткие видео (до 60 секунд) могут провоцировать развитие «клипового мышления» (28 %) и снижают концентрацию внимания (28 %). Но больше всего беспокойство вызывает отсутствие возрастных ограничений (35 %) у таких видео<sup>137</sup>. Таким образом, в настоящее время взаимодействие несовершеннолетних с цифровой средой становится малоконтролируемым. К тому же 7 % подростков 11–17 лет указали, что выкладывали на своих страницах или отправляли кому-то в личных сообщениях фото и видео очень личного характера.

Проблема информационной безопасности несовершеннолетних в Интернете находит отголоски в научных исследованиях<sup>138</sup>. На сегодня российская

<sup>135</sup> Конвенция о защите прав человека и основных свобод (Заключена в г. Риме 04.11.1950, с изм. от 24.06.2013) (вместе с «Протоколом [№ 1]» (Подписан в г. Париже 20.03.1952), «Протоколом № 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (Подписан в г. Страсбурге 16.09.1963), «Протоколом № 7» (Подписан в г. Страсбурге 22.11.1984)) // СЗ РФ. 2001. № 2. Ст. 163.

<sup>136</sup> Лаборатория Касперского. Исследование «Лаборатории Касперского»: дети онлайн. URL: <https://securelist.ru/issledovanie-laboratorii-kasperskogo-deti-onlajn/25212/> (дата обращения: 01.05.2025).

<sup>137</sup> Отчет «Лаборатория Касперского» от 23.05.2024 «Взрослые и дети в интернете: аналитический отчет 2023». URL: <https://kids.kaspersky.ru> (дата обращения: 01.05.2025).

<sup>138</sup> Белякова Е. Г., Загвязинская Э. В., Березенцева А. И. Информационная культура и информационная безопасность школьников // Образование и наука. 2017. Т. 19. № 8. С. 147-162; Гольяпина И. Ю., Мухаметова Д. Ф. Нормативно-правовое обеспечение информационной безопасности детей // Инновационная экономика и общество. 2017. № 3 (17). С. 71-79; Дадаева М. С. Государственная система кибербезопасности и предупреждение экстремизма среди несовершеннолетних // Современные научные исследования и разработки. 2018. Т. 1. № 5 (22). С. 183.

законодательная база в сфере защиты несовершеннолетних от информации, наносящей вред их развитию с помощью сети «Интернет», состоит из следующих основных нормативно-правовых актов: Рекомендация № CM/Rec (2018)7 Комитета министров Совета Европы «О соблюдении, защите и осуществлении прав детей в цифровой среде»<sup>139</sup>; Федеральный закон от 29 декабря 2010 г. № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон № 436-ФЗ)<sup>140</sup>; Федеральный закон от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»<sup>141</sup>; Указ Президента РФ от 05 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»<sup>142</sup>; Распоряжение Правительства РФ от 28 апреля 2023 г. № 1105-р «Об утверждении Концепции информационной безопасности детей в РФ»<sup>143</sup>; Комплексный план противодействия идеологии терроризма в Российской Федерации на 2024–2028 годы (в части работы с несовершеннолетними в сети «Интернет»)<sup>144</sup> и рядом других нормативно-правовых актов.

Уточним, что положения таких нормативно-правовых актов, как «Конвенция о правах ребенка», принятая Генеральной Ассамблеей ООН от 20 ноября 1989 г.<sup>145</sup>, Международный пакт о гражданских и политических правах» от 16 декабря 1966 г.<sup>146</sup>, носят скорее декларируемый характер, а не профильный в исследуемом вопросе. В 2024 году принята Конвенция ООН против киберпреступности<sup>147</sup>,

<sup>139</sup> Рекомендация № CM/Rec(2018)7 Комитета министров Совета Европы «О соблюдении, защите и осуществлении прав детей в цифровой среде» (Вместе с «Руководящими принципами...») (Принята 04.07.2018 на 1321-м заседании представителей министров) // Бюллетень Европейского суда по правам человека. Российское издание. 2018. № 12.

<sup>140</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>141</sup> Федеральный закон от 24.07.1998 № 124-ФЗ (ред. от 30.11.2024) «Об основных гарантиях прав ребенка в Российской Федерации» // СЗ РФ. 1998. № 31. Ст. 3802; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>142</sup> Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

<sup>143</sup> Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СЗ РФ. 2023. № 19. Ст. 348.

<sup>144</sup> Комплексный план противодействия идеологии терроризма в Российской Федерации на 2024 - 2028 годы (утв. Президентом РФ 30.12.2023 № Пр-2610) // СПС «КонсультантПлюс».

<sup>145</sup> Конвенция о правах ребенка от 20 ноября 1989 г. // Сборник международных договоров СССР. 1993. Вып. XLVI.

<sup>146</sup> Международный пакт о гражданских и политических правах от 16 декабря 1966 г. // Ведомости ВС СССР. 1976. № 17. Ст. 291.

<sup>147</sup> Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (принята резолюцией 79/243 Генеральной Ассамблеей от 24.12.2024). URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243> (дата обращения: 31.08.2025).

разработанная по инициативе России и которая относит к киберпреступлениям такие умышленные деяния, как размещение в сети «Интернет» материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации (ст. 14), домогательства или создание доверительных отношений с целью совершения сексуального преступления в отношении ребенка (ст. 15), а также дает уточнение в ч. 4 ст. 16.

В России с 2011 года действует Закон № 436-ФЗ, принятие которого «органически сочеталось» (термин К. Д. Рыдченко)<sup>148</sup> с концепцией Федеральных законов от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»<sup>149</sup> и от 24 июня 1999 г. № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»<sup>150</sup>, а также с действовавшей на тот момент Национальной стратегией действий в интересах детей на 2012–2017 гг., утвержденной Указом Президента РФ от 1 июня 2012 г. № 761<sup>151</sup>. Нормы и УК РФ, устанавливающие ответственность за распространение не ограниченной в доступе (не секретной) информации, не только получили нормативную основу, но и были дополнены, получив логичное развитие.

Статья 5 закона № 436-ФЗ не дает непосредственного определения информации, причиняющей вред здоровью и развитию детей, но определяет четкую классификацию и перечень подобной информации, а именно: 1) запрещенная информация, предусмотренная ч. 2 ст. 5 Закона № 436-ФЗ; к такой информации относится та, которая влечет вред жизни и здоровью детей и подростков, склоняет к терроризму, насилию, наркотическим средствам, проституции и т. д. Перечень запрещенной информации детальный и ограниченный; 2) ограниченная информация (распространение которой среди детей определенных возрастных категорий ограничено и которая предусмотрена ч.

<sup>148</sup> Рыдченко К. Д. Запрещенная для детей информация: легальная трактовка и толкование правоприменителя // Информационное право. 2014. № 5. С. 16–21.

<sup>149</sup> Федеральный закон от 24.07.1998 № 124-ФЗ (ред. от 30.11.2024) «Об основных гарантиях прав ребенка в Российской Федерации» // СЗ РФ. 1998. № 31. Ст. 3802; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>150</sup> Федеральный закон от 24.06.1999 № 120-ФЗ (ред. от 08.08.2024) «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» // СЗ РФ. 1999. № 26. Ст. 3177; СЗ РФ. 2025. № 14. Ст. 1588.

<sup>151</sup> Указ Президента РФ от 01.06.2012 № 761 «О Национальной стратегии действий в интересах детей на 2012 – 2017 годы» // СЗ РФ. 2012. № 23. Ст. 2994.



3 ст. 5 Закона № 436-ФЗ с учетом положений ст. 7–10 Закона № 436-ФЗ). К ограниченной информации относится контент с изображением или описанием насилия, жестокости и т. д.

Необходимость ст. 5 № 436-ФЗ обусловлена тем, что в сети «Интернет» имеется огромное количество деструктивно влияющей информации, которая с легкостью попадает на глаза несовершеннолетним. Вредоносными факторами можно считать: 1) контент порнографического характера, кибергруминг (процесс вхождения в доверие к несовершеннолетнему с целью использовать его в сексуальных целях, иначе говоря, виртуальное насилие), кибербуллинг (травля в сети «Интернет»); 2) риски, связанные с потреблением, какими обычно пользуются мошенники в своих целях; 3) безопасность размещения информации в своих социальных сетях, дети не всегда осознают риски. Общеизвестно, что размещенная информация в социальных сетях может быть использована против лица, ее разместившего, поэтому необходимо разумно подходить к размещению любой информации, в особенности в отношении несовершеннолетних лиц.

С учетом возрастных особенностей несовершеннолетних Законом № 436-ФЗ введена классификация информационной продукции до начала ее оборота и установлены ч. 3 ст. 6 пять групп: 1) запрещенная для детей; 2) для детей младше 6 лет; 3) старше 6 лет; 4) старше 12 лет; 5) старше 16 лет. Законом установлены (ст. 7–10) детальные требования информационной продукции согласно вышеобозначенным возрастным критериям. Требования к обороту информационной продукции, которая запрещена для детей, установлены Министерством связи и массовых коммуникаций<sup>152</sup>. Несомненно, важным инструментом правового механизма защиты несовершеннолетних от деструктивного контента явилось создание в 2012 г. Единого реестра доменов и сайтов, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие

---

<sup>152</sup> Приказ Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию» // Российская газета. 20.08.2014. № 187.

информацию, распространение которой в РФ запрещено<sup>153</sup>.

Ввиду отсутствия легально закрепленного понятия «информация, причиняющая вред здоровью и развитию несовершеннолетних», в научной литературе присутствуют разные суждения в отношении этого понятия, а также употребление в качестве тождественных понятий таких выражений, как «вредная информация», «вредоносная информация», «деструктивный контент» и «деструктивная информация». Ряд авторов использует термин «вредная информация». Например, И. Л. Бачило понимает под ней такую информацию, негативное воздействие которой в результате распространения или применения влечет необходимость защиты лиц<sup>154</sup>. По мнению В. С. Маурина, «вредной информацией» считается информация, посягающая на интересы – личные, общества, государства<sup>155</sup>. В. Н. Лопатин анализируемое понятие рассматривает как «информация, не являющаяся конфиденциальной, но обуславливающая необходимость охраны и защиты прав и законных интересов личности, общества и государства в силу возможного вреда, который нанесет этим субъектам ее распространение (применение)»<sup>156</sup>. К. Д. Рыдченко определяет сущность и основные признаки «вредоносной информации» в следующей редакции: «сведения, содержащие качества недостоверности, непристойности или деструктивности, негативное воздействие которых на индивидуальную психику и общественное сознание обуславливает необходимость ограничения или запрета их оборота в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства»<sup>157</sup>. Приведенные дефиниции свидетельствуют о том, что

<sup>153</sup> Постановление Правительства РФ от 26.10.2012 № 1101 (ред. от 21.02.2025) «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-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // СЗ РФ. 2012. № 44. Ст. 6044.

<sup>154</sup> Бачило И. Л. Информационное право. Основы практической информатики : учеб. пособие. М., 2003. С. 342.

<sup>155</sup> Маурин В. С. Правовой анализ вредной информации в условиях информационного общества : дис. ... канд. юрид. наук. М., 2004. С. 6.

<sup>156</sup> Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право / Под ред. Б. Н. Топорнина. СПб., 2001. С. 401.

<sup>157</sup> Рыдченко К. Д. Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации : дис. ... канд. юрид. наук. Воронеж, 2011. С. 53.

авторы едины в определении природы «вредной информации». Каждый из них связывает вредоносность информации с наличием в ней возможного вреда (В. Н. Лопатин), общественной опасности (В. С. Маурин), негативного воздействия ввиду наличия в распространяемых сведениях качеств недостоверности, непристойности или деструктивности (К. Д. Рыдченко)<sup>158</sup>. К. Э. Геляхов предлагает следующую трактовку анализируемого нами термина, выраженную в том, что подобная информация причиняет физический и (или) психический вред подростку<sup>159</sup>. В данном случае этот автор достаточно лаконично дает характеристику тому, что следует понимать под информацией, в частности, размещенной в сети «Интернет», наносящей вред развитию несовершеннолетних, так как идет указание, что она должна быть способной причинить определенный вред несовершеннолетнему. М. С. Власенко указывает на информацию, причиняющую вред подростку, так как акцентирует внимание, что она должна быть ограничена либо запрещена для лиц подобного возраста на законодательном уровне<sup>160</sup>. К. В. Бородин полагает, что в основе «вредной информации» для подростков лежит негативное влияние на несовершеннолетних. Причем подобная информация может нести угрозу не только самим несовершеннолетним, но также окружающим лицам и государству в целом<sup>161</sup>.

В настоящее время достаточно популярным и обоснованным термином является именно «деструктивный контент». Так, схожий термин используется законодателем в Распоряжении Правительства РФ от 01.07.2024 № 1734-р – «деструктивное информационно-психологического воздействия»<sup>162</sup>, в Распоряжении Правительства РФ от 28.04.2023 г. № 1105-р – «деструктивное

<sup>158</sup> Шуликов К. А. Административно-правовые основы противодействия распространению деструктивного контента в сети «Интернет»: дис. ... канд. юрид. наук. СПб., 2024. С. 27.

<sup>159</sup> Геляхов К. Э. Информационная безопасность несовершеннолетних: конституционно-правовой аспект // Научные исследования студентов и учащихся : сб. статей X Международной научно-практической конференции. Пенза, 2023. С. 63.

<sup>160</sup> Власенко М. С. Обеспечение информационной безопасности несовершеннолетних в сети Интернет: современное состояние и совершенствование правового регулирования // Вестник Волжского университета им. В. Н. Татищева. 2019. Т. 1, № 3. С. 98-105.

<sup>161</sup> Бородин К. В. Правовая защита несовершеннолетних от информации, приносящей вред их здоровью и развитию, распространяющейся в сети Интернет // Актуальные проблемы российского права. 2016. № 7(68). С. 68-74.

<sup>162</sup> Распоряжение Правительства РФ от 01.07.2024 № 1734-р (ред. от 04.04.2025) «Об утверждении Плана мероприятий по реализации в 2024 – 2026 годах Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // СЗ РФ. 2024. № 28. Ст. 4058.

информационное воздействие»<sup>163</sup>. В Постановлении Правительства РФ от 15.04.2014 № 313 указан термин «деструктивный контент»<sup>164</sup>. В коллективной монографии, посвященной правовому регулированию защиты несовершеннолетних от деструктивной информационной среды (С. Е. Титор, Ф. Г. Мышко, Т. Н. Каменева, В. В. Попов, М. Л. Горбунов)<sup>165</sup>, используют данные дефиниции: например, «деструктивный контент», «деструктивная информация». К сожалению, самого понятия терминов в цитируемой научной работе не приводится. В научно-правовых трудах подобная терминология встречается также у таких авторов, как К. М. Беликова<sup>166</sup>, К. А. Шуликов<sup>167</sup>, И. В. Медведева<sup>168</sup>, Ю. Н. Кириченко, Д. В. Меняйло, К. К. Крупенникова<sup>169</sup>, Г. А. Грищенко, В. Д. Никишин<sup>170</sup>, Ю. Б. Савва, Т. Ю. Савва<sup>171</sup>, Р. Е. Ренжигло<sup>172</sup>, С. А. Осипов<sup>173</sup>, В. Н. Цимбал, М. Ю. Толстых<sup>174</sup>, С. И. Чудинов<sup>175</sup> и др.

Можно сказать, что, как правило, приведенные авторы используют термин «деструктивная информация (контент)» как более краткий синоним понятию

<sup>163</sup> Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СЗ РФ. 2023. № 19. Ст. 348.

<sup>164</sup> Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 25.12.2024) «Об утверждении государственной программы Российской Федерации «Информационное общество»» // СЗ РФ. 2014. № 18 (часть II). Ст. 2159.

<sup>165</sup> Правовое регулирование защиты несовершеннолетних от деструктивной информационной среды : монография / Под общ. ред. С. Е. Титор. М. : РУСАИНС, 2025. 350 с.

<sup>166</sup> Беликова К. М. Некоторые направления и риски использования нейросетей для борьбы с деструктивным контентом: мнение юриста // Юрист. 2025. № 2. С. 8-13.

<sup>167</sup> Шуликов К. А. Субъекты противодействия распространению деструктивного контента в сети Интернет и административно-правовая характеристика их деятельности // Административное право и процесс. 2024. № 8. С. 69-73.

<sup>168</sup> Медведева И. В. Проблема защиты несовершеннолетних от деструктивного контента // Государство, общество и личность в современных условиях: актуальные вопросы правового регулирования : сб. научных статей II Всероссийской научно-практической конференции с международным участием. Саратов, 2024. С. 64-68.

<sup>169</sup> Кириченко Ю. Н., Меняйло Д. В., Крупенникова К. К. Социально-правовые аспекты профилактики преступлений несовершеннолетних, совершаемых под влиянием деструктивного контента в сети Интернет // Научный портал МВД России. 2024. № 2 (66). С. 75-81.

<sup>170</sup> Грищенко Г. А., Никишин В. Д. Проблемы правового регулирования деструктивной информации // В сб.: Организация работы по предупреждению деструктивной идеологии в подростковой среде. Материалы научно-практической конференции. Москва, 2025. С. 24-27.

<sup>171</sup> Савва Ю. Б., Савва Т. Ю. Использование искусственного интеллекта при модерации деструктивного контента социальных сетей // Интеллектуальные информационные системы : труды Международной научно-практической конференции, посвященной 40-летию кафедры САПРИС. Воронеж, 2024. С. 133-136.

<sup>172</sup> Ренжигло Р. Е. Влияние деструктивного интернет-контента на формирование экстремистских взглядов у молодежи // Вестник Донецкого национального университета. Серия Е: Юридические науки. 2023. № 2. С. 43-50.

<sup>173</sup> Никишин В. Д., Осипов С. А. Меры противодействия деструктивному контенту: опыт и перспективы // Обзор НЦПТИ. 2024. № 4 (39). С. 14-25.

<sup>174</sup> Цимбал В. Н., Толстых М. Ю. Противодействие деструктивному контенту в сети Интернет. М. : Московский университет Министерства внутренних дел Российской Федерации им. В. Я. Кикотя (Москва), 2023. 52 с.

<sup>175</sup> Чудинов С. И. Классификация девиантно-деструктивного контента в социальной сети ВКонтакте // Российская наука и образование сегодня: проблемы и перспективы. 2024. № 4 (59). С. 64-68.

«информация, причиняющая вред здоровью и развитию». Однако у К. А. Шуликова указано иное понимание, а именно: «содержательное определение деструктивного контента как разновидности вредной информации, локализуемой в сети Интернет»<sup>176</sup>.

Заслуживающей внимания для исследования представляется классификация основных форм криминогенного воздействия Интернета на несовершеннолетних, которая изложена в диссертационном исследовании Е. В. Кузнецовой: 1) контентное воздействие; 2) коммуникативное воздействие<sup>177</sup>. К первому воздействию относится влияние информации, которая причиняет вред здоровью и развитию несовершеннолетних (например, пропаганда насилия, наркотических веществ, проституции и т. д.); ко второму воздействию относится непосредственно межличностное общение, деструктивно влияющее (например, кибербуллинг, секстинг, троллинг и т. д.).

Как отмечает Е. Н. Тогузаева, единственная, пожалуй, юридико-техническая неточность состоит в том, что Закон № 124-ФЗ об основных гарантиях прав ребенка содержит ряд указаний запрещающего характера, которые не обусловлены несовершеннолетием субъекта правоотношений (запреты пропаганды различных неравенств касаются всех граждан: не только детей, но и взрослых индивидов)<sup>178</sup>. П. А. Астафичев выделяет два правовых недостатка положений Закона № 436-ФЗ: «1) выбранные законодателем критерии и способы «вычленения» вредоносной информации; 2) административно-правовые методы реализации установленных законом ограничений и запретов»<sup>179</sup>. По нашему мнению, согласиться с выводами П. А. Астафичева достаточно сложно, так как в законодательстве приведены

<sup>176</sup> Шуликов К. А. Деструктивный контент: понятие, административно-правовая характеристика, виды // Вестник Нижегородского университета им. Н. И. Лобачевского. 2023. № 2. С. 176-182.

<sup>177</sup> Кузнецова Е. В. Предупреждение делинквентного поведения несовершеннолетних, продуцируемого контентом сети Интернет : автореф. дис. ... канд. юрид. наук. Курск, 2019. С. 9.

<sup>178</sup> Тогузаева Е. Н. Опыт закрепления запрета пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду, в конституциях стран – членов Содружества Независимых Государств // Современное право. 2013. № 8. С. 131-134.

<sup>179</sup> Астафичев П. А. Законодательство о защите детей от приносящей им вред информации в механизме ограничений конституционных прав граждан на информацию и доступ к культурным ценностям // Конституционное и муниципальное право. 2020. № 2. С. 17-22.

достаточные обоснования информации, наносящей вред здоровью и развитию несовершеннолетних.

В Указе Президента РФ от 02 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» подчеркивается, что основным объектом такого деструктивного воздействия является молодежь»<sup>180</sup>.

В Концепции информационной безопасности детей в РФ<sup>181</sup> представлены принципы, задачи, мониторинг обеспечения безопасности несовершеннолетних в сети «Интернет». Концепция является одним из основных нормативно-правовых актов, регламентирующих безопасность несовершеннолетних в сети «Интернет». Несовершеннолетние в интернет-пространстве являются самыми уязвимыми. Это связано с их неопытностью при использовании сети «Интернет» и психологической незрелостью, особенностями когнитивных функций на возрастном этапе развития. Стоит вспомнить так называемое движение «Синего кита» или различные другие группы смерти. По словам лиц, состоявших в этих группах, обычно в них давали задания, не связанные со смертью, больше заданий было связано с нанесением человеком повреждений самому себе. Концепция информационной безопасности детей в РФ содержит перечень информации, распространение которой незаконно на территории РФ (этот перечень коррелирует со ст. 5 закона № 436-ФЗ), а также интересный в рамках нашего исследования тезис, что постоянно возрастающие возможности социальных сетей способствуют размещению детьми в открытом доступе в сети «Интернет» личной и семейной информации, которая нередко используется злоумышленниками в противоправных целях<sup>182</sup>.

В Указе Президента РФ от 05 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»<sup>183</sup> подчеркивается, что для обеспечения безопасности государства и общества

<sup>180</sup> Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (часть II). Ст. 5351.

<sup>181</sup> Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СЗ РФ. 2023. № 19. Ст. 3481.

<sup>182</sup> Там же.

<sup>183</sup> Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

необходимо осуществлять противодействие с использованием информационных технологий: пропаганде экстремизма; пресекать нанесение ущерба национальной безопасности; разглашению сведений, составляющих государственную тайну и иную информацию, которой по законодательству может владеть ограниченный круг лиц; нарушению традиционных духовно-нравственных ценностей.

Между тем, анализируя ряд отечественных нормативных правовых актов, можем сказать, что к информации, наносящей вред развитию несовершеннолетних с помощью сети «Интернет», можно отнести на основе ч. 1 ст. 10.6. Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: призывы к совершению преступлений, пропаганду порнографии, пропаганду насилия и жестокости и т. д.

Таким образом, детально изучив законодательство РФ в сфере защиты несовершеннолетних от информации, причиняющей вред их здоровью и развитию, можно сказать следующее. В Законе № 436-ФЗ<sup>184</sup> ставится вопрос о том, что в характеристике деструктивно влияющей информации указано, что она может причинять вред «здоровью» и «развитию» несовершеннолетнего, однако, на наш взгляд, имеется значительное законодательное упущение в виде отсутствия вреда для «жизни». Так, нами в этом параграфе были описаны такие деструктивные сообщества, как «Синий кит» и т. д., одной из целей которых является романтизация смерти и непосредственно самоубийства, что причиняет вред не только здоровью и (или) развитию несовершеннолетнего, а непосредственно его жизни. Статья 110.1 УК РФ «Склонение к совершению самоубийства или содействие совершению самоубийства» была введена Федеральным законом от 07.06.2017 № 120-ФЗ (то есть после принятия Федерального закона № 436-ФЗ); ч. 2 статьи 110 УК РФ «Доведение до самоубийства» устанавливает, что «доведение лица до самоубийства или до покушения на самоубийство путем угроз, жестокого обращения или систематического унижения человеческого достоинства потерпевшего – «а) в отношении несовершеннолетнего или лица, заведомо для

---

<sup>184</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

виновного находящегося в беспомощном состоянии либо в материальной или иной зависимости от виновного; <...> д) в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»))»<sup>185</sup>.

Здесь считаем важным обратить внимание, что использование сети «Интернет» считается таким же квалифицирующим признаком<sup>186</sup>, как преступление против беременной женщины, ребенка или совершенного группой лиц по предварительному сговору<sup>187</sup>.

Отметим, что кибербуллинг, заключающийся в доведении жертвы интернет-травли до самоубийства или в склонении к совершению самоубийства, влечет ответственность по ст. 110–110.1 УК РФ<sup>188</sup>.

Глава 16 УК РФ посвящена преступлениям против жизни и здоровья, при этом преступления против жизни объединяются объектом – то есть жизнью человека. В отличие от группы преступлений против жизни, где объектом выступает непременно чужая жизнь и обязательным признаком объективной стороны являются последствия в виде смерти, исключением является именно ст. 110 УК РФ и 110.1 УК РФ, где такое деяние, как доведение лица до покушения на самоубийство или склонение к нему, «сконструировано по типу состава создания опасности»<sup>189</sup>.

Несомненно, акцентирование на преступлениях против жизни законодателем полностью обосновано, ведь подобные деяния характеризуются повышенной общественной опасностью и необратимыми последствиями, ведь утрата жизни не поддается восстановлению или возмещению.

---

<sup>185</sup> Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) // СЗ РФ. 1996. № 25. Ст. 2954; Российская газета. 25.04.2025. № 93т.

<sup>186</sup> Ткачев И. О. Использование информационно-телекоммуникационных сетей как квалифицирующий признак состава преступления // Уголовное право. 2024. № 10. С. 72-83

<sup>187</sup> Кассационное определение Второго кассационного суда общей юрисдикции от 19.12.2024 № 77-3490/2024 (приговор: По п. «д» ч. 2 ст. 110 УК РФ (доведение до самоубийства)) // СПС «КонсультантПлюс».

<sup>188</sup> Ответственность за травлю (буллинг) : статья // СПС «КонсультантПлюс».

<sup>189</sup> Голенко Д. В. Преступления против жизни и здоровья : учеб. пособие. Самара, 2019. С. 12-14.



Таким образом, непосредственно в ст. 5 «Виды информации, причиняющей вред здоровью и (или) развитию детей» Закона № 436-ФЗ<sup>190</sup>, как и в его названии «О защите детей от информации, причиняющей вред их здоровью и развитию» и в тексте, следует излагать как «О защите детей от информации, причиняющей вред их жизни, здоровью и развитию». Наше предложение также подтверждается и тем, что фрагментарно законодатель добавляет формулировку «вред жизни», как, например, в части 2 ст. 5 Закона от 29.12.2010 № 436-ФЗ: «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». Следует сказать, что это единственный случай применения этой формулировки во всем данном законе, которая была представлена еще в самой первой редакции закона.

Таким образом, ст. 5 Закона № 436-ФЗ устанавливает два вида деструктивного контента в российском законодательстве: 1) запрещенная информация, перечень которой детальный и ограниченный; 2) ограниченная информация – распространение которой, в том числе в сети «Интернет», должно быть ограничено таким образом, чтобы избежать ее деструктивного влияния на малолетних и подростков (к ограниченной информации относится контент с изображением или описанием насилия, жестокости и т. д.).

### **1.3. Правовая характеристика деструктивного контента для несовершеннолетних в сети «Интернет» в зарубежном законодательстве**

Немецкий правовед Д. Халлинан (D. Hallinan) и нидерландский правовед Р. Геллерт (R. Gellert) считают, что в европейском законодательстве нет четкого определения понятия «информация»; также отсутствует структурированное и всеобъемлющее определение в судебной практике и оно получило недостаточно

---

<sup>190</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

внимания в научных юридических исследованиях<sup>191</sup>. При этом недостаточное изучение понятия «информация» противоречит концепции, которая является сложной, многогранной и функционально проблематичной в GDPR (Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных)<sup>192</sup>. Исходя из анализа вышеуказанного закона, Д. Халлинан (D. Hallinan) и Р. Геллерт (R. Gellert) выдвигают три совокупных тезиса: 1) понятие «информация» играет две разные роли: информация как критерий применимости и информация как объект регулирования; 2) содержательные границы понятий, описывающих эти две роли, различаются, то есть это два разных понятия, не связанных с одним и тем же содержательным явлением; 3) существенные различия между этими двумя понятиями информации важны для эффективности GDPR как инструмента информационного права.

Достаточно широкую поддержку в европейском научном сообществе<sup>193</sup> имеет позиция Ли А. Байгрейв (L. A. Bygrave), согласно которой «Информация в праве обычно обозначает форму семантического содержания... Право в первую очередь занимается регулированием человеческих отношений; в этом ключевую роль играют производство и обмен смыслами»<sup>194</sup>.

В Австралии согласно Online Safety Act 2021<sup>195</sup> установлены критерии для определения информации, причиняющей вред здоровью и развитию несовершеннолетнего. Так, согласно ст. 6 (1) Online Safety Act 2021, информация считается деструктивной, если обычный здравомыслящий человек пришел бы к

<sup>191</sup> Hallinan D., Gellert R. The Concept of «Information»: An Invisible Problem in the GDPR. SCRIPT-ed. 2020. Vol. 17(2). P. 269-319.

<sup>192</sup> Regulation EU 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (дата обращения: 01.05.2025).

<sup>193</sup> Например, Ritleng D. Chronique Jurisprudence administrative française intéressant le droit de l'UE - Le Conseil d'État rappelle comment faire le filtre des QPC portant sur des lois de transposition d'une directive européenne // *Revue générale de droit international public*. 2019. Vol. 1. P. 1-12; Yeung K., Bygrave L. A. Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship // *Regulation & Governance*. 2021. № 16(2). P. 1-9; Kuner C. and others. The EU General Data Protection Regulation (GDPR): A Commentary / Update of Selected Articles. Oxford University Press, 2020. 1486 p.

<sup>194</sup> Bygrave L. A. Information Concepts in Law: Generic Dreams and Definitional Daylight // *Oxford Journal of Legal Studies*. 2014. № 35(1). P. 91-120. (quote from p. 112).

<sup>195</sup> Online Safety Act 2021 No. 76. URL: <https://www.legislation.gov.au> (дата обращения: 01.05.2025).

выводу, что вполне вероятно, что материал был предназначен для воздействия на конкретного «австралийского ребенка»; и материал, вероятно, будет представлять для него серьезную угрозу, запугивать, беспокоить или унижать его достоинство.

Статья 107 Online Safety Act содержит перечень контента, который относится, по оценкам Квалификационной комиссии (а также такой контент, который не классифицирован комиссией, но который в случае оценки, вероятно, получил бы ограничение 18+), к возрастной группе старше 18 лет и который может быть опубликован только с учетом технических мер, которые пресекут доступ несовершеннолетних к этому контенту: порнографический материал; публикации, фильмы и компьютерные игры, содержащие порнографические элементы, сцены жестокости, насилия.

В целях обеспечения информационной безопасности несовершеннолетних в Великобритании в 2023 году был принят закон Online Safety Act<sup>196</sup>, в котором седьмая глава содержит перечень контента, который способен причинить вред несовершеннолетнему, а именно:

- 1) «незаконный контент» – «illegal content» (ст. 59);
- 2) «контент, вредный для детей» – «content that is harmful to children» (ст. 60);
  - контент с высоким приоритетом, вредный для детей – «primary priority content that is harmful to children» (ст. 61);
  - «приоритетный контент, вредный для детей» – «priority content that is harmful to children» (ст. 62);
  - или иной контент, не относящийся к пунктам (а) или (b), который представляет существенную опасность причинения значительного вреда большому количеству детей в Соединенном Королевстве (ст. 60).

Согласно (2) и (3) ст. 59 Online Safety Act под «незаконным контентом» понимают контент, который является правонарушением, а именно наличие слов (текстов), аудиофайлов, видеофайлов, которые считаются правонарушением при условии: использование; хранение, просмотр, доступ, распространение подобного контента. Кроме того, в незаконном контенте выделяют «приоритетный

<sup>196</sup> Online Safety Act 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50> (дата обращения: 21.07.2025).

незаконный контент», то есть «приоритетное правонарушение» (преступления, связанные с террористической направленностью, сексуальной эксплуатацией и насилием над детьми и другие тяжкие преступления).

Согласно ст. 60 Online Safety Act «контент, вредный для детей», включает:

(а) *контент с высоким приоритетом* или *главный приоритетный контент* («primary priority content that is harmful to children»), который может нанести вред детям (согласно содержанию ст. 61 данный контент содержит порнографию; информацию, которая поощряет, пропагандирует или содержит инструкции по совершению самовредительства и (или) самоубийства; расстройство пищевого поведения);

(б) *приоритетный контент, причиняющий вред детям* («priority content that is harmful to children»). Так, согласно ст. 62 Online Safety Act «приоритетный контент, вредный для детей», означает контент, направленный на дискриминацию (оскорбление) или разжигание ненависти к людям какой-либо расы, сексуальной ориентации, религии, инвалидности, смены пола — которая, уточним, законодательно запрещена в РФ; контент, поощряющий или пропагандирующий жестокость (насилие) в отношении человека (в том числе учитываются согласно (5) ст. 62 элементы буллинга), а также жестокость (насилие) в отношении животных; контент, поощряющий или пропагандирующий действия, которые травмоопасны или связаны с приемом внутрь (в том числе внутривенно или вдыханием) каких-либо веществ, способных нанести вред здоровью человека;

(с) *или иной контент*, не относящийся к пунктам (а) или (б), *который представляет существенную опасность причинения значительного вреда большому количеству детей* в Соединенном Королевстве.

Таким образом, перечень контента, причиняющего вред несовершеннолетним, согласно Online Safety Act является детальным и открытым.

В тексте Online Safety Act достаточно часто встречается (ст. 11, 12, 13 и т. д.) правовая конструкция «дети любого возраста» и «дети в разных возрастных группах», например, при оценке рисков, оказываемых на несовершеннолетних; при функционировании алгоритмов онлайн-платформ, баз данных и профилей

пользователей. Отметим, что непосредственно возрастные пределы «разных возрастных групп» несовершеннолетних в законе не раскрываются. Уточним, что на территории Европы существуют разные возрастные рейтинги, например, система возрастных рейтингов игр Pan-European Game Information (PEGI) классифицирует видеоигры по возрастным категориям (3, 7, 12, 16 и 18 лет)<sup>197</sup>.

Следует обратить внимание, что в Online Safety Act четко указаны признаки «контента, направленного на травлю» (буллинг), а именно: этот контент должен быть направлен (адресован) конкретному лицу; представлять серьезную угрозу и обладать унижительным или оскорбительным характером, а также носить системный характер, то есть представлять кампанию по жестокому обращению. В рамках темы исследования также представляет интерес понятие «контент», представленное в ст. 236 Online Safety Act: «контент означает все, что передается с помощью интернет-сервиса, как публично, так и в частном порядке, включая письменные материалы или сообщения, устные высказывания, фотографии, видео, визуальные образы, музыку и данные любого рода»<sup>198</sup>.

На наш взгляд, закон Великобритании в целях обеспечения информационной безопасности в сети «Интернет» достаточно проработан, детально регламентирует как теоретические аспекты (понятия, правовые характеристики), так и практические (порядок подачи жалоб, взаимодействия участников сети «Интернет», даже порядок раскрытия информации об использовании сервиса умершими несовершеннолетними пользователями (ст. 75)). Также отметим, что Закон об онлайн-безопасности принят 26.10.2023, и по состоянию на июль 2025 года уже внесено порядка сорока поправок, в том числе уточняющих терминологию.

Рассмотрим законодательство государств ЕС, в том числе и непосредственно законодательство Франции в исследуемой сфере. В пространстве ЕС осознание данной проблемы привело к выработке как на национальном, так и на общеевропейском уровне политико-правовых механизмов защиты детей от

<sup>197</sup> Advice on child internet safety 1.0. URL: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/251455/advice\\_on\\_child\\_internet\\_safety.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251455/advice_on_child_internet_safety.pdf) (дата обращения: 21.07.2025).

<sup>198</sup> Online Safety Act 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50> (дата обращения: 21.07.2025).

деструктивного контента в сети «Интернет»<sup>199</sup>. Можно сказать, что принятые нормативные акты в ЕС рассматривают несовершеннолетних как особую целевую аудиторию в сети «Интернет». В связи с этим политика ЕС направлена на выработку специальных механизмов обеспечения их безопасности в Интернете<sup>200</sup>, которые уже детализируются на национальном уровне государств – членов ЕС. Исходным актом в этой сфере можно назвать Договор о Европейском союзе<sup>201</sup>, в ст. 3 которого указано, что защита прав детей является одной из основных целей деятельности ЕС.

В 2018 году Комитетом министров Совета Европы (в их число ранее входила и Россия – с 28 февраля 1996 года и до исключения 16 марта 2022 года) приняты Рекомендации «О соблюдении, защите и осуществлении прав детей в цифровой среде», а также Руководящие принципы по соблюдению, защите и осуществлению прав детей в цифровой среде<sup>202</sup>. Согласно этим правовым актам государствам рекомендовано принять нормативно-правовые акты по обеспечению и мониторингу информационной защиты несовершеннолетних в сети «Интернет».

В ЕС 25.05.2018 вступил в силу GDPR (General Data Protection Regulation)<sup>203</sup> – новый регламент по защите данных, который касается защиты персональных данных как граждан стран ЕС, так и граждан других стран, чьи данные обрабатываются на территории ЕС. Нормы GDPR также регламентируют и цифровую сферу. Так, один из основных принципов этого GDPR посвящен несовершеннолетним, а именно ст. 8 GDPR в корреляции с подп. «а» п. 1 ст. 6 GDPR регламентирует условия получения согласия на обработку персональных данных несовершеннолетнего субъекта данных. Так, обработка персональных данных

<sup>199</sup> Смирнов А.А. Обеспечение информационно-психологической безопасности детей в Европейском союзе // Информационное право. 2010. № 4. С. 30-34.

<sup>200</sup> Servaes J. The European Information Society. Publisher: Intellect, Bristol Editor. 2003. 245 p.

<sup>201</sup> Лиссабонский договор, изменяющий Договор о Европейском Союзе и Договор об учреждении Европейского Сообщества (Лиссабон, 13 декабря 2007 г.) (2007/C 306/01). URL: <https://eulaw.ru/treaties/lisbon/> (дата обращения: 01.05.2025).

<sup>202</sup> Рекомендация № CM/Rec (2018)7 Комитета министров Совета Европы «О соблюдении, защите и осуществлении прав детей в цифровой среде» (Вместе с «Руководящими принципами...») (Принята 04.07.2018 на 1321-м заседании представителей министров) // Бюллетень Европейского суда по правам человека. Российское издание. 2018. № 12.

<sup>203</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: <https://ogdpr.eu/> (дата обращения: 30.03.2025).

несовершеннолетнего является законной при достижении им минимум 16 лет либо же при наличии согласия (или одобрения на согласие) законного представителя несовершеннолетнего. При этом государства в составе ЕС могут устанавливать и иной минимальный возраст субъекта данных в пределах от 13 до 16 лет, а п. 2. ст. 6 GDPR возлагает на «контроллера»<sup>204</sup> обязательства приложить «разумные усилия» для проверки законности получения согласия.

В рамках исследуемой темы важно сказать о нормативном правовом акте ЕС – Регламенте № 2022/2065 Европейского парламента и Совета ЕС «О едином рынке цифровых услуг и о внесении изменений в Директиву 2000/31/ЕС (Акт о цифровых услугах – European Digital Services Act (DSA))»<sup>205</sup>, который принят в г. Страсбурге 19.10.2022 и вступил в силу 17.12.2022, главной целью которого является создание безопасной среды в сети «Интернет», в том числе для несовершеннолетних. Отметим, что так называемый «The Digital Services Act package» включает в себя Закон о цифровых услугах (Digital Services Act) и Закон о цифровых рынках (Digital Markets Act)<sup>206</sup>. Оба законодательных акта были приняты Советом и Европейским парламентом в 2022 году. Необходимо уточнить, что Закон о цифровых услугах (DSA) не определяет, что такое «незаконный контент», оставляя определение и перечень информации, причиняющей вред здоровью и развитию несовершеннолетним, за государствами – членами союза.

Закон о цифровых услугах (DSA) – это, несомненно, важное и достаточно масштабное законодательство в области защиты цифрового пространства от распространения незаконного контента и основных прав пользователей, в том числе несовершеннолетних. Данный законодательный акт регулирует социальные

---

<sup>204</sup> Согласно (7) ст. 4 GDPR: «контроллер» – физическое или юридическое лицо, публичное учреждение, агентство или иная структура, которая самостоятельно или совместно с другими определяет цели и способы обработки персональных данных; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: <https://ogdpr.eu/> (дата обращения: 30.03.2025).

<sup>205</sup> European Digital Services Act (DSA) (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC) (the DSA). URL: <http://eur-lex.europa.eu/> (дата обращения: 30.03.2025).

<sup>206</sup> Digital Markets Act Regulation (EU) 2022/1925 of the European Parliament and of the Council. URL: <http://eur-lex.europa.eu/> (дата обращения: 30.03.2025).

сети, онлайн-площадки, крупные онлайн-платформы (VLOP)<sup>207</sup>, такие как YouTube, Wikipedia, TikTok и крупные поисковые системы (VLOSE), такие как Google, Meta.

Крупные онлайн-платформы (VLOP) и очень крупные поисковые системы (VLOSE) проводят анализ создаваемых ими системных рисков: рисков, связанных с распространением незаконного контента, негативным влиянием на основные права, избирательные процессы, гендерное насилие или психическое здоровье.

Как указано в Акте о цифровых услугах, для достижения цели обеспечения безопасной, предсказуемой и заслуживающей доверия онлайн-среды в рамках настоящего Регламента понятие «незаконный контент» должно в целом отражать существующие правила в офлайн-среде<sup>208</sup>. Согласно положению части (12) Закона о цифровых услугах (DSA) понятие «незаконный контент» («illegal content») должно быть определено широко, чтобы охватить информацию, касающуюся незаконного контента, продуктов, услуг и видов деятельности. Учитывая вопросы защиты несовершеннолетних, Закон о цифровых услугах (DSA) в ч. (39) требует от всех онлайн-платформ, доступных детям, чтобы их сервисы обеспечивали высокий уровень конфиденциальности, безопасности и защиты несовершеннолетних. Платформы также обязаны создавать механизмы, с помощью которых пользователи могут сообщать о незаконном контенте. Закон о цифровых услугах (DSA) в ч. (67) требует четких условий использования, чтобы несовершеннолетние могли их понять, и запрещает «темные паттерны» (то есть интерфейсы, которые вводят пользователей в заблуждение или манипулируют ими) и запрещает всем онлайн-платформам показывать детям рекламу, основанную на профилировании. DSA требует, чтобы крупные платформы и поисковые системы эффективно и пропорционально выявляли и снижали потенциальные риски для несовершеннолетних. Таким образом, Закон о цифровых услугах (DSA) содержит новые меры защиты несовершеннолетних и запрещает онлайн-платформам отображать целевую рекламу на основе профилирования несовершеннолетних.

<sup>207</sup> DSA классифицирует платформы или поисковые системы, у которых более 45 миллионов пользователей в месяц в ЕС, как очень крупные онлайн-платформы (VLOP) или очень крупные поисковые системы (VLOSE).

<sup>208</sup> Регламент Европейского Парламента и Совета Европейского Союза 2022/2065 от 19 октября 2022 г. о едином рынке цифровых услуг и о внесении изменений в Директиву 2000/31/ЕС (Акт о цифровых услугах) // СПС Гарант.



Отметим, что именно международные организации играют решающую роль в установлении глобальных стандартов регулирования цифровых платформ, ведь, как справедливо указал А. А. Сарабеков, «эти правила направлены на решение таких вопросов, как модерация контента, алгоритмическая прозрачность и рыночная власть цифровых привратников»<sup>209</sup>.

Однако подход ЕС не обошелся без критики. Некоторые европейские юристы (L. Cabral, J. Haucap, G. Parker, G. Petropoulos, T. Valletti, M. Van Alstyne) утверждают, что строгие требования, налагаемые этими правилами, могут подавлять инновации и непропорционально обременять небольшие технологические компании<sup>210</sup>. Более того, экстерриториальное применение правил ЕС вызвало опасения относительно чрезмерного регулирования и потенциальных конфликтов с законами других юрисдикций. Несмотря на вышеуказанную критику, следует сказать, что ЕС достаточно серьезно относится к защите несовершеннолетних в сети «Интернет», и именно стремление поддерживать, защищать, расширять возможности и уважать законные права и интересы несовершеннолетних стало фундаментом Стратегии «Лучший Интернет для детей» (BIK+)<sup>211</sup>, принятой Европейской комиссией в мае 2022 года и направленной на улучшение цифровых услуг, соответствующих возрасту детей, а также на обеспечение защиты, расширения возможностей и уважения каждого ребенка в сети «Интернет». Сразу уточним, что согласно примечанию (3) Стратегии: лица в возрасте до 18 лет в соответствии с Конвенцией ООН о правах ребенка в рамках Стратегии «Лучший Интернет для детей» (BIK+) «молодежь» также относится к детям в возрасте до 18 лет. В законодательстве используется термин «несовершеннолетние». Примечание (26) содержит отсылку к «запрещенной» информации, часто называемой в европейской доктрине «незаконный контент» или «вредный контент», а именно, что «запрещено для всех пользователей:

<sup>209</sup> Сарабеков А. А. Регулирование цифровых платформ и интернет-услуг: правовые аспекты и перспективы // *Universum: экономика и юриспруденция*. 2024. № 11-1 (121). С. 40-43.

<sup>210</sup> Cabral L., Haucap J., Parker G., Petropoulos G., et al. *The EU Digital Markets Act*. Publications Office of the European Union, Luxembourg, 2021. P. 1-36.

<sup>211</sup> Европейская стратегия «Лучший Интернет для детей+» (European strategy for a better Internet for kids (BIK+)) 11/05/2022. URL: <https://eur-lex.europa.eu> (дата обращения: 01.05.2025).

ксенофобский, террористический контент или материалы о сексуальном насилии над детьми».

Уточним, что Стратегия «Лучший Интернет для детей» (BIK+) является пересмотренной и актуализированной (в том числе с учетом обсуждаемых положений Закона о цифровых услугах (DSA)) «Лучший интернет для детей» 2012 года<sup>212</sup>, а также учитывает предложенную Европейской Комиссией в 2022 году «Европейскую декларацию о цифровых правах и принципах цифрового десятилетия» (European Declaration on Digital Rights and Principles for the Digital Decade)<sup>213</sup>, которая среди прочих предложенных прав предусматривает следующее: детям и молодежи должны быть предоставлены возможности осуществлять безопасный и информированный выбор и выражать свое творчество в онлайн-среде; дети имеют право быть защищенными от всех преступлений, совершаемых через или при содействии цифровых технологий; каждый имеет право на защиту своих персональных данных в сети; каждый должен иметь доступ к цифровым технологиям и услугам, которые являются безопасными и защищающими конфиденциальность; каждый имеет право на свободу выражения своих убеждений в онлайн-среде без боязни подвергнуться цензуре или запугиванию.

Стратегия «Лучший Интернет для детей» (BIK+) фундирована тремя основными принципами: 1) обеспечение информационной безопасности несовершеннолетних от незаконного и вредоносного контента, поведения и рисков, а также улучшение их благополучия с помощью безопасной, соответствующей возрасту цифровой среды; 2) расширение возможностей цифровых технологий, чтобы дети приобрели необходимые навыки и компетенции делать осознанный выбор и безопасно и ответственно выражать себя в онлайн-среде; 3) активное участие детей, с предоставлением им права голоса в цифровой среде, проведением большего количества мероприятий под руководством детей, чтобы способствовать

---

<sup>212</sup> European Strategy for a Better Internet for Children (BIK) 02/05/2012. URL: [https://eur-lex.europa.eu/legal-content/en \(expired\)](https://eur-lex.europa.eu/legal-content/en (expired) (дата обращения: 01.05.2025).) (дата обращения: 01.05.2025).

<sup>213</sup> European Declaration on Digital Rights and Principles for the Digital Decade 28/12/2022. URL: [https://eur-lex.europa.eu/legal-content/en](https://eur-lex.europa.eu/legal-content/en (дата обращения: 01.05.2025).) (дата обращения: 01.05.2025).

инновационному и творческому безопасному цифровому опыту<sup>214</sup>. Как отмечает А. А. Мензелинцева, в рамках ЕС были реализованы различные программы, адресованные не только государствам-членам, но и всем заинтересованным лицам, включая самих несовершеннолетних. Опыт ЕС представляется достаточно позитивным, поэтому он может быть смело заимствован государствами, не являющимися государствами – членами ЕС, для обеспечения информационной безопасности несовершеннолетних от деструктивного контента<sup>215</sup>.

В рамках исследуемой темы следует сказать и о возникшем концептуальном обобщении<sup>216</sup> «модель информационного беспорядка MDM (misinformation, disinformation, malinformation)»<sup>217</sup>. Ошибочная информация (misinformation) представляет собой поддающуюся проверке ложную информацию, распространяемую без намерения ввести в заблуждение, которой часто обмениваются, потому что пользователь верит, что она правдивая<sup>218</sup>. Под дезинформацией (disinformation) понимается поддающаяся проверке ложная информация или информация, вводящая в заблуждение, создаваемая, представляемая и распространяемая для экономической выгоды или для умышленного обмана общественности. Она может нанести вред общественности. Недобросовестная информация (malinformation) представляет собой фактически правдивую информацию, используемую для нанесения вреда.

<sup>214</sup> Press release. Strategy to protect and empower children in the online world. European Commission. 11.05.2022. URL: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_2825](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2825) (дата обращения: 01.05.2025).

<sup>215</sup> Мензелинцева А. А. Защита прав ребенка в цифровом пространстве в рамках Европейского Союза // Международное право прав человека: состояние и перспективы : материалы круглого стола XVIII Международного конгресса «Блищенковские чтения». Москва, 10 декабря 2022 г. = International Law of Human Rights: Current Status and Perspectives: Proceedings of the Roundtables Discussion of the XVIII Blischenko Congress. Moscow, 10 December 2022 / Отв. ред. А. Х. Абашидзе. М. : РУДН, 2023. С. 74-79.

<sup>216</sup> Santos-D'Amorim K., de Miranda, M. K. F. d. O. Misinformation, disinformation, and malinformation: Clarifying the definitions and examples in disinfodemic times. *Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação*. 2021. № 26. P. 1-23; Nolan S. A., Kimball M. The Intent behind a Lie: Mis-, Dis-, and Malinformation. Can you differentiate among the varieties of untruths you encounter online? // *Psychology Today*. 2021. URL: <https://www.psychologytoday.com/> (дата обращения: 30.03.2025).

<sup>217</sup> The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation (ed. by R. Greifeneder, M. E. Jaffé, E. J. Newman, N. Schwarz). 2020. N.Y. : Routledge. xii + 240 p.; Greene S., Asmolov G., Fagan A., Fridman O., Gjuzelov B. Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them. Study requested by the AFET Committee. European Parliament: Policy Department for External Relations, Directorate General for External Policies of the Union. PE 653.621. 2021. 104 p.; Сургуладзе В. Ш. Новые категории информационной борьбы: mis-, dis-, malinformation и правовые последствия использования модели информационного беспорядка mdm // *Власть*. 2024. Т. 32. № 1. С. 23-30.

<sup>218</sup> Module 8. (2022) «False News», Misinformation and Propaganda. Summary Modules on litigating Digital Rights and Freedom of Expression Online. London : Media Defense. 11 p.

Также следует сказать о Директиве Европейского Парламента и Совета ЕС 2010/13/ЕС от 10 марта 2010 года «О координации некоторых законодательных, регламентарных и административных положений, действующих в государствах – членах ЕС, относительно оказания аудиовизуальных медиауслуг» (AVMSD))<sup>219</sup>, которая была пересмотрена в 2018 году и регламентирует принятие мер для эффективной системы проверки возраста и, при необходимости, инструменты родительского контроля. Цель обновленной директивы: не допустить, чтобы несовершеннолетние подвергались воздействию вредоносного контента (безнравственного насилия, порнографии и т. д.), который может негативно сказаться на их психическом развитии. Уточним, что аудиовизуальные медиауслуги также оказываются и в цифровой среде.

Рассмотрим наиболее интересные примеры национального законодательства государств – членов ЕС. Так, итальянский парламент еще в 2017 году утвердил Legge n. 71/2017 sul cyberbullismo<sup>220</sup> для предотвращения и противодействия киберзапугивания, согласно которому родители детей или несовершеннолетние старше 14 лет могут потребовать от сайтов, размещающих контент, удалить вредоносные материалы в течение 48 часов. Законодательный декрет № 208 от 8 ноября 2021 года<sup>221</sup> определяет виды контента, которые могут нанести ущерб физическому, умственному или нравственному развитию несовершеннолетних, а именно в статьях 37 и 38 (перевод ст. 6а (1) AVMSD) о программах, которые могут нанести серьезный вред несовершеннолетним, включая те, которые содержат: необоснованное, настойчивое или экстремальное насилие; порнографические сцены; фильмы, которые были запрещены компетентными органами для публичного показа детям младше 18 лет.

<sup>219</sup> Directive 2010/13/EU on audiovisual media services (Audiovisual Media Services Directive). URL: <https://digital-strategy.ec.europa.eu/en/policies/audiovisual-and-media-services> (дата обращения: 30.03.2025).

<sup>220</sup> Legge n. 71/2017 sul cyberbullismo Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo. (17G00085) (GU n.127 del 3-6-2017). URL: // <https://www.senato.it/> (дата обращения: 30.03.2025).

<sup>221</sup> Decreto legislativo 8 novembre 2021, n. 208 Attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato. (21G00231). URL: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:DECRETO.LEGISLATIVO:2021-11-08;208!vig=> (дата обращения: 30.03.2025).

Во Франции в целях обеспечения информационной защиты несовершеннолетних в сети «Интернет» принят и действует ряд законов: Закон от 17 июня 1998 года о предупреждении и наказании половых преступлений и защите несовершеннолетних<sup>222</sup>, Закон от 4 апреля 2006 года об усилении профилактики и пресечении насилия в паре или в отношении несовершеннолетних<sup>223</sup>, а также Закон от 5 марта 2007 года, касающийся предупреждения правонарушений<sup>224</sup>, в которых термин «телекоммуникации» заменен термином «электронная сеть связи». Так, согласно ст. 7–1, 20 французского закона № 2018-493 от 20.06.2018 о защите персональных данных<sup>225</sup> устанавливается, что в контексте онлайн-сервисов и обработки данных на основании согласия пользователя, не являющегося договором, лицо (лица), обладающее родительскими правами, должно дать свое согласие совместно с ребенком, если последнему не исполнилось 15 лет. Это означает, что согласие на дополнительные функции, такие как установка публичного/частного статуса профиля в социальной сети или активация дополнительной геолокации в приложении, теоретически должно быть основано на совместном согласии ребенка и лица (лиц), обладающего родительскими правами, то есть родители не могут идти против воли ребенка в вопросах такого рода обработки данных, а ребенок не может игнорировать возражения родителей. Предоставление детям права распоряжаться своими данными при сохранении родительского контроля в эпоху цифровых технологий – огромное преимущество<sup>226</sup>.

Франция предприняла значительные шаги по защите детей в Интернете, приняв в марте 2022 года закон № 2022-300 об усилении родительского контроля над средствами доступа в сети «Интернет» (LOI n° 2022-300 du 2 mars 2022 visant à

<sup>222</sup> LOI n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs. URL: <https://www.legifrance.gouv.fr> (дата обращения: 01.05.2025).

<sup>223</sup> Loi n° 2006-399 du 4 avril 2006 renforçant la prévention et la répression des violences au sein du couple ou commises contre les mineurs (law reinforcing the prevention and repression of violence within couple or against minors). URL: <https://www.legifrance.gouv.fr> (дата обращения: 01.05.2025).

<sup>224</sup> Law no. 2007-297 of 5 March 2007 relating to the prevention of delinquency intends to improve the means for preventing delinquency by minors. URL: <https://eur-lex.europa.eu/eli/lex/2007/297/2007-03-05/eng> (дата обращения: 01.05.2025).

<sup>225</sup> LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952> (дата обращения: 01.05.2025).

<sup>226</sup> Талапина Э. В. Цифровая трансформация во Франции: правовые новеллы // Право. Журнал Высшей школы экономики. 2019. № 4. С. 164–184.

renforcer le contrôle parental sur les moyens d'accès à internet)<sup>227</sup>, который предписывает устанавливать системы родительского контроля на все продаваемые во Франции устройства с поддержкой Интернета, чтобы блокировать доступ несовершеннолетних к услугам и контенту, которые могут нанести вред их физическому, умственному или моральному развитию (абз. 1 ст. 1 LOI n° 2022-300). Средства контроля, доступные при активации устройства, являются важнейшим компонентом законодательства 2022 года, направленного на защиту детей от нежелательного онлайн-контента (абз. 3–5 ст. 1 LOI n° 2022-300). Таким образом, платформы социальных сетей не должны быть доступны для лиц, которым не исполнилось 15 лет либо же только при условии согласия законного представителя на создание аккаунта для несовершеннолетнего в социальных сетях; также законные представители (как правило, родители) вправе обратиться для удаления аккаунта в социальных сетях несовершеннолетнего, которому менее 15 лет. Таким образом, в законе LOI n° 2022-300 du 2 mars 2022<sup>228</sup> в абз. 1 ст. 1 указано: «контент, который может нанести вред их физическому, умственному или моральному развитию» без закрытого перечня этой информации и каких-либо легальных определений.

Существуют определенные законы Германии, которые содержат некоторые положения, касающиеся конфиденциальности в Интернете.

Закон об улучшении правоприменения в социальных сетях (Закон о правоприменении в сети 2017 года – *Netzwerkdurchsetzungsgesetz (NetzDG)*)<sup>229</sup>, целью которого является правовой механизм быстрого удаления с онлайн-платформ (социальных сетей) деструктивного контента. Так, с момента жалобы пользователя платформы в течение 24 часов оператор социальной сети должен произвести удаление или блокировку «явно незаконного» контента. Если отнесение контента к разрешенному или запрещенному требует дополнительной оценки (проверки), то

<sup>227</sup> LOI n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet. URL: <https://www.legifrance.gouv.fr> (дата обращения: 01.05.2025).

<sup>228</sup> Там же.

<sup>229</sup> *Netzwerkdurchsetzungsgesetz* vom 1. September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 29 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist. URL: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> (дата обращения: 01.05.2025).

эти действия осуществляются в пределах семи дней. Ответственность социальных сетей за систематическое несоблюдение положений NetzDG предусматривает штраф до 50 млн евро.

Рассмотрим содержание информации (контента), которая попадает под действие NetzDG, так называемого в правовой среде «Закона о защите прав пользователей сети» (термин N. Guggenberger<sup>230</sup>). Так, в сферу действия закона попадают сообщения, распространение которых является нарушением норм немецкого УК (Strafgesetzbuch – StGB)<sup>231</sup>. Перечень этих параграфов приведен в абз. 3 § 1 Закона о сетях. Всего упомянуты 22 параграфа. Для нас интересен подход немецкого законодателя к определению информации (контента), причиняющего вред здоровью или (и) развитию несовершеннолетнего. Однако в абз. (3) § 4а употребляется термин «незаконный контент» без легальной трактовки и/или характеристик этого понятия. Также во исполнение закона NetzDG в 2022 году комиссия по защите молодежи в медиасфере Германии (Kommission für Jugendmedienschutz) одобрила использование ИИ-систем, которые определяют возраст пользователя по биометрическим данным, чтобы оградить несовершеннолетних от вредоносного контента. Таким образом, можно сказать, в немецком законодательном акте выбран путь закрытого перечня информации (контента), который может причинять несовершеннолетнему вред, без легального определения понятия «вредоносный контент».

Как отмечает В. Г. Романовский, нормы закона NetzDG 2017 года отчасти продублированы в российском законе 2021 года № 236-ФЗ<sup>232</sup> в части законодательных российских требований для ключевых технологических компаний Google, Facebook, социальная сеть «X» (ранее - «Twitter»): создание филиала или представительства на территории РФ, регистрация личного кабинета на сайте

<sup>230</sup> Guggenberger N. Das Netzwerkdurchsetzungsgesetz in der Anwendung // Neue Juristische Wochenschrift. 201. № 36. Pp. 2577-2582.

<sup>231</sup> Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nr. 351) geändert worden ist. URL: <https://www.gesetze-im-internet.de/stgb/BJNR001270871.html> (дата обращения: 01.05.2025).

<sup>232</sup> Федеральный закон от 01.07.2021 № 236-ФЗ (ред. от 22.06.2024) «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» // СЗ РФ. 2021. № 27 (часть I). Ст. 5064; Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>. 22.06.2024.

Роскомнадзора, закрепление механизма рассмотрения обращений российских пользователей при нарушении их прав<sup>233</sup>. Опыт Германии активно изучается и обсуждается в других странах как пример возможного подхода к борьбе с распространением незаконного и вредоносного контента в интернете. Исходя из всего вышесказанного, можно только согласиться с мнением Д. С. Емельянова, что на «уровне одного отдельно взятого государства крайне сложно построить эффективный механизм административного воздействия на иностранные социальные сети, не прибегая к их блокировке»<sup>234</sup>.

Считаем возможным также уточнить, что понятие «контент», которое активно используется в европейском законодательстве, в то же время законодательно не закреплено. В Конвенции о киберпреступности<sup>235</sup> содержание этого термина не раскрывается, однако в Пояснительном докладе к Конвенции<sup>236</sup> также не представлено определение понятия «контент», но указано, что компьютерное сообщение составляют три типа данных: данные трафика, данные абонента и данные контента. Относительно данных контента в Пояснительном докладе к Конвенции (п. 136) сказано, что они указывают на «коммуникационное содержание сообщения», а именно на «значение или цель связи, сообщения или передаваемой информации». Следовательно, данные контента представляют собой самостоятельную категорию, определяющую качественное содержание размещаемой информации<sup>237</sup>. Так, в научной статье «Регулирование дезинформации в ЕС: обзор и открытые вопросы» профессора, доктора юридических наук А. Пеукерта (Alexander Peukert) используется термин «вредоносный» контент («harmful» content)<sup>238</sup>, но ему не дается авторской

<sup>233</sup> Романовский В. Г. Правовые основы противодействия терроризму в цифровом пространстве // *Ex Jure*. 2022. № 4. С.163-177.

<sup>234</sup> Емельянов Д. С. Ограничение права на свободу слова в эпоху социальных сетей // *Образование и право*. 2021. № 3. С.46-53.

<sup>235</sup> Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г., с изм. от 28.01.2003) // СПС «КонсультантПлюс».

<sup>236</sup> Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001. URL: <https://rm.coe.int/16800cce5b> (дата обращения: 01.05.2025).

<sup>237</sup> Кириллова Н. М. Негативный контент в информационно-телекоммуникационной сети Интернет: проблемы определения и классификации // *Вестник Московского университета. Серия 11: Право*. 2018. № 4. С. 116-127.

<sup>238</sup> Peukert A. The Regulation of Disinformation in the EU – Overview and Open Questions (June 30, 2023) // *Research Paper of the Faculty of Law of Goethe University Frankfurt/M*. 2023. № 2/2023. URL: SSRN: <https://ssrn.com/abstract=4496691> (дата обращения: 30.03.2025).



трактовки. Сам термин «вредоносный контент» достаточно распространен в научных трудах, но употребляется европейскими авторами без определений (M. Kladzinski, C. Büttne, E. Staksrud, S. Livingstone, V. A. M. Talley, M. Watney; F. R. Moreno)<sup>239</sup>.

В результате анализа информации, причиняющей вред здоровью, жизни, развитию малолетних и подростков, представленного в двух параграфах, посвященных российскому и зарубежному деструктивному контенту (Приложение А), предлагается авторская классификация вредоносного (деструктивного) контента для несовершеннолетних лиц в сети «Интернет»:

1) *незаконный (запрещенный) контент международного уровня*, представленный общепринятым противоправным контентом и включающим в себя: контент со сценами сексуальных надругательств над несовершеннолетними лицами или их сексуальной эксплуатации<sup>240</sup>; контент о жестоком обращении с несовершеннолетним лицом; информацию, которая склоняет к терроризму несовершеннолетних лиц; необоснованное или экстремальное насилие; незаконный дискриминационный контент (по признакам расы, цвета кожи, пола, религии, национальной принадлежности или социального происхождения); информацию, содержащие призывы к самоубийству или самоповреждению (членовредительству).

Следует обозначить следующее:

– нами используется термин «международный», так как имеется принятая резолюцией 79/243 Генеральной Ассамблеи от 24.12.2024 Конвенция ООН против

<sup>239</sup> Kladzinski M. Jugendmedienschutz in Polen // tv-diskurs. 2003. № 23. P. 4-1; Büttne C. The Protection of Minors Against Harmful Media Content in Europe // Nordicom Review. 2005. № 26(1). P. 121-129; Staksrud E., Livingstone S. Children and online risk: Powerless victims or resourceful participants? // Information, Communication & Society. 2009. № 12(3). P. 364-387; Talley V. A. M. Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR // Indiana Int'l & Comp. // Law Review. 2019. № 30(1). P. 127-162; Watney M. Regulation of social media intermediary liability for illegal and harmful content // European Conference on Social Media. 2022. № 9(1). P. 194-201; Moreno F. R. Generative AI and deepfakes: a human rights approach to tackling harmful content // International review of law, computers & technology. 2024. Vol. 38 (№ 3). P. 297–326.

<sup>240</sup> Ст. 14 – Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (принята резолюцией 79/243 Генеральной Ассамблеи от 24.12.2024. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243> (дата обращения: 31.08.2025)).

киберпреступности, содержащая один из видов незаконного (запрещенного) контента международного уровня;

– дискриминационные признаки, которые мы указали, также обозначены и в общепризнанных актах<sup>241</sup>;

– нами включен в этот перечень такой вид контента, как «склонение к самоубийству», хотя на уровне законодательства ЕС имеются особенности: так, в Законе о цифровых услугах (DSA) этот вид контента не упоминается в открытом перечне незаконного контента, а в Примечании (26) Стратегии ВІК+ указан как «суицид» в описательной части как «вредного контента», а не «незаконного» (отметим, что в Стратегии ВІК+ обозначено «суицид», а не «склонение к суициду»). Аналогичен подход Великобритании, при котором «информация, которая поощряет, пропагандирует или содержит инструкции по совершению самовредительства и (или) самоубийства», отнесена не к незаконной, а к контенту с высоким приоритетом вреда.

Однако ввиду нормативного регламентирования этого вида контента и несомненной общественной опасности, мы включили этот контент в международный незаконный контент для несовершеннолетних. Кроме того, при такой классификации нами учитываются положения ч. 2 и ч. 3 ст. 5 Закона № 436-ФЗ РФ, согласно которым разграничивается контент, содержащий призывы к самоубийству (самовредительству) и контент с изображением и (или) описанием самоубийства (самовредительства), так как первый наносит вред непосредственно жизни несовершеннолетнего, а второй имеет в первую очередь деструктивное влияние на его психоэмоциональное состояние и развитие;

2) *незаконный (запрещенный или ограниченный) контент национального, наднационального уровня, представленный противоправной информацией, распространение которой, в том числе в сети «Интернет», запрещено согласно национальным законодательствам и (или) наднациональным (например, на уровне*

---

<sup>241</sup> Например: Международная конвенция о ликвидации всех форм расовой дискриминации (Заключена 21.12.1965, с изм. от 15.01.1992) // Ведомости ВС СССР. 18.06.1969. № 25. Ст. 219 (ратифицировано СССР); Конвенция № 111 Международной организации труда «Относительно дискриминации в области труда и занятий» (принята в г. Женеве 25.06.1958 на 42-й сессии Генеральной конференции МОТ) // Ведомости ВС СССР. 1 ноября 1961 г. № 44. Ст. 448 (ратифицировано СССР)

ЕС) законодательствам. Этот вид контента в значительной мере обусловлен историко-культурными особенностями государств, действующими нормативными актами. Например, в РФ запрещенная информация включает в себя информацию, согласно ч. 2 ст. 5 Закона № 436-ФЗ: «отрицающую семейные ценности» и «пропагандирующую либо демонстрирующую нетрадиционные сексуальные отношения и (или) предпочтения», а также согласно ч. 1 ст. 5 Закона № 436-ФЗ информацию, способную нанести вред несовершеннолетнему: «4.3) способную вызвать у детей желание сменить пол». Однако, например, согласно ст. 62 Online Safety Act Великобритании «приоритетный контент, вредный для детей», означает «контент, направленный на дискриминацию смены пола» – которая, подчеркнем, законодательно запрещена в России (ст. 6.21 КоАП РФ).

Незаконный контент национального (наднационального) уровня может быть запрещен к распространению (например, пропаганда запрещенных наркотических веществ) или же иметь ограничения по возрастным критериям (например, откровенный контент или содержащий сцены жестокости);

3) *нежелательный контент* – контент, который не указан в законодательно закрепленных перечнях деструктивного контента государств, но из оценки которого выявляется, что он представляет опасность причинения вреда несовершеннолетним.

Например, в законодательстве РФ нет прямого запрета или ограничения упоминаний «эскорт-услуг». Однако сайты в сети «Интернет», посвященные этой тематике, были заблокированы по решению суда, который указал, что «размещенная на этих ресурсах информация о платных сексуальных услугах способствует пропаганде проституции, нарушает права неопределенного круга лиц, включая несовершеннолетних, противоречит требованиям законодательства и наносит вред общественной морали и здоровью»<sup>242</sup>.

В целом можно сказать, что в той или иной степени информация, наносящая вред развитию несовершеннолетних, чаще всего распространяется с помощью сети

---

<sup>242</sup> Официальный сайт АО «Газета.Ру». URL: <https://www.gazeta.ru/social/news/2025/08/26/26580014.shtml?updated> (дата обращения: 31.08.2025).

«Интернет», поэтому информация (вредоносный контент), причиняющая вред или представляющая угрозу жизни и (или) здоровью несовершеннолетних, их моральному и психическому состоянию, ограничивается или запрещается в сети «Интернет»<sup>243</sup>. Иными словами, информация, наносящая вред развитию несовершеннолетних с помощью сети «Интернет», характеризуется побуждением правонарушителей склонить несовершеннолетних к совершению посягательства на свое здоровье и жизнь или оказанием на подростков иного влияния, находящегося в коллизии с морально-нравственными отношениями, устоями общества и нормами, принятыми в государстве.

#### **1.4. Концептуальные подходы к пониманию категории «информационная безопасность» в законодательстве и юридической науке**

Современные информационные технологии не только открывают безграничные возможности для развития российского общества, но и порождают новые проблемы, вызовы и угрозы его безопасности, одна из важнейших ее составляющих – информационная безопасность<sup>244</sup>.

Несомненно, в настоящее время актуально правовое обеспечение несовершеннолетних в информационной сфере, что обусловлено, как справедливо отмечают Н. В. Новикова и Е. А. Брылева, как возрастными, психологическими и физиологическими особенностями формирующейся личности, так и тем, что несовершеннолетние в наибольшей степени подвержены негативному воздействию информации, наносящей вред их здоровью и нравственному развитию<sup>245</sup>. В этом параграфе диссертационного исследования будет рассмотрено концептуальное

---

<sup>243</sup> Любченко М. И. Правовые основы защиты несовершеннолетних от информации, причиняющей вред их здоровью и духовному развитию // Тенденции развития современной юриспруденции : материалы VII Всероссийской студенческой научно-практической конференции Юридического института Балтийского федерального университета имени Иммануила Канта, Калининград, 19–21 апреля 2019 г. / Под общ. ред. О. А. Заячковского. Калининград : Издательство Балтийского федерального университета имени Иммануила Канта, 2019. С. 63; Ситкова О. Ю. Механизмы регулирования информационного потребления в странах Европейского Союза в целях обеспечения кибербезопасности детей // Правовая политика и правовая жизнь. 2021. № 4. С. 58–68.

<sup>244</sup> Смирнов А. И. Информационная глобализация и Россия: вызовы и возможности. М., 2005. С. 235.

<sup>245</sup> Новикова Н. В., Брылева Е. А. О некоторых аспектах информационной безопасности несовершеннолетних на примере Пермского края // Вопросы ювенальной юстиции. 2013. № 6. С. 7–9.

понимание «информационной безопасности» и «кибербезопасности» в юридической науке и законодательстве РФ, Австралии, Великобритании, Франции, постепенно раскрывая особенности непосредственного понятия «информационная безопасность несовершеннолетних».

Понятия «информационная безопасность» и «кибербезопасность» являются дискуссионными. В немалой степени это продиктовано именно тем, что эти термины являются относительно новыми для общества и государственных органов, принимающих нормативные правовые акты, направленные в том числе и на обеспечение информационной безопасности. Определение международной информационной безопасности на уровне ООН было дано еще в 2000 году и представляет собой «состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве»<sup>246</sup>, а также «состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве»<sup>247</sup>. Таким образом, в этом случае предполагается именно защита как отдельного человека, так государства от деструктивной информации в рамках информационного пространства. Определение кибербезопасности, которое использует ООН, было предложено в 2010 году Международным союзом электросвязи (МСЭ), а позднее доработано Н. Кшетри (N. Kshetri)<sup>248</sup>: «кибербезопасность подразумевает технологии, концепции, меры государственной политики, процедуры и практики, направленные на защиту активов (компьютеров, инфраструктуры, приложений, услуг, систем связи и информации) и киберпространства от атак, нанесения ущерба и неавторизованного доступа»<sup>249</sup>.

<sup>246</sup> Резолюция 55/33 Генеральной Ассамблеи ООН «Всеобщее и полное разоружение» (Принята в г. Нью-Йорке 20.11.2000 на 69-м пленарном заседании 55-й сессии Генеральной Ассамблеи ООН) // СПС «Гарант», заковичен текст, опубликованный: Прохорова Д. А. Международная информационная безопасность как современная проблема // Информационное общество. 2022. № 5. С. 80-90.

<sup>247</sup> Конвенция об обеспечении международной информационной безопасности. URL: <https://interkomitet.ru/> (дата обращения: 01.05.2025).

<sup>248</sup> Определение было принято в ходе Полномочной конференции МСЭ в Гвадалахаре (Мексика) в 2010 г. - Kshetri N. (2016) *Global Cybersecurity: Key Issues and Concepts. The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies* / N. Kshetri (ed.). Springer International Publishing, p. 3.

<sup>249</sup> International Telecommunications Union (ITU) (2008). *Overview of Cybersecurity, Recommendation ITU– T X.1205*. URL: <https://www.itu.int/rec/T-REC-X.1205-200804-I> (дата обращения: 01.05.2025).

Несомненно, первоочередной задачей любого государства является охрана здоровья и нравственности детей как демографического ресурса нации и объекта национальной безопасности, подлежащего первоочередной защите. Соответственно, как указывают А. С. Дугенец и Л. В. Павлова, «безопасность несовершеннолетних в информационном поле необходимо рассматривать в контексте национальной безопасности государства»<sup>250</sup>. Так, в РФ национальная безопасность определена как состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан РФ, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие РФ<sup>251</sup>. Такая широкая трактовка позволяет говорить о том, что составной частью национальной безопасности является информационная безопасность. В научной статье Т.А. Полякова и А. А. Смирнов абсолютно справедливо отмечают, что информационную безопасность нельзя считать константой, «неизменной величиной»<sup>252</sup>, ведь совершенствование информационных технологий становится источником появления ранее не существовавших информационных угроз, которые, в свою очередь, требуют эффективного и своевременного правового реагирования. Современные технологии постоянно порождают новые виды (разновидности) деструктивных информационных угроз, таких как киберхарассмент, треш-стримы, флейминг, гриферство, троллинг, фейки, киберсталкинг, секстинг и т. д., которые распространяются за пределы отдельного государства или наднационального объединения, носят массовый характер и требуют мер правового пресечения на государственном и международном уровне.

---

<sup>250</sup> Дугенец А. С., Павлова Л. В. Государственное регулирование обеспечения информационной безопасности несовершеннолетних как составляющая национальной безопасности России // Административное право и процесс. 2023. № 5. С. 22-25.

<sup>251</sup> Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (часть II). Ст. 5351.

<sup>252</sup> Полякова Т. А., Смирнов А. А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Российский юридический журнал. 2022. № 3. С. 7-15.

Вышеобозначенное получило отражение и в Указе Президента РФ от 12.04.2021 № 213<sup>253</sup>, устанавливающем основы российской государственной политики в области международной информационной безопасности. Россия входит в ряд межгосударственных организаций. В рамках Содружества независимых государств (СНГ), Организации Договора о коллективной безопасности (ОДКБ) и Шанхайской организации сотрудничества (ШОС) тоже имеется свое видение понятия «информационная безопасность». Так, в рамках СНГ и ОДКБ дается идентичное определение этого термина как состояния защиты первоочередно личности, затем общества, а в последнюю очередь государства от негативного воздействия в информационном пространстве<sup>254</sup>.

Информационная безопасность в силу своей специфики также может рассматриваться и как состояние защищенности определенных субъектов (личность, общество, государство), и как свойство чего-либо (определенных объектов), позволяющее обеспечивать защиту (например, безопасность используемых технических средств)<sup>255</sup>.

Представляет научный интерес проведенный С. А. Авакьяном анализ направлений опасностей в информационной сфере. Он отмечает, что «добившись конституционных и в целом нормативных гарантий права на информацию, на ее создание и распространение, на владение информацией, тем более права на защиту информации, мы сталкиваемся с повальной необходимостью защиты *от* информации», наглядно показывая, что «свобода информации очень быстро продемонстрировала свою обратную сторону – возможность проявления неуважения к личности, неуправляемое заимствование и распространение частных (персональных) данных, а тем более лжи и клеветы, беззащитность человека»<sup>256</sup>. В

<sup>253</sup> Указ Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СЗ РФ. 2021. № 16 (Часть I). Ст. 2746.

<sup>254</sup> Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. // Бюллетень международных договоров. 2019. № 9; Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. // Бюллетень международных договоров. 2015. № 10. С. 7-13.

<sup>255</sup> Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере : монография / Н. С. Волкова, А. А. Ефремов, С. М. Зырянов и др.; отв. ред. Л. К. Терещенко. М. : Инфотропик Медиа, 2024. С. 7.

<sup>256</sup> Авакьян С. А. Задачи конституционного права в аспекте защиты (от) информации // Конституционное и муниципальное право. 2022. № 8. С. 3-11.

этом контексте, по мнению Т. М. Гришиной, к основным информационным угрозам в сетевом пространстве, как правило, относят: «открытый доступ к вредоносной информации; идеологическое загрязнение сетей; отсутствие барьеров; неконтролируемые контакты; недостаточность правовых знаний о работе с информацией, авторском праве и др.»<sup>257</sup>

Вопрос об информационной безопасности в рамках законодательства России начал подниматься с начала 1990-х гг., когда был принят закон о правовой защите компьютерных программ в 1992 г.<sup>258</sup> и логическое, актуализированное регламентирование было в 2006 г. представлено в законе об информации, информационных технологиях и о защите информации», в ч. 1 ст. 2 которого указано, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации.

В некоторых нормативных правовых актах и публикациях речь идет о «безопасности информации». Это действительно важная составляющая информационной безопасности, но она не сводится исключительно к безопасности информации<sup>259</sup>. В настоящее время с появлением новых технологий и новых угроз на первый план выдвигаются другие составляющие информационной безопасности – например, непосредственно защита самой информации от неправомерного доступа к ней, в том числе в сети «Интернет».

Построение системы информационной безопасности несовершеннолетних в России базируется на международных, конституционных принципах и правовых

<sup>257</sup> Гришина Т. М. Обеспечение безопасности российского бизнеса в сетевом обществе: некоторые правовые вопросы // Безопасность бизнеса. 2017. № 4. С. 3-8.

<sup>258</sup> Закон РФ от 23.09.1992 № 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных» // Ведомости СНД РФ и ВС РФ. 1992. № 42. Ст. 2325; Российская газета. 08.02.2006. № 25 (утратил силу).

<sup>259</sup> Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. ГОСТ Р 52448-2005 (утв. Приказом Ростехрегулирования от 29.12.2005 № 449-ст). М. : Стандартинформ, 2006.



нормах в области охраны семьи и детства, развития и воспитания детей на основе традиционных российских духовно-нравственных ценностей, к которым государство относит прежде всего жизнь, достоинство, права и свободы человека, патриотизм, высокие нравственные идеалы, крепкую семью, созидательный труд, приоритет духовного над материальным, гуманизм, милосердие, справедливость, коллективизм, взаимопомощь и взаимоуважение, историческую память и преемственность поколений, единство народов России<sup>260</sup>.

Согласно Указу Президента РФ от 05.12.2016 № 646 информационная безопасность РФ – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства<sup>261</sup>. Можно сказать, что под информационной безопасностью значит именно обеспечение, во-первых, гарантированных нормами Конституции РФ прав и свобод человека и гражданина, так как они являются высшей ценностью в нашем государстве, во-вторых, делается акцент на государственной безопасности в широком смысле слова, так как к ней можно отнести и социально-экономические правоотношения. В разделе «1. Общие положения» Распоряжения Правительства РФ от 22.12.2022 № 4088-р<sup>262</sup> имеется разделение угроз информационной безопасности в зависимости от «точки зрения»: 1) техническая; 2) психологическая. К первой точке зрения относится неправомерный доступ к информационным ресурсам или нарушение их функционирования и т. д. Ко второй точке зрения относится распространение деструктивного контента.

В связи с вышесказанным законодательство в сфере информационной безопасности образует два блока: 1) нормы, устанавливающие правовой режим

<sup>260</sup> Указ Президента РФ от 2 июля 2021 г. N 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. N 27 (часть II). Ст. 5351.

<sup>261</sup> Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

<sup>262</sup> Распоряжение Правительства РФ от 22.12.2022 № 4088-р «Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации» // СЗ РФ. 2022. № 52. Ст. 9726.

информации, права, обязанности, ответственность субъектов информационных отношений, меры по созданию и обеспечению состояния информационной защищенности тех или иных объектов, формированию единой среды доверия; 2) нормы, устанавливающие требования к техническим средствам, сетям связи, условия передачи информации и т. п., что обуславливает их свойство обеспечивать защищенность информации и самих объектов.

Поэтому, исходя из анализа положений Распоряжения Правительства РФ от 22.12.2022 № 4088-р, можно сделать вывод, что угрозы информационной безопасности с психологической точки зрения в значительной степени коррелируют с содержанием (характеристикой) информации, причиняющей вред здоровью и развитию несовершеннолетних, ведь согласно ст. 2 Закона № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»: «информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию». Также следует указать корреляцию с нормами ст. 14 Закона № 124-ФЗ<sup>263</sup>, регламентирующей защиту несовершеннолетних от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию. Таким образом, еще раз приходим к выводу, который достаточно четко изложил Л. К. Терещенко: «Время, новые технологии, вызовы и угрозы меняют приоритеты, требования к информационной безопасности, что предполагает адекватное реагирование»<sup>264</sup>. Более того, меняется и объем, и состав информационной безопасности. При этом содержательно информационная безопасность одной группы субъектов может частично не совпадать с информационной безопасностью другой группы субъектов.

<sup>263</sup> Федеральный закон от 24.07.1998 № 124-ФЗ (ред. от 30.11.2024) «Об основных гарантиях прав ребенка в Российской Федерации» // СЗ РФ. 1998. № 31. Ст. 3802; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>264</sup> Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере : монография / Отв. ред. Л. К. Терещенко. М. : Инфотропик Медиа, 2024.

Неслучайно в Доктрине информационной безопасности РФ<sup>265</sup> речь идет о сбалансированных интересах личности, общества и государства в информационной сфере. Безопасность может различаться и внутри одной группы субъектов. Например, «информационная безопасность личности взрослого человека содержательно не совпадает с информационной безопасностью детей и подростков»<sup>266</sup>. Следует сказать, что на уровне отраслевого законодательства происходит конкретизация положений, касающихся информационной безопасности в определенной сфере с учетом существующих особенностей.

Так, согласно Распоряжению Правительства РФ от 28.04.2023 № 1105-р<sup>267</sup>, несовершеннолетние выделяются в отдельную крайне уязвимую аудиторию с точки зрения информационной безопасности, так как, с одной стороны, имеется риск проявления асоциальных форм поведения в цифровой среде; с другой же, нестабильность эмоциональной сферы и низкий уровень критичности восприятия и обработки информационного потока детьми и подростками свидетельствуют о том, что именно дети и подростки находятся в группе потенциального риска для негативного воздействия и интернет-манипуляций с последующим вовлечением в деструктивную деятельность.

Концепция информационной безопасности детей в России 2023 года перечисляет основные принципы обеспечения информационной безопасности детей, приоритетные задачи государственной политики в области информационной безопасности детей. Проанализировав правовые нормы российского права, регламентирующего информационную безопасность несовершеннолетних, можно сделать вывод, что информационное законодательство РФ, с одной стороны, достаточно обширно и охватывает международные, национальные сферы правовой регламентации, с другой стороны, имеет разрозненный характер, отсутствие единого понятийного аппарата, что указывает на необходимость его актуализации

---

<sup>265</sup> Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. №50. Ст. 7074.

<sup>266</sup> Глава 1. Информационная безопасность и цифровизация: взаимовлияние / Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере / Отв. ред. Л. К. Терещенко. М., 2024. С. 10-11.

<sup>267</sup> Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СЗ РФ. 2023. № 19. Ст. 3481.

и модернизации. Информационная безопасность граждан в целом и несовершеннолетних в частности можно охарактеризовать двухполярностью: с одной стороны, современные технологии расширяют доступ к информации, с другой, способствуют ограничениям доступа к деструктивной информации.

В рамках первого вышеобозначенного направления следует отметить, что доступ к информации расширяется за счет внедрения и функционирования различных цифровых платформ, в том числе публичных цифровых платформ, (например, «Электронный дневник» как электронный муниципальный сервис), государственных информационных систем<sup>268</sup> (например, одним из видов ГИС является «Цифровой профиль учащегося»).

В ракурсе ограничения доступа к информации следует отметить, что кроме информации, распространение которой нарушает требования закона и (или) несет вред жизни, здоровью, развитию несовершеннолетних, также имеется относительно новое правовое явление – «право на забвение», которое, на наш взгляд, имеет важное значение в сфере информационной безопасности.

В России право на забвение законодательно функционирует с 01.01.2016<sup>269</sup>: операторы поисковых систем в сети «Интернет» обязаны удалить (скрыть) ссылки на информацию: 1) с персональными данными пользователей при условии их обращения с соответствующим запросом об удалении данных к оператору поисковых систем; 2) распространяемую с нарушением законодательства; 3) являющуюся недостоверной, неактуальной, утратившей значение для заявителя в силу последующих событий или действий заявителя.

Следует сказать, что истоком теории о праве на забвение является французское законодательство («le droit a l'oubli» или «право на забвение»)<sup>270</sup>. В

<sup>268</sup> «Статья 14. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях». – Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; СЗ РФ. 2024. № 48. Ст. 7218.

<sup>269</sup> Федеральный закон от 13.07.2015 № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса РФ» // СЗ РФ. 2015. № 29 (часть I). Ст. 4390. – начало действия с 01.01.2016.

<sup>270</sup> Дедов Д. И., Гаджиев Х. И. Сфера применения права на забвение: комментарий к Постановлению Большой палаты Европейского суда по правам человека по делу «Хурбейн против Бельгии» // Журнал зарубежного законодательства и сравнительного правоведения. 2024. № 2. С. 84-94.

Европейском Союзе эта норма действует с 2014 года, когда, появившись в решении Суда Европейского союза<sup>271</sup>, право на забвение получило закрепление в ст. 17 Европейского общего регламента о защите персональных данных<sup>272</sup>. Оба названия – право на удаление и право на забвение – использованы в названной статье как равнозначные<sup>273</sup>. Уточним, что критерий «является ли субъект данных несовершеннолетним?» имеет большое значение и получил правовое закрепление в Руководстве по выполнению решения Суда ЕС<sup>274</sup>.

Таким образом, единый стандарт защиты персональных данных в сети Интернет<sup>275</sup> для всех государств – членов ЕС вступил в силу с 1 января 2018 г. и имеет значительный объем правовых норм, регламентирующих заявительный порядок реализации «права на забвение»; внедрение стандартизированных символов уведомлений об обработке персональных данных (запрет на мелкий нечитаемый шрифт и т. д.); по умолчанию устанавливается включение режима конфиденциальности в настройках, а иной режим выбирается пользователем онлайн-ресурса; запрет на передачу для провайдеров персональных данных пользователей за пределы ЕС. Как отмечает О. С. Соколова, «дети до 16 лет регистрируются в социальных сетях с разрешения родителей. Страны ЕС могут снизить этот возраст до 13 лет. <...> Компании, находящиеся за пределами ЕС, должны следовать правилам ЕС, если предлагают свои услуги и информационные продукты на территории ЕС. Подсудность по таким спорам предусмотрена в стране истца, что существенно облегчит судебную защиту заявителя»<sup>276</sup>. Иными словами, можно сказать, что в законодательной системе ЕС судебный прецедент в отношении

<sup>271</sup> CJEU. Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia de Datos (AEPD) and. ECLI: EU:C:2014:317. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131> (дата обращения: 01.05.2025).

<sup>272</sup> Регламент № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» // Official Journal of the European Union N L 119. 04.05.2016. P. 1. (пер. на русск. яз.)

<sup>273</sup> Талапина Э. В. Право на забвение: французский опыт // Конституционное и муниципальное право. 2023. № 11. С. 42-45.

<sup>274</sup> Guidelines on the implementation of the Court of Justice of the European Union judgment in the case of Google Spain SL and Google Inc. v. Agencia Espanola de Protection de Datos (AEPD) and Mario Costeja Gonzalez (C-131/12).

<sup>275</sup> Пресс-релиз Еврокомиссии «Agreement on Commission's EU data protection reform will boost Digital Single Market». URL: [http://europa.eu/rapid/press-release\\_IP-12-46\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en) (дата обращения: 01.05.2025).

<sup>276</sup> Соколова О. С. Защита персональных данных посредством права на забвение // Современное право. 2016. № 9. С. 69-72.

«права на забвение» послужил импульсом для совершенствования информационной безопасности как граждан в целом, так и несовершеннолетних в частности.

Обратимся далее к трудам научного сообщества, в которых имеется разное понимание изучаемых в этом параграфе правовых понятий. Так, под информационной безопасностью следует понимать, по суждению А. М. Шарипова, нормальное функционирование всех систем при различных обстоятельствах, ведь это общее трактование термина «информационная безопасность»<sup>277</sup>. В целом, по нашему суждению, действительно, это определение более уместно в качестве общего, так как не несет в себе сущностных признаков, а просто констатирует, что должно быть нормальное функционирование при различных обстоятельствах. Следует сказать, что в научных трудах существуют разные суждения по трактовке понятия «информационная безопасность несовершеннолетних». Так, например, С. В. Иванов полагает, что под исследуемым термином понимается гарантированное нормами международного и конституционного права состояние защищенности подростков, выраженное в неразглашении личных, семейных и т. п. сведений, а также устранении рисков получения ими информации, причиняющей вред здоровью, физическому развитию, психическому, духовному, нравственному и интеллектуальному развитию<sup>278</sup>. Отчасти это предложенное понятие коррелирует с нормативным трактованием, но при этом С. В. Иванов подчеркивает, что информационная безопасность должна обеспечивать и личную тайну, которая, к примеру, отражена в ст. 23 Конституции РФ. Также исследователь указывает на необходимость обеспечения и интеллектуального развития без негативного влияния со стороны СМИ (включая сеть «Интернет»). По нашему суждению, интеллектуальное развитие относится к иным формам развития, указанным в законодательных актах и представленным также данным автором. Подобное

---

<sup>277</sup> Шарипов А. М. Информационная безопасность в современных условиях: понятие, сущность // Обеспечение безопасности личности, общества и государства в условиях глобализации: правовые и организационные проблемы и перспективы : сб. статей Всероссийской научно-практической конференции студентов, магистров и молодых ученых, посв. 50-летию юридического образования в Удмуртской Республике. Ижевск, 2022. С. 129-134.

<sup>278</sup> Иванов С. В. Информационная безопасность детей (теоретико-правовой аспект) // Вестник Екатеринбургского института. 2011. № 2(14). С. 62-66.

развитие заключается в способности осознавать и пользоваться определенными знаниями, полученными, в частности, из информационных источников (включая сеть «Интернет»).

С. А. Буданов полагает, что «информационная безопасность несовершеннолетних заключается в организационных и правовых средствах, в рамках которых защищаются права подростков от влияния на них с помощью информации (в частности, сети «Интернет»), способной причинить вред их физическому и психическому здоровью, а также происходит искажение нравственных и духовных норм»<sup>279</sup>. Тем самым С. В. Буданов фактически определяет ключевые признаки информационной безопасности несовершеннолетних схоже с их нормативным указанием. С. Ю. Оловенцова полагает, что безопасность этой категории лиц должна быть продиктована проведением государством единой политики, а также участием родителей или лиц, их заменяющих, педагогов и правоохранительных органов, направленным на запрет информации, причиняющей вред здоровью, а также нравственному и духовному развитию несовершеннолетних<sup>280</sup>. Можно сказать, что С. Ю. Оловенцова называет какие-то новые признаки, характеризующие, что следует понимать под анализируемым нами термином в настоящем параграфе диссертационного исследования. Е. В. Горбачева на основе анализа правовых актов указывает следующие признаки, характерные для информационной безопасности несовершеннолетних: предупреждение нанесения вреда нравственному и духовному развитию, распространение специальных режимов демонстрации, трансляции информации для этой категории лиц<sup>281</sup>. В. Н. Стрельникова в лаконичной форме указывает, что информационная безопасность

<sup>279</sup> Буданов С. А. Правовое обеспечение информационной безопасности несовершеннолетних : дис. ... канд. юрид. наук. Воронеж, 2006. 220 с.

<sup>280</sup> Оловенцова С. Ю. Информационная безопасность несовершеннолетних: условия возникновения и средства предупреждения // Уголовная ответственность и наказание : сб. материалов Международной научно-практической конференции, посв. памяти профессоров кафедры уголовного права Рязанской высшей школы МВД СССР В. А. Елеонского и Н. А. Огурцова / Под редакцией В. Ф. Лапшина. Рязань, 2018. С. 139-144.

<sup>281</sup> Горбачева Е. В. Административно-правовое обеспечение информационной безопасности несовершеннолетних : дис. ... канд. юрид. наук. Ростов-на-Дону, 2011. 206 с.

несовершеннолетних предполагает именно обеспечение физического и психического здоровья и развития детей<sup>282</sup>.

По суждению А. А. Кузнецова, Ю. А. Ланчевой и Д. С. Малец, данная дефиниция содержит «личную информационную неприкосновенность», устранение возможных нарушений гарантированных законом России прав и свобод несовершеннолетнего, а также получение безопасной для их физиологического и психологического здоровья информации из сети «Интернет»<sup>283</sup>.

Таким образом, на основе вышеизложенного можем предложить авторское понятие, что информационная безопасность несовершеннолетних представляет собой состояние защищенности физических лиц (граждан и лиц без гражданства), не достигших возраста 18 лет, обеспечиваемое комплексом правовых средств, направленных на защиту несовершеннолетних лиц и их прав от воздействия на них информации, причиняющей вред их жизни, здоровью или развитию. Исходя из представленного определения, можно выделить следующие признаки: 1) единый подход к правовым средствам, направленным на защиту лиц, не достигших возраста 18 лет и их прав от воздействия на них вредной информации предполагает, что на уровне как международных, так и национальных правовых актов вырабатывается единая политика с целью создания благоприятных условий для подростков в информационном поле сети «Интернет»; 2) обеспечение духовного благополучия ребенка, то есть развитие его с учетом нравственных, духовных, моральных и иных устоявшихся в обществе норм; 3) обеспечение физического благополучия ребенка, то есть обеспечение его здоровья и предотвращение совершения посягательств на жизнь. Следует отметить, что Д. В. Куц, Н. С. Виноградова, Н. В. Третьяк считают, что «информационная безопасность – это более широкий термин, чем кибербезопасность. В рамках понятия информационной безопасности рассматриваются не только технические стороны защиты информации, но и факторы, воздействующие на человека, общество и

---

<sup>282</sup> Стрельникова В. Н. Системный подход к обеспечению информационной безопасности детства // Вестник Самарского университета. История, педагогика, филология. 2021. Т. 27. № 4. С. 92-98.

<sup>283</sup> Кузнецов А. А., Ланчева Ю. А., Малец Д. С. Защита прав и свобод несовершеннолетних в цифровом пространстве // Юридический факт. 2021. № 148. С. 13-15.



государство. Кибербезопасность же не рассматривает вопросы, связанные с воздействием вредоносного контента и использованием информационных и коммуникационных технологий на общественное сознание»<sup>284</sup>. А. В. Кубышкин в своем диссертационном исследовании отмечает, что при определении информационной безопасности важно понимать, что она представляет социальное, а не чисто техническое явление, в связи с чем он возражает относительно попытки сведения некоторыми учеными понятия «информационная безопасность» исключительно к применению технических средств и методов<sup>285</sup>. По его мнению, информационная безопасность включает в себя не только защиту информации, но и организационные, правовые и другие меры, направленные на обеспечение устойчивого, стабильного развития общества и государства.

Как отмечает О. А. Пучков, информационная безопасность представляет собой процесс цифрового противодействия несанкционированному доступу к информации; кибербезопасность – это деятельность, которая имеет более выраженный технологичный характер. То есть эти понятия обладают разным наполнением и объемом<sup>286</sup>. Они существенно различаются на трех уровнях: 1) законодательном: информационная безопасность в качестве понятия отражена в законодательных актах, термин «кибербезопасность» – отсутствует в российском законодательстве (используется понятие только в проекте Концепции Стратегии кибербезопасности РФ. Однако этот проект был предложен еще в 2014 году, в настоящее время страница на сайте Совета Федерации Федерального Собрания РФ, предназначенная для обсуждения этого проекта, не существует)<sup>287</sup>; 2) теоретико-научном: предполагает разное толкование информационной безопасности в качестве: защиты информации<sup>288</sup>, системы, способной противостоять

<sup>284</sup> Куц Д. В., Виноградова Н. С., Третьяк Н. В. Понятие информационной безопасности государства и основные направления ее обеспечения // Вестник УрФО. 2016. № 3(21). С. 56-61.

<sup>285</sup> Кубышкин А. В. Международно-правовые проблемы обеспечения информационной безопасности государства : дис. ... канд. юрид. наук : 12.00.10 / Московская гос. юридическая академия. М., 2002. С. 26-27.

<sup>286</sup> Пучков О. А. Разграничение понятий «информационная безопасность» и «кибербезопасность» в законодательстве Российской Федерации, доктрине и юридической практике // Право и государство: теория и практика. 2019. № 5 (173). С. 66-69.

<sup>287</sup> Концепция Стратегии кибербезопасности Российской Федерации (проект). URL: <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf> (дата обращения: 30.03. 2025).

<sup>288</sup> Стасьев В. Ю., Тиньков В. А. Информационная безопасность распределенных информационных систем // Информационное общество. 1997. № 1. С. 68.

дестабилизирующему воздействию внешних и внутренних информационных угроз<sup>289</sup>, как деятельности по предотвращению несанкционированного доступа. В определении кибербезопасности также превалируют разные подходы: использование технических способов защищенности, «исключительная защита данных, исходящих в цифровой форме»<sup>290</sup>, особый режим охраны данных и информации<sup>291</sup>; 3) правоприменительном: в текстах судебных решений эти понятия почти не встречаются, что свидетельствует о неиспользовании судами возможности формирования правовой основы не закреплённого в законодательстве понятия «кибербезопасность».

Исследователи отмечают наличие определенной группы противоречий в современном состоянии информационной безопасности, которые связаны с противоречиями в законодательной базе, расширением сфер автоматизации и использованием искусственного интеллекта, «субъектно-объектным подходом при обеспечении информационной безопасности и фактической разомкнутостью систем управления»<sup>292</sup>. Информационная безопасность и кибербезопасность, обладающие разными характеристиками, взаимоувязаны при помощи «коммуникационных и информационных систем, важным элементом которых являются люди, определяющие процессы, происходящие в киберпространстве, и их динамику»<sup>293</sup>. Если под кибербезопасностью понимают совокупность условий, направленных на защиту от киберугроз, то информационная безопасность обеспечивает «защиту информации в любых формах – как цифровых, так и физических»<sup>294</sup>. Появился новый термин «цифровая безопасность», подразумевающий, по мнению одних ученых, «процесс для защиты личности в

<sup>289</sup> Ищейнов В. Я. Информационная безопасность и защита информации : учеб. пособие. М. : Директ-Медиа, 2020. 271 с.

<sup>290</sup> Козлова Н. Ш., Довгаль В. А. Кибербезопасность: сходства и отличия // Вестник АГУ. 2021. Вып. 3 (286). С. 90.

<sup>291</sup> Пучков О. А. Разграничение понятий «информационная безопасность» и «кибербезопасность» в законодательстве Российской Федерации, доктрине и юридической практике» // Право и государство: теория и практика. 2019. № 5 (173). С. 68.

<sup>292</sup> Правиков Д. И., Петухов А. В. Кибербезопасность как новое информационное направление в области информационной безопасности // Вестник современных цифровых технологий. 2019. № 1. С. 18.

<sup>293</sup> Аникина Н. А., Чувашова Я. А. Некоторые аспекты информационной безопасности и кибербезопасности. Проблемная зона // Научный альманах. 2024. № 1-3 (111). С. 24.

<sup>294</sup> Баландин А. Ю. Кибербезопасность и информационная безопасность. Демаркация правовых категорий // Правовая политика и правовая жизнь. 2023. № 3. С. 261.

Интернете»<sup>295</sup>, а подход других предлагает брать во внимание «факторы, воздействующие на человека, общество и государство»<sup>296</sup>. Несомненно, заслуживает внимания определение О. А. Пучкова: «Информационная безопасность – состояние защищенности личности, институтов общества и органов государства от всех типов информационных угроз»<sup>297</sup>. В отличие от отечественных исследователей у представителей зарубежной науки сложился иной подход, в котором они рассматривают кибербезопасность в качестве своеобразной «организации и совокупности ресурсов, процессов и структур, используемых для защиты киберпространства»<sup>298</sup>. В отдельных исследованиях считают, что кибербезопасность – более расширенное понятие в отличие от информационной безопасности. Другие считают их взаимозаменяемыми терминами или даже отождествляют. Например, А. В. Борисенко объединяет эти два термина, трактуя их в качестве «совокупности методов защиты»<sup>299</sup> для технологических систем, что представляется не совсем верным. Правильным будет воспринимать кибербезопасность как составляющую часть информационной безопасности или ее некий элемент, а не наоборот<sup>300</sup>.

Для сбережения своих личных данных люди должны быть осведомлены об информационной безопасности. Попытка кражи персональных данных способствует негативным проявлениям, таким как нарушение конфиденциальности, целостности или доступности информации. Фундаментальные подходы к осуществлению инфобезопасности включают в себя три концепции: защищенного рубежного периметра, отражения множественности

<sup>295</sup> Ащепкова М. М., Маглинова Т. Г. Что такое цифровая безопасность: обзор, типы и применение / Актуальные проблемы международных отношений в условиях формирования мультиполярного мира : сб. научных статей, Курск, 15 декабря 2023 года. Курск : Университетская книга, 2023. С. 14.

<sup>296</sup> Куц Д. В., Виноградова Н. С., Третьяк Н. В. Понятие информационной безопасности государства и основные направления ее обеспечения // Вестник УрФО. 2016. №3 (21). С. 56–61.

<sup>297</sup> Пучков О. А. Разграничение понятий «информационная безопасность» и «кибербезопасность» в законодательстве Российской Федерации, доктрине и юридической практике» // Право и государство: теория и практика. 2019. № 5 (173). С. 67.

<sup>298</sup> Крейген Д., Диакун-Тибо Н., Пёрс Р. Определение кибербезопасности // Обзор управления технологическими инновациями. 2014. № 4 (10). С. 13–21.

<sup>299</sup> Борисенко А. В. Понятие кибербезопасности. Кибербезопасность государственных органов. // Актуальные проблемы развития экономических, финансовых и кредитных систем : сб. материалов X Междунар. научно-практич. конф. Белгород, 2022. С. 297-299.

<sup>300</sup> Правиков Д. И., Петухов А. В. Кибербезопасность как новое фундаментальное направление в области информационной безопасности // Вестник современных цифровых технологий. 2019. № 1. С. 17-23.

угроз, управления рисками. А. А. Нечай выделяет четыре основных сценария нарушения кибербезопасности: кибериздевательства, приводящие к психологическому воздействию на человека с помощью шантажа или запугивания; риск домашней автоматизации, последствием чего может быть несанкционированный доступ к информации; похищение или «компрометация интеллектуальной собственности, не влияющая на конфиденциальность и целостность информации»<sup>301</sup>; кибертерроризм.

На наш взгляд, основное различие между понятиями «информационная безопасность» и «кибербезопасность» заключается в том, что в основе информационной безопасности находится комплексный подход, включающий организационные и правовые аспекты и опирающиеся на критерии: «надежность, целостность, конфиденциальность информации»<sup>302</sup>, в то время как кибербезопасность в основном связана с защитой мобильных и электронных устройств от кибератак.

Таким образом, на наш взгляд, само же понятие «информационная безопасность» подразумевает состояние защищенности от внешних и внутренних угроз в рамках информационной среды. Можно также представить и следующее авторское определение: *«информационная безопасность несовершеннолетних в сети «Интернет»* представляет собой состояние защищенности лиц, не достигших возраста 18 лет, от информации, обращение которой в сети «Интернет» правовыми актами признается запрещенным». Обеспечение информационной безопасности несовершеннолетних в сети «Интернет» – это деятельность административных органов публичной власти и частных лиц, связанная с применением мер: 1) административными органами публичной власти – административно-предупредительных, административно-пресекательных, восстановительных (профилактических), мер административной ответственности; 2) частными лицами (общественными организациями и непосредственно родителями (законными

---

<sup>301</sup> Нечай А. А. Кибербезопасность и информационная безопасность: сущность, содержание и отличие понятий // В сб.: XXIV Царскосельские чтения. Материалы международной научной конференции. 2020. С. 230.

<sup>302</sup> Лаврухин В. А. Информационная безопасность и кибербезопасность в условиях вызовов современности: актуальность, сходства, различие // Человек и образование. 2024. № 1 (78). С. 126.

представителями) несовершеннолетних, владельцами социальных сетей, организаторами распространения информации в сети «Интернет») – мер, направленных на мониторинг контента, правовое воспитание несовершеннолетних; повышение родительских компетенций в сфере безопасного поведения детей в сети «Интернет»; проведение мероприятий, направленных на повышение грамотности детей по вопросам информационной безопасности в сети «Интернет»; формирование навыков законопослушного и ответственного поведения в цифровой среде; формирование у детей навыков самостоятельного и ответственного потребления контента в сети «Интернет».

Проанализируем нормы законодательства зарубежных стран в сфере понятий «информационная безопасность» и «кибербезопасность» как в целом, так и непосредственно в отношении несовершеннолетних. Понятия «информационная безопасность» и «кибербезопасность» в законодательстве Австралии не раскрываются, в то же время и Стратегия кибербезопасности Австралии 2023–2030 годов<sup>303</sup> не раскрывает терминологию, а направлена на достижение такой цели, как достижение Австралией к 2030 году лидирующей позиции в мире в киберпространстве. Для достижения указанной цели в стратегии предусмотрено три этапа: первый этап (2023–2025) был посвящен деятельности по устранению пробелов, в том числе законодательных, в информационной безопасности, выявлению и усилению информационной защиты уязвимых групп населения (несовершеннолетних); второй этап (2026–2028) направлен на расширение и укрепление кибериндустрии и кибербезопасности; третий этап (2029–2030) направлен на разработку (как регионального, так и мирового масштаба) кибертехнологий, способных к предупреждению новых рисков в онлайн-среде.

В Великобритании действующей является National Cyber Strategy 2022<sup>304</sup>, в которой, на наш взгляд, интересным является трехуровневое киберпространство: 1) виртуальный уровень, который представляет собой виртуальное представление

<sup>303</sup> Australian Cyber Security Strategy. URL: <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy> (дата обращения: 21.07.2025).

<sup>304</sup> National Cyber Strategy 2022. URL: <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022> (дата обращения: 21.07.2025).

пользователей сети «Интернет» в общем онлайн-пространстве; 2) логический уровень, состоящий из кода и (или) электронных данных. Этот уровень базируется на физических носителях (серверы и т. д.); 3) физический уровень, представленный разнообразным оборудованием. В целом Стратегия носит декларационный характер и утверждает Великобританию как «кибердержаву».

Как отмечает в своем диссертационном исследовании В. А. Гирис, «в официальных стратегических документах ЕС и нормативных правовых актах используются термины «сетевая и информационная безопасность», «кибербезопасность»»<sup>305</sup>. Понятие «кибербезопасность» в законодательстве ЕС впервые указано в 2013 году в «EU cybersecurity strategy: an open, safe and secure cyberspace» (Стратегия кибербезопасности ЕС)<sup>306</sup> и определено как «меры защиты и действия, которые могут быть использованы для защиты киберпространства как в гражданской, так и в военной сферах от тех угроз, которые связаны или могут нанести ущерб взаимозависимым сетям и информационной инфраструктуре. Кибербезопасность стремится сохранить доступность и целостность сетей и инфраструктуры, а также конфиденциальность содержащейся в них информации». А вот в первом и основном нормативном правовом акте ЕС, регламентирующем рассматриваемую сферу правоотношений, а именно – в Директиве № 2016/1148 Европейского парламента и Совета ЕС «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза»<sup>307</sup>, использовался термин «сетевая и информационная безопасность», легально не определяя понятие. В Директиве (ЕС) 2022/2555 о мерах по обеспечению высокого уровня кибербезопасности на территории Союза, согласно отсылочной норме (3) ст. 6, «под термином «кибербезопасность» понимается кибербезопасность в значении пункта

<sup>305</sup> Гирис В. А. Правовое регулирование деятельности Европейского Союза в области обеспечения кибербезопасности : дис. ... канд. юрид. наук. М., 2023. С. 22-23.

<sup>306</sup> EU cybersecurity strategy: an open, safe and secure cyberspace (European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP))) // Brussels, 7.2.2013. URL: <https://eur-lex.europa.eu/legal-content/EN/> (дата обращения: 01.05.2025).

<sup>307</sup> Директива № 2016/1148 Европейского парламента и Совета Европейского Союза «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» [рус., англ.] (Принята в г. Страсбурге 06.07.2016) // Офиц. сайт законодательства Европейского Союза. URL: <http://eur-lex.europa.eu> (дата доступа: 30.03.2025). [Россия не участвует].

(1) ст. 2 Регламента (ЕС) 2019/881»<sup>308</sup>. При обращении к п. (1) ст. 2 Регламента (ЕС) 2019/881 от 17.04.2019, «кибербезопасность» означает действия, необходимые для защиты сетевых и информационных систем, пользователей таких систем и других лиц, пострадавших от киберугроз»<sup>309</sup>. Таким образом, в законодательстве ЕС термин «сетевая и информационная безопасность» был заменен на термин «кибербезопасность», который легально определен и получил распространение во многих нормативных правовых актах. Исходя из анализа положений Регламента (ЕС) 2019/881 и Директивы (ЕС) 2022/2555 можно сказать, что понятие «кибербезопасность» имеет два признака: 1) состояние защищенности от киберугроз согласно п. (1) ст. 2 Регламента (ЕС) 2019/881; 2) непосредственно действия, направленные на достижение вышеуказанного состояния (ст. 2–3 Директивы (ЕС) 2022/255). В Рекомендациях № 2006/952/ЕС «О защите несовершеннолетних и человеческого достоинства, а также о праве на ответ в отношении конкурентоспособности европейской аудиовизуальной и онлайн-индустрии информационных услуг»<sup>310</sup> отражаются фактически те же признаки, что и в российском праве. В ст. 7 Директивы (ЕС) 2022/2555 указывается, что каждое государство – член ЕС должно принять национальную стратегию кибербезопасности, которая определяет стратегические цели, ресурсы, необходимые для достижения этих целей, а также соответствующие политические и нормативные меры для достижения и поддержания высокого уровня кибербезопасности.

Как справедливо отмечает К. R. Ludvigsen, ЕС не может принимать прямые законодательные меры в таких областях, как кибербезопасность, или в других

---

<sup>308</sup> Директива № 2022/2555 Европейского парламента и Совета Европейского Союза «О мерах по обеспечению высокого общего уровня кибербезопасности на территории Союза, о внесении изменений в Регламент (ЕС) 910/2014 и Директиву (ЕС) 2018/1972, а также об отмене Директивы (ЕС) 2016/1148 (Директива NIS 2)» [рус., англ.] // Официальный сайт законодательства Европейского Союза. URL: <http://eur-lex.europa.eu/> (дата доступа: 30.03.2025). [Россия не участвует].

<sup>309</sup> Регламент (ЕС) 2019/881 Европейского парламента и Совета от 17 апреля 2019 года «О Европейском агентстве по кибербезопасности ENISA и сертификации информационных и коммуникационных технологий», а также об отмене Регламента (ЕС) №526/2013.

<sup>310</sup> Рекомендация № 2006/952/ЕС Европейского парламента и Совета Европейского Союза «О защите несовершеннолетних и человеческого достоинства, а также о праве на ответ в отношении конкурентоспособности европейской аудиовизуальной и онлайн-индустрии информационных услуг». URL: <http://eur-lex.europa.eu/> (дата обращения: 01.05.2025).

случаях, связанных с безопасностью<sup>311</sup>, поскольку это ограничено Договором о функционировании Европейского союза<sup>312</sup>, ведь согласно п. 2 ст. 2 кибербезопасность относится к совместной компетенции Союза и государств-членов. Как правило, в национальном законодательстве государств – членов ЕС используется наднациональная правовая терминология в целом и термин «кибербезопасность» в частности. В подавляющем большинстве государств – членов ЕС используется национальная стратегия кибербезопасности (цифровой безопасности) – во Франции<sup>313</sup>, Ирландии<sup>314</sup>, Словакии<sup>315</sup>, Финляндии<sup>316</sup>, Швеции<sup>317</sup> и других государствах – членах ЕС. Некоторые государства – члены ЕС (например, Латвия) в качестве определения «кибербезопасности» используют определение Международного союза электросвязи, в котором также признается защита пользователей. Подходы других государств – членов ЕС к определению понятия «кибербезопасность» базируются на «триаде CIA» (Confidentiality, Integrity, Availability), которая является базовой концепцией информационной безопасности, определяющей три ключевых аспекта, которые необходимо защищать: конфиденциальность, целостность (защищает от несанкционированного изменения данных, а также от преднамеренной или случайной порчи), доступность (Availability). Так, согласно Национальной стратегии по кибербезопасности Болгарии 2020 г.<sup>318</sup>, под «кибербезопасностью» понимается состояние, определяемое и измеряемое уровнем конфиденциальности, целостности, доступности, подлинности и отказоустойчивости информационных ресурсов, систем и услуг. В § 2 Закона Эстонской Республики «О кибербезопасности» от

<sup>311</sup> Ludvigsen K. R. Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law. 2025. Preprints. URL: <https://www.researchgate.net/> (дата доступа: 30.03.2025).

<sup>312</sup> Договор о функционировании Европейского Союза [рус., англ.] (Вместе со «Списком, предусмотренным в статье 38...», «Заморскими странами и территориями, к которым применяются положения части четвертой Договора...») (Подписан в г. Риме 25.03.1957) (с изм. и доп. от 13.12.2007). URL: <http://eur-lex.europa.eu/> (дата обращения: 01.05.2025).

<sup>313</sup> Stratégie nationale française de sécurité de l'information. URL: [https://cyber.gouv.fr/sites/default/files/IMG/pdf/2011-02-15\\_Defense\\_et\\_securite\\_des\\_systemes\\_d\\_information\\_strategie\\_de\\_la\\_France.pdf](https://cyber.gouv.fr/sites/default/files/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf) (дата обращения: 01.05.2025).

<sup>314</sup> Cyber Ireland Cluster Strategy 2024- 2027. URL: <https://cyberireland.ie> (дата обращения: 01.05.2025).

<sup>315</sup> National Cybersecurity Strategy 2021-2025. URL: <https://digital-skills-jobs.europa.eu/en/> (дата обращения: 01.05.2025).

<sup>316</sup> Finland's Cyber Security Strategy 2024-2035. URL: <https://www.itu.int/en/> (дата обращения: 01.05.2025).

<sup>317</sup> Sweden Unveils Ambitious Cybersecurity Strategy for 2025-2029. URL: <https://www.government.se/> (дата обращения: 01.05.2025).

<sup>318</sup> Национална стратегия за киберсигурност «Киберустойчива България 2020. URL: <https://cyberbg.eu/> (дата обращения: 01.05.2025).



09.05.2018 (Küberturvalisuse seadus (lühend – KüTS))<sup>319</sup> представлена терминология данного закона, однако отсутствует понятие «кибербезопасность», но в § 6 перечислены принципы обеспечения кибербезопасности: 1) принцип индивидуализма: обеспечение безопасности системы поставщиком услуг; 2) принцип комплексной защиты: поставщик услуг должен определить потенциальные опасности системы и внедрить систему организационных и технических мер защиты; 3) вредные последствия принципа сокращения: поставщик услуг осуществляет необходимую комплексную проверку и стремится предотвратить киберинциденты, последствия расширения и потенциального распространения другой системы, а также информировать нарушителя об этом законе, установленном надзорным органом; 4) сотрудничество: для обеспечения кибербезопасности и урегулирования разногласий стороны должны сотрудничать.

Таким образом, понятие «информационная безопасность» согласно позиции Международной организации по стандартизации является более широким (родовым) понятием по отношению к понятию «кибербезопасность». Такой подход к соотношению рассматриваемых понятий находит отражение в рамках исследований российских и зарубежных ученых. Б. Коркоран (Brian Corcoran), признаёт, что «кибер» является общеизвестно неясным термином, означающим, что «это просто означает «относящийся к Internet»»<sup>320</sup>. По мнению Г. Шпор (Grażyna Szpor), «кибербезопасность» представляет собой термин, который широко используется в правовых актах, научных публикациях и правовом лексиконе, но не имеет общепринятого понятия, поэтому в целях избежания неоднозначных трактований термин «кибербезопасность» нуждается в лаконичном и общепризнанном определении<sup>321</sup>. По мнению Г. Г. Фустера (Fuster G. G.), термин «кибербезопасность» с точки зрения ЕС подразумевает сочетание киберустойчивости, киберпреступности, киберзащиты, непосредственно

<sup>319</sup> Küberturvalisuse seadus (lühend - KüTS) 09.05.2018. URL: <https://www.riigiteataja.ee/akt/122052018001> (дата обращения: 01.05.2025).

<sup>320</sup> Corcoran B. A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace // Harvard National Security Journal 11. 2020. № 1. P. 1–9.

<sup>321</sup> Szpor G. The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland // Review of European and Comparative Law. 2021. № 46(3). P. 219-235.

кибербезопасности и глобальных проблем киберпространства<sup>322</sup>.

В завершение главы 1 исследования, в результате анализа российского и зарубежного законодательства, судебной практики и трудов ученых-правоведов, можно сделать следующие выводы.

1. Нормы Конвенции о правах ребенка 20.11.1989 регламентируют правовое положение ребенка как в РФ, так и в зарубежных государствах, устанавливая верхний возрастной порог ребенка – 18 лет, хотя в национальных законодательствах используются и иные возрастные критерии, например, «дети старше 18 лет» или «дети в возрасте до 23 лет...»<sup>323</sup>.

2. Как в российском законодательстве, так и в изучаемых законодательствах зарубежных государств нет единообразного подхода к понятиям «ребенок (дети)», «подросток», «несовершеннолетний», «молодежь». В российской и зарубежной научной литературе отсутствует единообразие в трактовке вышеуказанных понятий. Приведенный в главе 1 анализ наглядно отображает, что термин «ребенок (дети)» является, с одной стороны, межотраслевым и декларационным, «рамочным», с другой стороны, имеет значение родственной (кровной, генетической) связи.

3. В результате исследования понятия «несовершеннолетний» в юридической науке, законодательстве РФ и зарубежных государств, соотношения понятия «несовершеннолетний» с терминами «ребенок» и «подросток» нами предложены авторские понятия «малолетний ребенок» и «подросток».

4. Предложена и обоснована градация возрастных групп в рамках общего понятия «несовершеннолетний». Кроме того, стоит напомнить, что понятие «подросток» принимается отечественным законодателем на уровне подзаконных актов. На основе проведенного анализа законодательства предложена классификация субъектов ответственности в административном праве:

– лица от 0 до 6,6 лет – не имеют дееспособности и не несут ответственности;

<sup>322</sup> Fuster G. G. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights // The Ethics of Cybersecurity. 2020. Pp. 97-115.

<sup>323</sup> Указ Президента РФ от 11.03.2020 № 180 «О дополнительных мерах социальной защиты некоторых категорий граждан Российской Федерации» // СЗ РФ. 2020. № 11. Ст. 1530.

– лица от 6,6 до 14 лет – имеют частичную дееспособность и не подлежат ответственности за исключением случаев, предусмотренных законодательством;

– лица от 14 до 16 лет – имеют ограниченную дееспособность и подлежат юридической ответственности, но осуществляют свои права и обязанности в большем объеме, чем предыдущие группы – российский законодатель эту возрастную категорию наделяет правом получения паспорта гражданина, осуществления различных действий с согласия законного представителя;

– лица от 16 до 18 лет – подлежат административной ответственности.

Следовательно, отграничение в российском праве понятия «несовершеннолетний» от понятий «малолетний ребенок» и «подросток» позволяет унифицировать подход к вышеуказанным понятиям во всех областях права России. Мы группируем в изучаемой сфере лиц от 14 до 18 лет, объединяя их термином «подростки», и этот термин предлагается использовать в сфере информационной безопасности несовершеннолетних в сети «Интернет».

5. В России и зарубежных государствах отсутствует единообразный легальный подход к определению «информации, причиняющей вред их здоровью и развитию», «вредоносного онлайн-содержания», «деструктивного контента» и к правовому регулированию ограничения их распространения, а основными механизмами защиты детей от вредоносного контента являются фильтрация и возрастная категоризация.

6. Несомненным достоинством российского законодательства является наличие профильного Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», в котором указан закрытый перечень подобной информации. Однако следует указать, что в проанализированном зарубежном законодательстве более полно регламентируется защита несовершеннолетних от информации, причиняющей вред их здоровью и развитию (от незаконного и вредоносного контента), например, введение «цифрового совершеннолетия» (15 лет), до которого действия несовершеннолетнего в сети «Интернет» и особенно в социальных сетях подлежат ограничению или запрещению без одобрения законного представителя.

7. Предлагается дополнить текст, в том числе и название Закона № 436-ФЗ<sup>324</sup> новым объектом правовой охраны – «жизнь», которому может быть причинен вред от информации наравне со здоровьем и развитием несовершеннолетнего лица. Обоснована целесообразность изложения названия Федерального закона от 29.12.2010 № 436-ФЗ в следующем виде: «О защите детей от информации, причиняющей вред их *жизни*, здоровью и развитию».

8. Проведен детальный анализ зарубежного законодательства в части определения и видов деструктивного контента. Проведя анализ зарубежных актов и мнений научного сообщества зарубежных государств, можно сделать вывод, что в Австралии, Великобритании, государствах – членах ЕС, в том числе Франции, имеются следующие виды информации, причиняющей вред здоровью и развитию несовершеннолетних: 1) незаконный контент: контент, содержащий информацию, распространение которой нарушает законы (террористический, дискриминационный контент и т. д.), либо же побуждающий к насилию и т. д. Как правило, подобный контент запрещен административными или уголовными национальными кодексами; 2) вредоносный контент: представляет собой контент, который непосредственно предназначен для несовершеннолетних, причиняет вред их здоровью и развитию путем призыва (пропаганды) нарушения пищевых привычек, сексуальной распущенности, членовредительства, а также клевета, оскорбления и кибериздевательства; дезинформация (disinformation), а также ошибочная информация (misinformation) и недобросовестная информация (malinformation); защита несовершеннолетних от сексуальных злоупотреблений; 3) иной контент, который представляет опасность причинения вреда для несовершеннолетних лиц.

9. Разработана авторская классификация контента, наносящего вред жизни, здоровью и развитию несовершеннолетнего (деструктивного контента) в сети «Интернет». В результате анализа информации, причиняющей вред здоровью, жизни, развитию малолетних и подростков, представленного в двух параграфах,

<sup>324</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

посвященных российскому и зарубежному деструктивному контенту, обоснована авторская классификация деструктивного контента, наносящего вред жизни, здоровью и развитию несовершеннолетних (деструктивного контента) в сети «Интернет»: 1) незаконный (запрещенный) контент международного уровня; 2) незаконный (запрещенный или ограниченный) контент национального, наднационального уровня; 3) нежелательный контент.

10. Все изученные легально-зафиксированные понятия и авторские трактования «информационной безопасности», «кибербезопасности» как граждан в целом, так и несовершеннолетних в частности, несомненно представляют научный интерес, отражают важные признаки многогранных вышеуказанных понятий, но в то же время иллюстрируют необходимость выработки единого общепринятого понятийного аппарата, так как проблема информационной безопасности несовершеннолетних в сети «Интернет» имеет трансгосударственный характер.

11. Изучив законодательство России и зарубежных стран в сфере информационной безопасности несовершеннолетних в сети «Интернет», различные авторские дефиниции ключевых понятий в этой области правоотношений, автор предлагает определения «информационная безопасность несовершеннолетних» и «информационная безопасность несовершеннолетних в сети «Интернет».

## **ГЛАВА 2. ПРАВОВОЙ СТАТУС ОРГАНОВ ПУБЛИЧНОЙ ВЛАСТИ И ЧАСТНЫХ ЛИЦ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ «ИНТЕРНЕТ»**

### **2.1. Публичные властные субъекты по обеспечению информационной безопасности несовершеннолетних в зарубежных государствах**

В зарубежной и отечественной научной юридической литературе и законодательстве при обозначении субъектов административного права и их классификации используется понятийно-категориальный аппарат с разнообразным смысловым наполнением участников правоотношений, в том числе и в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет». В этой связи в нашем диссертационном исследовании используется классификация субъектов административного права профессора А. Б. Зеленцова, который выделяет: 1) публичные властные субъекты (публичные лица), включающие в себя индивидуальные (физические) публичные лица и коллективные публичные лица; 2) частные невластные субъекты (частные лица), состоящие из индивидуальных (физических) частных лиц и коллективных частных лиц (невластные организации)<sup>325</sup>.

Рассмотрим публичные властные субъекты по обеспечению информационной безопасности несовершеннолетних в зарубежных государствах. Несомненно, на протяжении последних двух десятилетий Австралия выступает новатором в правовом регулировании безопасности в сети «Интернет» как в законодательной сфере, так и в исполнительной сфере в рамках изучаемой темы диссертационного исследования. В 1999 году был принят закон<sup>326</sup> о государственном контроле над содержимым сети «Интернет»: «для борьбы с

<sup>325</sup> Подробнее: Зеленцов А. Б. Частное лицо как субъект административного права // Административное право и процесс. 2025. № 2. С. 3-20; Зеленцов А. Б. Концептуальные подходы к определению административного права: опыт сравнительно-правового исследования // Административное право и процесс. 2019. № 7. С. 5-21.

<sup>326</sup> Broadcasting Services Amendment (Online Services) Act 1999 No. 90 (утратил силу). URL: <https://www.legislation.gov.au/C2004A00484/asmade/text> (дата обращения: 01.05.2025).

вредным онлайн-контентом, включая материалы о жестоком обращении с детьми»<sup>327</sup>, в соответствии с которым предусмотрена рейтинговая система контента сети «Интернет»; при выявлении признаков «порнографичности» контент подлежал удалению в срок до 24 часов. В 2015 году правительство учредило должность первого в мире комиссара по безопасности детей, а в 2017 году его полномочия были расширены и в его сферу ответственности были включены все австралийцы<sup>328</sup>. Считаем важным обозначить, что в ряде источников, например, в коллективной монографии под общей редакцией С. Е. Титора<sup>329</sup>, эта должность указана как «уполномоченный по вопросам кибербезопасности», однако, на по нашему мнению, правильно называть должность «комиссар по электронной безопасности» («eSafety Commissioner»). На наш взгляд, использование перевода термина «eSafety» как кибербезопасность является неверным, потому что «кибер» соответствует «cyber», но не Esafety (Electronic safety), тем более, в тексте закона употребляются и «esafety», и «cyber».

В Австралии в 2015 году согласно Закону о повышении безопасности детей в интернете № 24 от 2015 года<sup>330</sup>, который в настоящее время уже утратил силу, учредили должность комиссара по электронной безопасности (Commissioner) и определили его функции и полномочия; была создана система подачи жалоб на материалы, содержащие кибербуллинг и адресованные австралийским несовершеннолетним; а также сформирована двухуровневая схема для быстрого удаления из крупных социальных сетей материалов о кибербуллинге, нацеленных на несовершеннолетних. Иными словами, до 2017 года функционировало Управление комиссара по электронной безопасности детей, которое отвечало за обучение детей и подростков Австралии правилам безопасности в сети «Интернет»,

<sup>327</sup> Commonwealth law uses the term 'child abuse material' to capture material that depicts or represents the sexual or physical abuse of a person who is or appears to be under 18 years of age. URL: <https://www.criminalsolicitorsmelbourne.com.au/blog/child-abuse-material> (дата обращения: 01.05.2025).

<sup>328</sup> Department of Communications and the Arts, Online Safety Legislative Reform: Discussion Paper, (Canberra: Department of Communications and the Arts, December 2019), p. 36. URL: <https://www.communications.gov.au> (дата обращения: 01.05.2025).

<sup>329</sup> Правовое регулирование защиты несовершеннолетних от деструктивной информационной среды : монография / Под общ. ред. С. Е. Титор. М. : РУСАИНС, 2025. 350 с.

<sup>330</sup> Enhancing Online Safety for Children Act 2015 (No. 24 of 2015). URL: [https://www4.austlii.edu.au/au/legis/cth/num\\_act/eosfca2015321/](https://www4.austlii.edu.au/au/legis/cth/num_act/eosfca2015321/) (дата обращения: 01.05.2025).

защищало их в случае серьезного кибербуллинга и рассматривало жалобы на оскорбительный или незаконный онлайн-контент.

В 2017 году Федеральное правительство Австралии внесло законопроект о внесении поправок в Закон о повышении безопасности детей в сети «Интернет»<sup>331</sup>, который расширял полномочия комиссара по электронной безопасности детей, в результате чего целью деятельности комиссара по электронной безопасности стали все возрастные категории, а должность была переименована в должность «Комиссар по электронной безопасности» согласно расширению полномочий, что упростило австралийским гражданам поиск информации о том, куда они могут обратиться за помощью и советом по целому ряду вопросов, связанных с безопасностью в Интернете, независимо от возраста.

С 2021 года согласно принятому закону Online Safety Act 2021<sup>332</sup> регламентируется деятельность Управления по вопросам электронной безопасности и непосредственно комиссара по электронной безопасности, а также порядок привлечения нарушителей к юридической ответственности.

Управление по вопросам электронной безопасности (eSafety) – это независимая государственная организация, деятельность которой поддерживается Австралийским управлением по коммуникациям и СМИ (АСМА)<sup>333</sup>. За исключением комиссара все сотрудники, выполняющие функции «eSafety», являются сотрудниками Австралийского управления по коммуникациям и СМИ (АСМА) и пользуются правами, защитой и обязательствами АСМА.

В ч. 1 ст. 5 Online Safety Act 2021, содержащей определения этого закона, установлено, что «Комиссар означает Комиссара по электронной безопасности». Согласно ст. 25 Online Safety Act к функциям Комиссара отнесено: 1) повышение безопасности в Интернете для австралийцев; 2) управление системой подачи жалоб на материалы, содержащие кибербуллинг, направленные против австралийских детей; 3) управление системой подачи жалоб на материалы, содержащие

<sup>331</sup> Federal Government Introduces Bill to Expand Role of the Children's e-Safety Commissioner. URL: <https://www.timebase.com.au/news/2017/AT04136-article.html> (дата обращения: 01.05.2025).

<sup>332</sup> Online Safety Act 2021 No. 76. URL: <https://www.legislation.gov.au> (дата обращения: 01.05.2025).

<sup>333</sup> Official website eSafety Commissioner. URL: <https://www.esafety.gov.au/about-us/our-structure> (дата обращения: 01.05.2025).



кибероскорбления, адресованные взрослым австралийцам; 4) управление системой жалоб и возражений в отношении распространения интимных изображений без согласия; 5) администрирование схемы онлайн-контента; 6) координация деятельности департаментов, органов власти и агентств Содружества, связанной с безопасностью австралийцев в Интернете.

Согласно ст. 28 Online Safety Act 2021<sup>334</sup> полномочия Комиссара заключаются в том, что он имеет право делать все необходимое или целесообразное для выполнения своих функций или в связи с ними. Также имеется отсылочное примечание к ст. 178 Online Safety Act 2021 г., согласно которой имеются дополнительные полномочия, а именно: право заключать договоры; любой договор, заключённый Комиссаром, заключается от имени Содружества. В функции Комиссара также включены координация соответствующей деятельности департаментов Содружества, органов власти и агентств; поддержка, проведение, аккредитация и оценка программ в области образования и повышения осведомленности общественности; предоставление грантов и консультирование министра. Таким образом, можно сказать, что Online Safety Act 2021 устанавливает должность Комиссара по электронной безопасности (the Commissioner), который является независимым статутным учреждением в составе Австралийского государственного управления по коммуникациям и СМИ (ACMA, то есть «means the Australian Communications and Media Authority»). Статья 30 Online Safety Act 2021 рассматривает жалобы на кибербуллинг (с использованием материалов, размещенных на определенном сервисе социальных сетей; или конкретная соответствующая электронная услуга; или конкретный назначенный интернет-сервис), при этом идет градация в зависимости от субъекта подачи жалобы: 1) «жалоба, поданная австралийским ребенком» (п. 1 ст. 30), подается Комиссару, если ребенок полагает, что он был или является жертвой кибербуллинга; 2) «жалоба, поданная от имени австралийского ребенка» (п. 2 ст. 30) – ответственное лицо (родители или опекуны, а также лица, которых ребенок уполномочил подать жалобу по этому вопросу) может от имени ребенка подать жалобу комиссару; 3)

<sup>334</sup> Online Safety Act 2021 No. 76. URL: <https://www.legislation.gov.au> (дата обращения: 01.05.2025).

«жалоба, поданная взрослым, который был австралийским ребенком» (п. 3 ст. 30), в случаях, если лицо достигло 18 лет или у лица есть основания полагать, что, когда он был ребенком в Австралии, он подвергался кибербуллингу, то лицо может подать жалобу комиссару при условиях: жалоба подана в течение разумного срока после того, как лицу стало известно о случившемся; жалоба подается в течение 6 месяцев после достижения лицом 18-летнего возраста; 4) «жалоба, ранее поданная поставщику услуг» (п. 4 ст. 30), в случаях, если жалоба подана лицом в соответствии со ст. 30, 31 Online Safety Act 2021 и лицо хочет, чтобы комиссар направил поставщику услуг уведомление, требующее от поставщика удалить материал из сервиса. При этом жалоба должна сопровождаться доказательствами того, что материал был предметом жалобы, поданной ранее поставщику услуг.

Норма п. 5 ст. 30 Online Safety Act 2021 устанавливает, что для целей п. 4 ст. 30 доказательства должны быть представлены в форме, требуемой уполномоченным органом. Например, в виде номера жалобы (п. 6 ст. 30). Если заявителю не выдана квитанция или номер жалобы, комиссар может потребовать предоставить доказательства в виде снимка экрана; или в форме официального заявления; или в такой иной форме, какую укажет комиссар (п. 7 ст. 30).

Комиссар по электронной безопасности имеет полномочия расследовать жалобы и проводить такие расследования. Комиссар может также рассмотреть вопрос о том, направлять ли уведомление об удалении в службу социальных сетей, соответствующую электронную службу или специальную интернет-службу в связи с информацией, причиняющей вред несовершеннолетнему. Комиссар также может усилить требования к отрасли по защите детей от контента, не соответствующего их возрасту, например порнографии. Считаем возможным уточнить, что действует аналогичная система подачи жалоб на материалы о кибератаках, направленных против взрослого австралийца (ст. 36, 37 Online Safety Act 2021): жалобы могут быть поданы комиссару взрослым гражданином Австралии или ответственным лицом, действующим с разрешения этого взрослого, если материалы с кибератаками были или представлены в определенной социальной сети, соответствующем электронном сервисе или специальном интернет-сервисе.

Глава 5 Online Safety Act 2021 устанавливает, что Комиссар имеет право потребовать от провайдера социальных сетей, соответствующих электронных сервисов или назначенных интернет-сервисов удалить материалы кибертравли, нацеленные на австралийского ребенка, в течение 24 часов (или более длительного периода, который разрешает Комиссар), если соблюдены определенные предварительные условия. Они заключаются в том, что Комиссар получил жалобу на материал; материал был предметом предварительной жалобы на поставщика услуг; материал не был удален с сервиса в течение 48 часов после подачи жалобы поставщику (провайдеру) или в течение более длительного периода, который разрешает Комиссар; Комиссар проверил, что материал представляет собой кибертравлю, направленную против австралийского ребенка. Комиссар также может потребовать от поставщика услуг хостинга предпринять все разумные шаги для прекращения размещения материала. За нарушение сроков удаления, указанных в уведомлении о необходимости удаления от Комиссара, социальные сети, интернет-сервис или хостинг-провайдер несут правовые взыскания. Несмотря на наличие детально разработанного специального законодательного акта, в 2024 году общественные деятели и родители подчеркивали уязвимость несовершеннолетних в сети «Интернет» от информации, оказывающей вред, например: доступ к неприемлемому контенту, отличному от порнографии (38 %); нахождение в контакте с незнакомыми людьми (37 %); травля в Интернете (34 %)<sup>335</sup>. При этом отмечается, что несовершеннолетние, сталкиваясь с деструктивным онлайн-контентом, часто не обращаются за помощью к родителям, опекунам, педагогам, цифровым платформам или не знают, что могут обратиться за помощью таким образом.

В Австралии Комиссией по электронной безопасности в контексте запрета доступа детей к онлайн-порнографии были опубликованы рекомендации в виде «Дорожная карты по проверке возраста», согласно которым в ноябре 2023 года были разработаны и проведены испытания технологии проверки возраста в

---

<sup>335</sup> Official website eSafety Commissioner. eSafety Research. 2024. Parenting in the Digital Age, p. 4. URL: <https://www.esafety.gov.au/> (дата обращения: 01.05.2025).

социальных сетях. В законопроекте было указано о необходимости механизма применения технологии на платформах социальных сетей, однако он был отклонен. В ноябре 2024 года был разработан и внесен законопроект «О внесении поправок в Закон о безопасности в интернете (минимальный возраст для использования социальных сетей) 2024 года» с целью внесения поправок в Закон о безопасности в интернете 2021 года (Online Safety Act 2021)<sup>336</sup>, чтобы обязать некоторые социальные сети принимать разумные меры для предотвращения создания учетных записей детьми младше 16 лет. Законопроект также внес поправки в Закон о возрастной дискриминации 2004 г.<sup>337</sup>, чтобы облегчить проведение реформы. Этот законопроект вызвал общественное обсуждение, однако в итоге был принят и предусматривает: запрет несовершеннолетним младше 16 лет пользоваться социальными сетями, причем именно сами интернет-платформы должны блокировать доступ несовершеннолетним и уничтожать все данные, собранные у пользователей младше 16 лет. Исключения предусмотрены для образовательных и медицинских сервисов, таких как Headspace, Google Classroom и YouTube<sup>338</sup>; при этом в обязанности Комиссара по электронной безопасности входит разработка рекомендаций по «разумным мерам», которые должны приниматься платформами социальных сетей с возрастными ограничениями, но при этом – и что, на наш взгляд, является важным уточнением – подробная информация о том, что может быть включено в эти рекомендации, например, какие технологии определения или подтверждения возраста могут быть использованы, в закон не включена.

Законодательно зафиксировано, что обязанность платформ социальных сетей ограничивать доступ несовершеннолетних пользователей к аккаунтам вступит в силу не ранее чем через 12 месяцев. Как отмечает в своей научной статье Т. Ху (Tengyue Hu)<sup>339</sup>, по состоянию на март 2025 года в Австралии все еще не существует

<sup>336</sup> Online Safety Act 2021 No. 76 0/. URL: <https://www.legislation.gov.au> (дата обращения: 01.05.2025).

<sup>337</sup> Age Discrimination Act 2004 No. 68. URL: <https://www.legislation.gov.au/C2004A01302/latest/text> (дата обращения: 01.05.2025).

<sup>338</sup> Online Safety Amendment (Social Media Minimum Age) Act 2024. URL: <https://www.legislation.gov.au/C2024A00127/asmade/text> (дата обращения: 01.05.2025).

<sup>339</sup> Hu T. The Role of Age Verification Systems in Protecting Minors from Harmful Online Content in Australia // International Journal of Social Sciences and Public Administration. 2025. № 6(2). P. 134-141.

общенациональной системы обязательной проверки возраста для всего онлайн-контента, хотя обсуждения и предложения по ужесточению мер продолжаются. Несмотря на наличие опасений, что повышение точности систем проверки возраста часто означает необходимость собирать больше информации о пользователе, и если масштабы сбора информации не будут должным образом оценены, это может привести к вторжению в личную жизнь пользователя. Например, чтобы соответствовать новым требованиям, человеку придется предъявить весь свой паспорт, который содержит гораздо больше информации о личности, чем просто дату рождения<sup>340</sup>. Эти риски обоснованны и необходимы, ведь для того, чтобы обойти систему верификации возраста, несовершеннолетние пользователи часто используют разные меры обхода, такие как использование удостоверений личности родителей или использование реалистичных фильтров для изменения возраста людей на изображениях и видео<sup>341</sup>. Однако при этом, несмотря на позицию Комиссара по электронной безопасности, правительство Австралии отклонило законопроект о дезинформации в социальных сетях<sup>342</sup>, основной аргументацией его критики выступало возникновение «цензуры» и «ограничение свободы слова».

Как отмечают в своем правовом исследовании П. Крофтс (Penny Crofts) и Х. Рейсвейк (Honnivan Rijswijk), «Комиссар по электронной безопасности обращается к крупным технологическим корпорациям и просит их соблюдать закон, он недостаточно использует свои полномочия, чтобы добиваться штрафов за неэффективные и неадекватные действия со стороны корпораций»<sup>343</sup>.

Достаточно интересен с позиции обеспечения информационной безопасности спор между австралийским комиссаром по вопросам электронной безопасности и компанией X Corp. (ранее известной как Twitter) по поводу распоряжения, требующего глобального удаления определенных видеозаписей с

<sup>340</sup> Scheffle S. Age Verification Systems Will Be a Personal Identifiable Information Nightmare // Communications of the ACM. 2024. № 67(7). P. 31-33.

<sup>341</sup> Там же.

<sup>342</sup> Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024. URL: [https://www.aph.gov.au/Parliamentary\\_Business/Committees/Senate/Environment\\_and\\_Communications/MisandDisinfobi1](https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/MisandDisinfobi1) (дата обращения: 01.05.2025).

<sup>343</sup> Crofts P., Rijswijk Honni van. Bringing Cyber Hate Under Control Through a Pro-active Legal Approach: An Australian Case Study // Handbook on Cyber Hate. 2024. Pp. 261-274.

места преступления, связанного с нанесением ножевых ранений, который привлек внимание к теме «сферы юрисдикции» с учетом сети «Интернет». По мнению Д. Свантессона (Dan Svantesson), «у Австралии неоднозначный «послужной список» в вопросах, связанных со сферой юрисдикции»<sup>344</sup>. Так, в Сиднее 15.04.2024 епископ получил ножевое ранение, удар ножом был записан и транслировался в прямом эфире. После этого события австралийский комиссар по электронной безопасности работал в сотрудничестве с ведущими технологическими компаниями (включая Google, Microsoft, Snap и TikTok) над удалением материала. 16 апреля 2024 года комиссар выдал компаниям Meta и X Corp уведомления об удалении; Meta удалила материалы, указанные в уведомлении. Однако X Corp. этого не сделала и использовала технологии геолокации, чтобы предотвратить доступ австралийских пользователей к материалам. Комиссар «не был удовлетворен действиями, которые он предпринял в соответствии с уведомлением об удалении», и запросил временный судебный запрет в Федеральном суде. Суд вынес временный судебный запрет 22 апреля 2024 года и с тех пор продлил его новым приказом от 24 апреля 2024 года<sup>345</sup>. Позиция X Corp. основана на отсылке к «ценности для свободы слова»<sup>346</sup>, однако, на наш взгляд, материалы с жестокостью и насилием не представляют ценности для свободы слова.

Требование о глобальном удалении контента – это, несомненно, и «сфера юрисдикции». Всякий раз, когда суд принимает решение, связанное с контентом, он должен рассматривать вопрос о «сфере юрисдикции»<sup>347</sup> или «сфере судебной юрисдикции», как предпочел Апелляционный суд Британской Колумбии в деле *Equustek*<sup>348</sup>. Сфера юрисдикции относится к соответствующему географическому

<sup>344</sup> Svantesson D. Global content orders: A legal analysis of eSafety Commissioner v X Corp. (May 7, 2024). URL: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4819178](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4819178) (дата обращения: 01.05.2025).

<sup>345</sup> Statement on removal of extreme violent content 23/4/24. URL: <https://www.esafety.gov.au/newsroom/media-releases/statement-on-removal-of-extreme-violent-content> (дата обращения: 01.05.2025).

<sup>346</sup> Юридические вопросы на слушании 10 мая 2024 г. X Corp. компания четко обозначила, в чем она видит две основные юридические проблемы: «Во-первых, мы считаем, что эти посты вообще не должны были запрещаться в Австралии. [...] Во-вторых, мы выступаем против требования глобально удалить этот контент с сайта X». URL: <https://www.capitalbrief.com/briefing/x-says-stabbing-video-does-not-encourage-or-provoke-violence-f7fadc50-21a9-4eb2-a5f9-01f20a4788b2/> (дата обращения: 01.05.2025).

<sup>347</sup> Nordic Yearbook of Law and Informatics 2010-2012: Internationalisation of Law in the Digital Information Society, p. 195-215. Posted: 2013.

<sup>348</sup> *Equustek Solutions Inc v Google Inc* [2015] BCCA 265. URL: <https://www.eff.org/files/2015/12/16/2015bcc265.pdf> (дата обращения: 01.05.2025).

охвату решения, связанного с содержанием такого понятия, как судебный приказ<sup>349</sup>. Таким образом, предполагая, что Федеральный суд примет решение ограничить распространение соответствующего видеоматериала, он должен решить, распорядиться ли ограничить соответствующий контент только в Австралии, по всему миру или где-то посередине между этими крайностями. Разумеется, это ключевой вопрос с точки зрения управления сетью «Интернет»<sup>350</sup>. Учитывая, что широкая сфера юрисдикции может оказать существенное влияние на другие государства и на лиц в других государствах, суд, определяющий сферу юрисдикции в конкретном вопросе, связан как внутренним (нормы международного частного права, а также, например, конституционное право), так и международным правом<sup>351</sup>. Это бесспорно и действительно часто, но, к сожалению, не всегда отражается в решениях судов. Интересный прецедент произошел в 2017 году в деле «Х против Твиттер»<sup>352</sup>. Так, судья Пембрук удовлетворил решение суда, требующее от Twitter удалять контент, размещенный одним из его пользователей «в любой точке мира». На самом деле, решение доходило до того, что требовало от Twitter запретить пользователю-нарушителю когда-либо снова публиковать любой тип контента в Twitter, даже если было возможно, что пользователь-нарушитель не был австралийцем<sup>353</sup>. Закон, на котором Комиссар по электронной безопасности основал свое требование, имел следующие положения: «...могут ли к материалам получить доступ конечные пользователи в Австралии», не обсуждая, что это означает на практике<sup>354</sup>. Аналогичным образом, благодаря недавней реформе австралийского законодательства суды получают право предписывать цифровому посреднику, такому как платформа социальных сетей, предпринять шаги по предотвращению

<sup>349</sup> Lindskoug Patrik (2013) Global content orders: A legal analysis of eSafety Commissioner 14 Legal Theories of Private International Law: Overview and Practical Implications for Internet Regulation // Essays in Honour of Michael Bogdan. P. 539-555.

<sup>350</sup> Svantesson D. «Scope of Jurisdiction» - A Key Battleground for Private International Law Applied to the Internet, Yearbook of Private International Law // These ten principles were first. 2020. Vol. 22. P. 245-274.

<sup>351</sup> Svantesson Dan Jerker B., Symeonides Symeon C. Cross-border internet defamation conflicts and what to do about them: Two proposals // Journal of Private International Law. 2023. № 19(2). P. 137-185.

<sup>352</sup> X v Twitter Inc [2017] NSWSC 1300 (28 September 2017). URL: <https://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html> (дата обращения: 01.05.2025).

<sup>353</sup> URL: <https://www.linkedin.com/pulse/sydney-become-internet-content-blocking-capital-world-svantesson/?trackingId=yA8980A1Q0GE23P4zsRsjw%3D%3D> (дата обращения: 01.05.2025).

<sup>354</sup> Smith M., Nolan M., Gaffey J. Online safety and social media regulation in Australia: eSafety Commissioner v X Corp. // Griffith Law Review. 2024. № 33(1). P. 1-17.

доступа или другие шаги, которые суд сочтет необходимыми в данных обстоятельствах для предотвращения или ограничения продолжения публикации или переиздания материалов дела; однако разработчики закона отказались рассматривать вопрос о сфере юрисдикции, поэтому они не устанавливают каких-либо ограничений, препятствующих изданию приказов, имеющих глобальное действие, или не дают указаний в отношении них<sup>355</sup>. Сфера юрисдикции должна определяться с учетом потенциального воздействия на другие государства и на лиц в других государствах. Однако, как признано, например, AG Szpunar и Апелляционным судом в деле Google Канада, в любом случае любое решение суда, затрагивающее суверенитет другого государства, должно быть тщательно оценено на предмет того, является ли оно, тем не менее, уместным<sup>356</sup>.

Таким образом, регулирование онлайн-контента поднимает ряд сложных вопросов, с которыми обычно приходится сталкиваться судам и законодателям и, учитывая центральную роль свободы выражения мнений в любой функционирующей демократии, поставленные вопросы действительно важны. В настоящее время в Австралии есть законодательно установленный минимальный возраст для использования социальных сетей. Уточним, что ранее какие-то ограничения (для несовершеннолетних младше 13 лет) предполагались только исходя из общих ограничений, которые устанавливались на крупнейших онлайн платформах в сети «Интернет», которые созданы или функционируют в соответствии с законодательством США. В этом контексте следует сказать, что как в государстве – родоначальнике социальных сетей, в США вопросы информационной безопасности достаточно обширно регламентированы следующими нормативными правовыми актами: от Закона о компьютерном мошенничестве и злоупотреблениях (CFAA)<sup>357</sup> до более специализированных

---

<sup>355</sup> Svantesson D. Global content orders: A legal analysis of eSafety Commissioner v X Corp. (May 7, 2024). URL: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4819178](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4819178) (дата обращения: 01.05.2025).

<sup>356</sup> Decision of the Court of Appeal of British Columbia dated June 11, 2015. URL: <https://www.eff.org/files/2015/12/16/2015bcca265.pdf> (дата обращения: 01.05.2025).

<sup>357</sup> The Computer Fraud and Abuse Act 1986 (CFAA). URL: <https://www.congress.gov/bill/99th-congress/house-bill/4718> (дата обращения: 01.05.2025).



законов «О защите детей в Интернете» (CIPA))<sup>358</sup> и «О защите частной жизни детей в Интернете» (COPPA))<sup>359</sup>. Основным органом США, который обеспечивает информационную безопасность несовершеннолетних в сети «Интернет», является Федеральная торговая комиссия (FTC), приоритетной задачей которой выступает защита конфиденциальности детей и безопасности данных граждан, а также надзор за соблюдением закона о защите конфиденциальности детей в Интернете (COPPA), который регулирует сбор и использование личной информации детей в возрасте до 13 лет в Интернете. FTC уделяет особое внимание вопросам конфиденциальности детей в Интернете<sup>360</sup>, в связи с чем Конгресс поручил Федеральной торговой комиссии (FTC), национальному агентству по защите прав потребителей, издать Правила о защите конфиденциальности детей в Интернете. Эти правила действовали с 2000 года, и FTC пересмотрела их только в 2013 году<sup>361</sup>. Некоторые полномочия FTC в рамках COPPA: 1) устанавливать требования к операторам коммерческих сайтов и онлайн-сервисов, направленных на детскую аудиторию или собирающих личную информацию от детей младше 13 лет; 2) требовать от операторов получения поддающегося проверке согласия родителей детей перед сбором, использованием или раскрытием информации о детях (за некоторыми ограниченными исключениями); 3) давать родителям доступ к личной информации их ребенка; 4) запрещать требовать от ребенка предоставления большего объема личной информации, чем необходимо для участия в определенном действии; 5) устанавливать и поддерживать процедуры для защиты конфиденциальности, безопасности и целостности личной информации; 6) закон применяется к сайтам, которые находятся под юрисдикцией США, имеют серверы на территории США или рассчитаны на американскую аудиторию. FTC осуществляет надзор за соблюдением требований COPPA, которые также распространяется на операторов,

<sup>358</sup> Children's Internet Protection Act 2000 (CIPA). URL: <https://www.congress.gov/congressional-report/106th-congress/senate-report/141> (дата обращения: 01.05.2025).

<sup>359</sup> Children's Online Privacy Protection Act 2000 (COPPA). URL: <https://www.congress.gov/> (дата обращения: 01.05.2025).

<sup>360</sup> Gengler B. FTC rules for children on the Internet // Computer Fraud & Security. 1999. № (6). P. 8-9.

<sup>361</sup> FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule. URL: <https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over-their-information-amending-childrens> (дата обращения: 01.05.2025).

если они «фактически знают», что собирают персональные данные пользователей другого сайта или онлайн-сервиса, ориентированного на детей младше 13 лет. Это означает, что в определенных обстоятельствах COPPA распространяется на рекламные сети, плагины и других третьих лиц. Интересен тот момент, что понятие «actual knowledge» («фактически знают») легально не определено, но FTC исходит из того, что оператор обладает фактическими знаниями о возрасте пользователя, если сайт или сервис запрашивает и получает от пользователя информацию, которая позволяет определить его возраст. Например, оператор, запрашивающий дату рождения на странице регистрации сайта, обладает фактическими знаниями в соответствии с определением COPPA, если пользователь указывает год рождения, который позволяет предположить, что ему меньше 13 лет. Закон о защите конфиденциальности детей в интернете (COPPA) дает родителям контроль над тем, какую информацию веб-сайты могут собирать об их детях<sup>362</sup>. В своей научно-правовой статье W. Hartzog (В. Харцог) и D. J. Solove (Д. Дж. Солов), рассматривая сферу полномочий FTC в области конфиденциальности и безопасности данных, в том числе и по информационной защите несовершеннолетних в сети «Интернет», пришли к выводу, что FTC не только обладает полномочиями регулировать защиту данных в той мере, в какой она это делает, но и предоставленная ей юрисдикция может значительно расширить сферу ее действий, то есть нынешние полномочия FTC по защите данных являются неотъемлемой частью режима защиты данных в США и должны быть в полной мере использованы для устранения вреда, причиняемого конфиденциальности, который не устраняется существующими средствами правовой защиты, доступными в рамках деликтного или договорного права, а также различными законами. В отличие от правовых теорий, лежащих в основе этих других исковых требований, FTC может регулировать вопрос с совершенно иным и более гибким пониманием вреда, чем то, которое сосредоточено на денежном или физическом ущербе<sup>363</sup>.

<sup>362</sup> The Children's Online Privacy Protection Rule (COPPA Rule). URL: <https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule> (дата обращения: 01.05.2025).

<sup>363</sup> Hartzog W., Solove D. J. The scope and potential of FTC data protection. November 2015 // The George Washington law review. 2015. № 83(6). P. 2230-2300.

Также считаем важным отметить, что имеется Законопроект S.1409 Kids Online Safety Act от 2023 (Закон о безопасности детей в Интернете)<sup>364</sup>, который устанавливает требования по защите несовершеннолетних от вреда в сети «Интернет». Требования распространяются на платформы, которые являются приложениями или сервисами (например, социальными сетями), подключенными к Интернету и, вероятно, используемыми несовершеннолетними. Однако законопроект освобождает от этих требований интернет-провайдеров, почтовые сервисы, образовательные учреждения. Кроме того, платформы, подпадающие под действие закона, должны предоставлять: 1) несовершеннолетним – определенные меры защиты, такие как настройки, ограничивающие доступ к их личным данным; 2) законным представителям несовершеннолетних – инструменты для контроля использования несовершеннолетними платформы, такие как контроль конфиденциальности и настроек учетной записи. Законопроект предусматривает принудительное исполнение требований через FTC и, кроме того, требует, чтобы FTC заключила контракт с Национальной Академией наук США для изучения рисков причинения вреда несовершеннолетним при использовании социальных сетей и других онлайн-платформ. В результате исследования законодательного обеспечения информационной политики США О. Likhota (Олександр Лихота)<sup>365</sup> приходит к выводу, что, хотя в США существует надежная правовая база, сохраняются проблемы, связанные с быстрыми темпами технологических изменений, ростом роли социальных сетей в качестве основных источников информации (и дезинформации) и растущей изоционностью киберугроз. Растущее влияние алгоритмов на модерацию контента создает новые проблемы, связанные с предвзятостью и цензурой.

Рассмотрим далее органы публичной власти, обеспечивающие информационную безопасность несовершеннолетних в государствах ЕС и Великобритании.

<sup>364</sup> S.1409 Kids Online Safety Act 2023. URL: <https://www.congress.gov/bill/118th-congress/senate-bill/1409> (дата обращения: 01.05.2025).

<sup>365</sup> Likhota O. Legislative support of the US information policy // Economics Finances Law 3/2024(-). 2025. P. 65-68.

Во Франции в настоящее время действуют три основных закона в сфере обеспечения информационной безопасности несовершеннолетних: 1) Закон Франции № 78-17 от 06.01.1978 «Об обработке данных, файлах и свободах»<sup>366</sup>, принятый в целях обеспечения прав и законных интересов лиц, в том числе несовершеннолетних, в электронном пространстве; 2) Закон № 2022-140 от 07.02.2022 «О защите детей»<sup>367</sup>, содержащий меры по защите несовершеннолетних; 3) Закон Франции № 2024-449 от 21.05.2024 «О безопасности и регулировании цифрового пространства» (LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique)<sup>368</sup>, который устанавливает случаи возрастных ограничений для несовершеннолетних в сети «Интернет».

На основании Кодекса социального действия и семьи Франции<sup>369</sup> и для реализации вышесказанных законов создан Национальный совет по защите детей, в состав которого вошли представители различных органов власти (в том числе и мировых судей), а также представители общественных организаций, занимающихся воспитанием и (или) защитой прав несовершеннолетних<sup>370</sup>. Компетенцию Национального совета по защите детей составляют рекомендации по профилактике негативного влияния на детей и защиты от информации, причиняющей вред здоровью и (или) развитию несовершеннолетних (ст. 147-13), а также рекомендации по проектам французским законов, которые затрагивают вопросы защиты несовершеннолетних лиц.

Также в ведении председателя окружного совета осуществляет свою деятельность Служба социальной помощи детям (Aidesocialeal'enfance (ASE), выполняя следующие задачи: 1) оказание различных видов помощи (материальной, психологической, воспитательной, образовательной) несовершеннолетним лицам, а

<sup>366</sup> Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Journal officiel du 7 janvier 1978 et rectificatif au J.O. du 25 janvier 1978). URL: <https://www.ssi.ens.fr/textes/178-17-text.html> (дата обращения: 01.05.2025).

<sup>367</sup> LOI n° 2022-140 du 7 février 2022 relative à la protection des enfants. URL: <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000043668561/> (дата обращения: 01.05.2025).

<sup>368</sup> LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368> (дата обращения: 01.05.2025).

<sup>369</sup> Code de l'action sociale et des familles. URL: [https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006074069/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006074069/) (дата обращения: 01.05.2025).

<sup>370</sup> Правовое регулирование защиты несовершеннолетних от деструктивной информационной среды : монография / Под общ. ред. С. Е. Титов. М. : РУСАИНС, 2025. С. 35-36.

также членам их семей в ситуациях, которые могут поставить под угрозу здоровье, безопасность, нравственность этих несовершеннолетних или серьезно поставить под угрозу их физическое, эмоциональное, интеллектуальное и психологическое развитие (1° ст. L221-1)); 2) осуществление профилактических мер (2° ст. L221-1); 3) предотвращение рисков, в том числе информационных, в отношении несовершеннолетних (3° ст. L221-1); 4) контроль взаимодействий между несовершеннолетним лицом и третьими лицами (за исключением родителей), когда отношения должны поддерживаться и развиваться в интересах ребенка и др. (6°–8° ст. L221-1)<sup>371</sup>. Согласно УК Франции (Code pénal)<sup>372</sup> вовлечение несовершеннолетнего лица в перевозку, хранение, передачу, распространение запрещенных веществ (наркотических и т. д.), в том числе совершенные с применением сети «Интернет», наказывается сроком лишения свободы до 7 лет и штрафом в размере 150 тысяч евро. Интересным является тот факт, что в соответствии со ст. 227-17 Code pénal установлена уголовная ответственность для родителей (законных представителей) несовершеннолетнего лица, если ими без уважительной причины не выполнялись обязанности по воспитанию или их действия (бездействие) причинили вред здоровью, безопасности, нравственности несовершеннолетнего лица. Ответственность предусмотрена в виде лишения свободы сроком до двух лет и штрафа в размере 30 тысяч евро.

Также функционирует официальный правительственный портал internet-signalement.gouv.fr, предназначенный для сообщения в правоохранительные органы пользователями сети «Интернет» о выявлении незаконного или подозрительного контента, который находится в публичном доступе и может деструктивно влиять на несовершеннолетних лиц. Все сайты во Франции должны пройти регистрацию в ICRA (Ассоциация рейтинга интернет-контента) или в RTA («только для взрослых»), которые присваивают сайту (странице сайта) рейтинг (метки). Метка «Только для взрослых» на веб-сайтах была создана Ассоциацией сайтов,

<sup>371</sup> Там же.

<sup>372</sup> Code pénal. URL: [https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006070719/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/) (дата обращения: 01.05.2025).

выступающих за защиту детей (ASACP) для более эффективной родительской фильтрации и демонстрации стремления индустрии онлайн-развлечений для совершеннолетних помогать родителям предотвращать просмотр детьми деструктивного для них контента. Метка RTA является бесплатной, добровольной и общедоступной для любого веб-сайта, который обозначает себя как контент, не предназначенный для просмотра лицами до 18 лет.

Министерство внутренних дел Франции ведет борьбу со всеми формами киберпреступности, направленной как против национальных учреждений и интересов, юридических лиц и государственных органов, так и против физических лиц. С этой целью министерство опирается на специализированные центральные службы и территориальные сети национальной полиции, национальной жандармерии и силы внутренней безопасности. Им поручено ведение следственной деятельности с целью выявления и привлечения к судебной ответственности лиц, виновных в злонамеренных действиях в компьютерных системах и сетях. Эти службы также участвуют в профилактической и информационной работе с соответствующими категориями граждан, в том числе с несовершеннолетними. Так, работа специализированных отделов в региональных отделениях полиции направлена на борьбу с преступлениями в сфере информации и непосредственно совершенных в онлайн-среде, в том числе деятельность этих отделов направлена на обеспечение информационной безопасности несовершеннолетних лиц в сети «Интернет».

Не так давно принят Закон Франции № 2024-449 от 21.05.2024 «О безопасности и регулировании цифрового пространства»<sup>373</sup>, в котором раздел 1 посвящен защите несовершеннолетних в сети «Интернет» (ст. 1–6). Так, ст. 1 касается надежности контроля возраста пользователей и уважения их конфиденциальности; орган, регулирующий аудиовизуальные и цифровые коммуникации, может потребовать от издателей и поставщиков услуг, в том числе в сети «Интернет», упомянутых в первом абзаце настоящего пункта I, провести

---

<sup>373</sup> LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368> (дата обращения: 01.05.2025).

аудит систем проверки возраста, которые они внедряют, чтобы подтвердить соответствие этих систем техническим требованиям, установленных законом. Иными словами, законодательно потребовали от платформ, имеющих риски деструктивной информации для совершеннолетних (например, порнографические видеоролики), установить системы проверки возраста для предотвращения доступа несовершеннолетних; ввели новый вид правонарушения – оскорбление в Интернете, позволяющий налагать фиксированный штраф на любого, кто, оставаясь безнаказанным, допускает дискриминационное, оскорбительное или домогательское поведение в сети «Интернет». Теоретически социальные сети не открыты для детей младше 13 лет. Однако первая регистрация в среднем происходит в возрасте 8,5 лет и, по данным Национальной комиссии по информационным технологиям и гражданским свободам (CNIL), в них присутствует более половины детей в возрасте 10–14 лет<sup>374</sup>. Отметим, что Национальная комиссия по информационным технологиям и гражданским свободам (Commission nationale de l'informatique et des libertés (CNIL)) – национальный орган защиты данных во Франции, с 2022 года проводит исследования по вариантам онлайн-верификации возраста.

В своих Рекомендациях<sup>375</sup> CNIL обозначает принципы системы проверки возраста: минимизация, пропорциональность, надежность, простота, стандартизация, вмешательство третьей стороны.

Предлагает следующие варианты подтверждения возраста в сети «Интернет»<sup>376</sup>:

- подтверждение возраста с помощью валидации платежной карты;
- проверка возраста с помощью оценки, основанной на анализе лица;
- автономная система верификации (собственно, это офлайн-проверка: например, получение «карт для регистрации» в местах, где могут продавать

<sup>374</sup> URL: [https://www.lemonde.fr/pixels/article/2023/06/29/reseaux-sociaux-vote-final-au-parlement-pour-instaurer-un-accord-parental-obligatoire-pour-les-mineurs-de-moins-de-15-ans\\_6179745\\_4408996.html](https://www.lemonde.fr/pixels/article/2023/06/29/reseaux-sociaux-vote-final-au-parlement-pour-instaurer-un-accord-parental-obligatoire-pour-les-mineurs-de-moins-de-15-ans_6179745_4408996.html) (дата обращения: 01.05.2025).

<sup>375</sup> Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy 09 August 2021. URL: <https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childrens-privacy> (дата обращения: 01.05.2025).

<sup>376</sup> Online age verification: balancing privacy and the protection of minors. URL: <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors> (дата обращения: 01.05.2025).

алкоголь или табак, при покупке которых нужно предоставить документ, подтверждающий возраст);

- проверка возраста путем анализа документов, удостоверяющих личность;
- использование инструментов, предоставляемых центральным правительством, для проверки личности и возраста (использование общедоступных баз данных или системы аутентификации);
- системы проверки возраста на основе логических выводов (варианты: импорт истории просмотров в сети «Интернет»; анализ «зрелости» с помощью опросника; анализ просмотров на собственных сервисах издателя (в частности, на основных цифровых платформах)).

В целом, исследование показало, что универсальных мер подтверждения на сегодняшний день не выявлено, так как либо предусматривается массовый сбор персональных (в том числе биометрических) данных, либо меры неэффективны.

Как написано в главе 1 нашего исследования, в Федеративной Республике Германия действуют следующие основные нормативные правовые акты в сфере обеспечения информационной безопасности несовершеннолетних: Закон о защите молодежи от 23.07.2002 (JuSchG)<sup>377</sup>; Закон об улучшении правоприменения в социальных сетях от 01.10.2017 (NetzDG)<sup>378</sup>; Государственный договор о защите детей и молодежи в сфере СМИ от 13.09.2002 ((JMStV)<sup>379</sup>. Так, согласно § 21 JuSchG ведется «Список средств массовой информации, представляющих опасность для молодежи». Нормы NetzDG устанавливают обязательность и порядок рассмотрения жалоб на незаконный или нежелательный контент (например, содержащий интернет-травлю), которые направляются владельцам или администрации интернет-сайтов. При этом сам удаленный контент должен храниться, так как в случае обращения заинтересованных лиц в суд, по

<sup>377</sup> Jugendschutzgesetz vom 23. Juli 2002 (BGBl. I S. 2730), das zuletzt durch Artikel 1 des Gesetzes vom 9. April 2021 (BGBl. I S. 742) geändert worden ist. URL: <https://www.buzer.de/JuSchG.htm> (дата обращения: 01.05.2025).

<sup>378</sup> Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) 1. September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 29 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist. URL: <https://www.buzer.de/gesetz/12799/index.htm> (дата обращения: 01.05.2025).

<sup>379</sup> Jugendmedienschutz-Staatsvertrag (JMStV) vom 13. September 2002 (GVBl. 2003 S. 147, BayRS 02-21-S), der zuletzt durch Art. 2 des Vertrages vom 27. Februar 2024 (GVBl. S. 326) geändert worden ist. URL: <https://www.gesetze-bayern.de/Content/Document/JMStV> (дата обращения: 01.05.2025).



требованию суда владельцы сайтов должны предоставить материалы (контент). Кроме того, NetzDG закрепляет за надзорным органом по защите несовершеннолетних право досудебного воздействия на лиц, которые распространяли информацию, причиняющую вред здоровью или развитию несовершеннолетних лиц. Согласно ст. (1) § 17 Закона о защите молодежи (JuSchG) Федеральный центр защиты детей и молодежи (Die Bundeszentrale für Kinder und Jugendmedienschutz – BzKJ) является независимым федеральным надзорным органом в сфере деятельности Федерального министерства по делам семьи, пожилых людей, женщин и молодежи (BMFSFJ) со штаб-квартирой в Бонне. Его обязанности вытекают из Закона о защите молодежи (JuSchG)<sup>380</sup>. Федеральный центр защиты детей и молодежи от СМИ» (BzKJ) имеет расширенную сферу деятельности:

- BzKJ по-прежнему отвечает за индексацию СМИ, представляющих опасность для несовершеннолетних, и имеет для этого соответствующий контрольный орган. Кроме того, BzKJ несет обширную ответственность за содействие дальнейшему развитию защиты несовершеннолетних от СМИ. Он выполняет ориентирующую функцию для родителей, специалистов, а также для самих несовершеннолетних;

- кроме того, он следит за соблюдением установленных законом требований к поставщикам услуг и имеет право налагать крупные штрафы (до 50 млн евро) даже на поставщиков, штаб-квартира которых находится за пределами Германии.

Согласно § 21, регламентирующему процедуры, которые проводятся органом по проверке СМИ, представляющих опасность для молодежи: 1) агентство по проверке СМИ, представляющих опасность для молодежи, обычно действует по запросу; 2) имеют право на подачу заявления: Федеральное министерство по делам семьи, пожилых людей, женщин и молодежи; высшие государственные органы по делам молодежи; центральный надзорный орган стран по защите молодежных СМИ; государственные органы по делам молодежи; молодежные отделения; признанные институты добровольного самоконтроля; органы по рассмотрению

---

<sup>380</sup> Jugendschutzgesetz vom 23. Juli 2002 (BGBl. I S. 2730), das zuletzt durch Artikel 1 des Gesetzes vom 9. April 2021 (BGBl. I S. 742) geändert worden ist. URL: <https://www.buzer.de/JuSchG.htm> (дата обращения: 01.05.2025).

жалоб в сети «Интернет», финансируемые за счет средств ЕС, Федерального правительства, штатов или государственных средств массовой информации; а также за ходатайство об исключении из списка и за ходатайство об установлении того, что носитель не является полностью или по существу идентичным по содержанию носителю, уже включенному в список.

При этом следует учитывать, что согласно (6) § 21 прежде чем принимать решение о включении в список цифровой услуги или разграничиваемого контента в рамках цифровой услуги как единицы оценки, Орган по проверке СМИ, представляющих опасность для молодежи, должен предоставить центральному надзорному органу стран по защите молодежных СМИ возможность незамедлительно прокомментировать телемедиа. Мнения и запросы центрального органа стран по защите молодежных СМИ, представляющих опасность для молодежи, должен в значительной степени учитывать Орган по проверке СМИ при принятии своих решений. Если в течение пяти рабочих дней с момента запроса у Органа по проверке СМИ, представляющих опасность для молодежи, не будет заключения центрального надзорного органа стран по защите молодежных СМИ, он может принять решение без такого заключения. Раздел 3 Закона, посвященный защите детей в СМИ, устанавливает категории возрастной классификации и соответствующую маркировку информационной продукции, а в разделе 4 конкретизируются полномочия и порядок формирования BzKJ. Поставщики сервисов и владельцы интернет-ресурсов обязаны защищать несовершеннолетних пользователей от кибербуллинга, и особое внимание уделяется возрастной маркировке сайтов и контента.

Договор о защите детей и молодежи в сфере СМИ (JMStV)<sup>381</sup> представляет собой государственный договор, заключенный между всеми землями Германии, содержит положения о защите несовершеннолетних, и для этих задач учреждает в § 14 Комиссию по защите молодежи (KJM), которая является центральным надзорным органом по защите молодежи в сфере частного вещания и телемедиа (в

<sup>381</sup> Jugendmedienschutz-Staatsvertrag (JMStV) vom 13. September 2002 (GVBl. 2003 S. 147, BayRS 02-21-S), der zuletzt durch Art. 2 des Vertrages vom 27. Februar 2024 (GVBl. S. 326) geändert worden ist. URL: <https://www.gesetze-bayern.de/Content/Document/JMStV> (дата обращения: 01.05.2025).

том числе сети «Интернет»). При этом государственный договор о защите молодежных СМИ – (JMStV) объединяет частное вещание (телевидение и радиовещание) и телемедиа (в первую очередь сеть «Интернет») под надзором комиссии по защите молодежи (KJM). Это предотвратит подчинение одного и того же контента разным правилам на разных носителях. В соответствии со своим мандатом KJM проверяет наличие нарушений JMStV и принимает решение о мерах в отношении поставщиков средств массовой информации. KJM не только считает себя контролирующим органом, но и стремится инициировать социально-политические процессы. Федеральный центр по защите детей и молодежи (BzKJ) отвечает за процедуры индексации.

Государственное медиа – учреждение, имеющее лицензию на соответствующую вещательную станцию или в штате которого находится провайдер сети «Интернет», принимает меры (жалобы, запреты, штрафы), принятые KJM, который представляет собой специальный надзорный орган, отвечающий за защиту несовершеннолетних от нежелательного контента в интернете. В 2022 году сообщалось, что комиссия одобрила использование искусственного интеллекта для определения возраста пользователя, чтобы оградить детей и молодежь от «вредоносного контента». Одобрены три системы, которые с помощью искусственного интеллекта проверяют возраст пользователей, чтобы предотвратить доступ несовершеннолетних к вредоносному контенту<sup>382</sup>.

При этом, как указывают в своей научной статье Ч. Джарви (Chelsea Jarvie) и К. Ренод (Karen Renaud), «комиссия Германии по защите несовершеннолетних в СМИ одобрила использование искусственного интеллекта (ИИ) для целей проверки возраста в мае 2022 года<sup>383</sup>. <...> допустимая погрешность для некоторых технологий оценки возраста может составлять около 2 лет<sup>384</sup>, то есть в систему должен быть встроен пятилетний «буфер», поэтому 18-летним пользователям

<sup>382</sup> URL: <https://www.euractiv.com/section/digital/news/german-youth-protection-body-endorses-ai-as-biometric-age-verification-tool/> (дата обращения: 01.05.2025).

<sup>383</sup> Kabelka L. German Youth Protection Body Endorses AI as Biometric Age-Verification Tool. 2022. URL: <https://www.euractiv.com/section/digital/news/german-youth-protection-body-endorses-ai-as-biometric-age-verification-tool/> (дата обращения: 01.05.2025).

<sup>384</sup> Yoti. Yoti Age Scan. 2021. URL: <https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-May-2022.pdf> (дата обращения: 01.05.2025).

потребуется, чтобы система оценивала их возраст как минимум в 23 года, чтобы получить доступ к онлайн-продуктам или услугам»<sup>385</sup>.

В 2023 году в Великобритании принят единый акт, обеспечивающий информационную безопасность несовершеннолетних, – Закон о безопасности в Интернете 2023 года (Online Safety Act 2023)<sup>386</sup>, который защищает несовершеннолетних и взрослых в Интернете. Он возлагает ряд новых обязанностей на компании, занимающиеся социальными сетями, и поисковые сервисы, делая их более ответственными за безопасность пользователей на своих платформах. Закон налагает на провайдеров новые обязанности по внедрению систем и процессов для снижения рисков использования их сервисов в незаконных целях, а также по удалению незаконного контента в случае его появления<sup>387</sup>.

Закон о безопасности в Интернете 2023 года (Online Safety Act 2023)<sup>388</sup> устанавливает: обязанности по оценке рисков для детей (ст. 11); обязанности по обеспечению безопасности, защищающие детей (ст. 12); обязанности по обеспечению безопасности, защищающие детей: толкование (ст. 13).

Самые строгие меры защиты в законе предусмотрены для защиты несовершеннолетних: интернет-платформы должны будут предотвращать доступ детей к вредоносному и неприемлемому для их возраста контенту и предоставлять родителям и детям понятные и доступные способы сообщать о проблемах в Интернете, когда они возникают. Реализация норм Закона о безопасности в Интернете 2023 года возлагается на Управление по коммуникациям (Office of Communications (Ofcom)) как на независимого регулятора в сфере онлайн-безопасности. Ofcom определяет шаги, которые провайдеры могут предпринять для выполнения своих обязанностей по обеспечению безопасности, в сводах правил, обладает широким спектром полномочий для оценки и обеспечения соблюдения провайдерами требований. Управление по коммуникациям – регулирующий и

<sup>385</sup> Jarvie C., Renaud K. Online Age Verification: Government Legislation, Supplier Responsibilization, and Public Perceptions // Children. 2024. № 11(9). P. 1068.

<sup>386</sup> Online Safety Act 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50/enacted> (дата обращения: 01.05.2025).

<sup>387</sup> Phippen A. Online Safety Policy–Moving On? // Policy and Rights Challenges in Children’s Online Behaviour and Safety. 2025. № 2017–2023. P.p. 1-18.

<sup>388</sup> Online Safety Act 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50/enacted> (дата обращения: 01.05.2025).

антимонопольный орган в сфере телекоммуникаций Великобритании, который создан согласно Закону о коммуникациях 2003 года<sup>389</sup> и регулирует телевизионную и радиовещательную отрасли, фиксированную связь, мобильную связь, почтовые услуги, а также радиоволны, на которых работают беспроводные устройства. Также Ofcom имеет полномочия блокировать доступ к конкретным веб-сайтам и сотрудничает с Министерством науки, инноваций и технологий. У Ofcom изначально широкий спектр полномочий, а со временем он получил дополнительные обязанности и полномочия. Этот орган был впервые учрежден в соответствии с Законом об управлении связью 2002 г. (ст. 21, часть 1, раздел 3)<sup>390</sup>, а затем в соответствии с законом о безопасности в Интернете Ofcom также получил дополнительные полномочия, например, может штрафовать компании, которые не соблюдают новую обязанность по защите пользователей от вредоносного контента в Интернете (ст. 21, ч. 1, раздел 3 Закона о коммуникациях 2003 г.). Ofcom назначен регулятором режима онлайн-безопасности и получил новую основную обязанность – обеспечивать надлежащую защиту граждан (в том числе несовершеннолетних) от информации, причиняющей вред их здоровью или развитию. Это достигается за счет того, что онлайн-сервисы обязаны надлежащим образом использовать системы и процессы (например, позволяющие пользователям сообщать о вредоносном контенте и удалять его) для обеспечения безопасности пользователей. Управление по коммуникациям имеет право принуждать компании к соблюдению требований, налагать штрафы в размере 18 млн фунтов стерлингов или 10 % от общего годового оборота (в зависимости от того, какая сумма больше) и блокировать сервисы, не соответствующие требованиям. Ofcom публикует своды правил, которые помогают компаниям справиться с этими новыми требованиями (ст. 41 ч. 5 разд. 3 Закона о безопасности в Интернете 2023 года (Online Safety Act 2023))<sup>391</sup>.

Согласно ст. 152 ч. 7 разд. 4 Online Safety Act 2023 должен быть учрежден Консультативный комитет по дезинформации и ложной информации в составе

<sup>389</sup> Communications Act 2003. URL: [www.legislation.gov.uk/ukpga/2003/21/section/3](http://www.legislation.gov.uk/ukpga/2003/21/section/3) (дата обращения: 01.05.2025).

<sup>390</sup> Office of Communications Act 2002. URL: <https://www.legislation.gov.uk/ukpga/2002/11> (дата обращения: 01.05.2025).

<sup>391</sup> Online Safety Act 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50/enacted> (дата обращения: 01.05.2025).

OFCOM для создания и поддержания работы комитета, предоставляющего консультации, указанные в этом разделе. Комитет должен состоять из председателя, назначенного OFCOM, и такого количества других членов, назначенных OFCOM, которое OFCOM сочтет целесообразным. Согласно требованиям законодательства (4) ст. 152 Online Safety Act 2023, функция комитета состоит в предоставлении рекомендаций в Ofcom по конкретным направлениям работы, связанным с дезинформацией и ложной информацией. Уточним, что на момент написания диссертационного исследования «Консультативный комитет по дезинформации и ложной информации» (Advisory Committee on Disinformation and Misinformation) «находится в процессе создания Ofcom»<sup>392</sup>, хотя «Положение о Консультативном комитете по дезинформации и недостоверной информации» подготовлено еще от 29 ноября 2024 года<sup>393</sup>. Также следует сказать, что технологии верификации возраста, которые не нарушали бы конфиденциальность пользователей и предусмотрены Online Safety Act 2023<sup>394</sup>, по состоянию на начало ноября 2025 разрабатываются и тестируются.

Ofcom обеспечивает, чтобы технологические компании при разработке и предоставлении своих услуг в Великобритании в первую очередь заботились о безопасности. Меры включают:

1) более безопасные каналы. Персонализированные рекомендации – основной способ, с помощью которого несовершеннолетние могут столкнуться с вредоносным контентом в Интернете. Любой провайдер, использующий рекомендательную систему и представляющий себе средний или высокий риск распространения вредоносного контента, должен настроить свои алгоритмы таким образом, чтобы отфильтровывать вредоносный контент из детских каналов;

2) эффективная проверка возраста. Наиболее рискованные сервисы должны использовать высокоэффективную проверку возраста, чтобы определять, кто из

<sup>392</sup> Официальный сайт OFCOM. URL: <https://www.ofcom.org.uk/about-ofcom/structure-and-leadership/advisory-committee-on-disinformation-and-misinformation> (дата обращения: 01.05.2025).

<sup>393</sup> Advisory Committee on Disinformation and Misinformation Terms of Reference 29 November 2024. URL: <https://www.ofcom.org.uk/siteassets/resources/documents/about-ofcom/how-ofcom-is-run/mis-and-dis-information-committee/advisory-committee-on-disinformation-and-misinformation-terms-of-reference.pdf?v=386330> (дата обращения: 01.05.2025).

<sup>394</sup> Online Safety Act 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50/enacted> (дата обращения: 01.05.2025).

пользователей является несовершеннолетним. То есть они могут защитить несовершеннолетнего от вредоносного контента, сохраняя при этом права взрослых на доступ к легальному контенту. Это может включать в себя запрет несовершеннолетним на доступ ко всему сайту или приложению или только к некоторым частям или видам контента (ст. 12 (4) Online Safety Act 2023) и т. д. Вышеуказанные меры основаны на правилах, которые также дополняют специальные требования к порнографическим сайтам, чтобы несовершеннолетние не сталкивались с порнографией в Интернете, а именно: Ofcom опубликовал первое издание свода правил и рекомендаций<sup>395</sup> по борьбе с информацией, несущей вред (таким как терроризм, ненависть, мошенничество, сексуальное насилие над детьми, а также содействие или поощрение самоубийств) в соответствии с Законом Великобритании о безопасности в Интернете<sup>396</sup>. Принимая во внимание эти уникальные сведения, меры были специально разработаны Ofcom для борьбы с путями, ведущими к онлайн-грумингу<sup>397</sup>. Это означает, что по умолчанию на платформах, где пользователи общаются друг с другом, профили и местоположения несовершеннолетних, а также их друзья и связи не должны быть видны другим пользователям, а пользователи, не состоящие в отношениях, не должны иметь возможности отправлять им личные сообщения. Несовершеннолетние также должны получать информацию, которая поможет им принимать взвешенные решения о рисках, связанных с раскрытием личной информации.

У поставщиков услуг, к которым могут получить доступ несовершеннолетние в Великобритании, есть время до 24 июля 2025 года, чтобы завершить и зафиксировать оценку рисков, которые их услуги представляют для несовершеннолетних. Затем они должны внедрить меры безопасности для

<sup>395</sup> Statement: Protecting people from illegal harms online. URL: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-people-from-illegal-harms-online> (дата обращения: 01.05.2025).

<sup>396</sup> Закон возлагает новые обязанности по обеспечению безопасности на компании, работающие в сфере социальных сетей, поисковых систем, обмена сообщениями, игр и приложений для знакомств, а также на сайты с порнографией и файлами для обмена.

<sup>397</sup> Под «онлайн-грумингом» понимается одна из форм сексуальной эксплуатации детей, а именно общение взрослого человека с несовершеннолетним в сети «Интернет» с целью совращения, получения личных чувствительных данных несовершеннолетнего, шантажа. Подробнее: Sani A. I., Vara M., Dinis M. A. P. Online Sexual Grooming of Children: Psychological and Legal Perspectives for Prevention and Risk Management // *Modern Insights and Strategies in Victimology* (pp. 25-55) Chapter: 2. Publisher: IGI Global. 2024.

снижения этих рисков и с 25 июля 2025 года должны применять меры безопасности, изложенные Ofcom, для снижения этих рисков.

В Ирландии 10 декабря 2022 года принят Закон о безопасности в Интернете и регулировании СМИ (OSMR)<sup>398</sup>, при этом 18 мая 2021 года правительство одобрило интеграцию законопроекта «Телерадиовещание (поправка)» от 2019 года в законопроект OSMR и введение трех дополнительных глав законопроекта. Управление по вопросам вещания Ирландии было упразднено, а Coimisiún na Meán официально учрежден в качестве национального регулирующего органа Ирландии в соответствии со ст. 30 Директивы ЕС об аудиовизуальных медиауслугах (AVMSD). Coimisiún отвечает за надзор за регулированием вещания и услуг видео по запросу, а также за новую нормативно-правовую базу в сфере онлайн-безопасности. Часть 2 ст. 7 Закона Ирландии о безопасности в сети «Интернет» и регулировании СМИ (OSMR) устанавливает полномочия Coimisiún na Meán в части обеспечения информационной безопасности несовершеннолетних: ввести отраслевые сборы для финансирования своей деятельности; требовать предоставления информации от регулируемых служб; назначить уполномоченных должностных лиц для расследования предполагаемого несоблюдения; добиваться наложения административных финансовых санкций в размере до 20 млн евро или 10 % от оборота в случае несоблюдения требований; рассылать уведомления о прекращении несоблюдения требований; добиваться привлечения к ответственности высшего руководства указанных онлайн-сервисов за несоблюдение требований уведомления о прекращении нарушений; пытаться заблокировать доступ к определенным онлайн-сервисам; направлять уведомления об ограничении контента в отношении отдельных фрагментов вредоносного онлайн-контента в соответствующие онлайн-сервисы.

<sup>398</sup> Online Safety and Media Regulation Act Number 41 of 2022. URL: <https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/html> (дата обращения: 01.05.2025).



Закон OSMR предусматривает назначение комиссара по безопасности в сети «Интернет» в Coimisiún na Meán (часть 2 (ст. 11) Закона OSMR), который отвечает за соблюдение обязательного кодекса безопасности в Интернете<sup>399</sup>.

Соответствующие онлайн-сервисы, находящиеся под юрисдикцией Ирландии и признанные Coimisiún na Meán, в том числе платформы для обмена видео, должны соблюдать обязательные к исполнению Кодексы онлайн-безопасности, которые Coimisiún na Meán разрабатывает (2A (1) Закона OSMR). Эти Кодексы направлены на то, чтобы обеспечить принятие соответствующими поставщиками онлайн-услуг надлежащих мер для сведения к минимуму доступности вредоносного контента, как это определено в Законе OSMR. Хотя в Законе уже перечислен широкий спектр видов вреда, Coimisiún na Meán может предлагать правительству новые категории вредоносного онлайн-контента. В отношении онлайн-сервисов, находящихся за пределами ирландской юрисдикции, Coimisiún na Meán будет иметь право заключать добровольные соглашения с этими провайдерами для соблюдения Кодексов. В соответствии с этим законом Coimisiún na Meán обладает широкими полномочиями по мониторингу и обеспечению соблюдения правил безопасности в Интернете, в том числе по проведению расследований в случае подозрений в несоблюдении правил и наложению санкций, таких как крупные штрафы (часть 2 Закона OSMR)<sup>400</sup>. Закон OSMR и его реализация, в том числе посредством применения и соблюдения первого кодекса онлайн-безопасности, являются лишь одним из трех компонентов общей системы онлайн-безопасности Coimisiún na Meán. Двумя другими компонентами являются Закон ЕС о цифровых услугах и Положение о террористическом контенте в Интернете<sup>401</sup>. Coimisiún na Meán отвечает за реализацию этих мер в Ирландии, но ответственность за их политику лежит на Министерстве предпринимательства, торговли и занятости и Министерстве юстиции соответственно. Закон OSMR также

<sup>399</sup> Online Safety Code 2024 (Coimisiún na Meán). URL: <https://www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf> (дата обращения: 01.05.2025).

<sup>400</sup> Online Safety and Media Regulation Act Number 41 of 2022. URL: <https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/html> (дата обращения: 01.05.2025).

<sup>401</sup> Регламент (ЕС) 2021/784 Европейского парламента и Совета от 29 апреля 2021 года о борьбе с распространением террористического контента в интернете (текст с учётом ЕОЗ). URL: <https://eur-lex.europa.eu/eli/reg/2021/784/oj> (дата обращения: 01.05.2025).

позволяет Coimisiún na Meán разрабатывать рекомендательные к исполнению материалы по безопасности в Интернете, касающиеся не только вредоносного онлайн-контента, но и контента, не соответствующего возрасту, в том числе порнографии и грубого и бессмысленного насилия.

## **2.2. Органы публичной власти в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в России**

Российская система органов публичной власти по обеспечению информационной безопасности несовершеннолетних в сети «Интернет» регламентируется федеральными законами «О защите детей от информации, причиняющей вред их здоровью и развитию»<sup>402</sup>, «Об основных гарантиях прав ребенка в Российской Федерации»<sup>403</sup>, «Об информации, информационных технологиях и о защите информации»<sup>404</sup> и иными нормативно-правовыми актами.

По мнению Т. М. Заниной и Е. И. Лукиной, именно на государстве лежит обязанность «построения целостной и сбалансированной системы обеспечения информационно-психологической безопасности несовершеннолетних»<sup>405</sup>. В своем диссертационном исследовании 2003 года О. А. Федотова указывает, что в научных трудах принята «трехуровневая система субъектов обеспечения информационной безопасности»: органы публичной власти; объединения и организации; физические лица, при условии их участия в рассматриваемых нами правоотношениях<sup>406</sup>. В. А. Зоз и А. С. Лагуточкина в 2016 году провели исследование практики зарубежных государств в сфере защиты несовершеннолетних от деструктивного контента в сети «Интернет», выделили при этом «три возможных способа само-

<sup>402</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>403</sup> Федеральный закон от 24.07.1998 № 124-ФЗ (ред. от 30.11.2024) «Об основных гарантиях прав ребенка в Российской Федерации» // СЗ РФ. 1998. № 31. Ст. 3802; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>404</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; СЗ РФ. 2024. № 48. Ст. 7218.

<sup>405</sup> Занина Т. М., Лукина Е. И. Формирование государственной системы защиты несовершеннолетних от вредоносной информации в Российской Федерации // Научный вестник Омской академии МВД России. 2016. № 3 (62). С. 40-44.

<sup>406</sup> Федотова О. А. Административная ответственность за правонарушения в сфере обеспечения информационной безопасности : дис. ... канд. юрид. наук. М., 2003. С. 24.

сорегулирования отношений»<sup>407</sup>, а именно: государственный (принятие и реализация НПА, контрольно-надзорные полномочия и т. д.); саморегулирование (например, при условии высокой организованности цифровых платформ, а также иными участниками онлайн-отношений); комплексный способ, выраженный в сочетании публичного и общественных способов регулирования. На наш взгляд, в РФ представлен комплексный способ регулирования отношений по обеспечению информационной безопасности несовершеннолетних. Рассмотрим этот вопрос более детально. Так, ст. 4 Закона № 436-ФЗ<sup>408</sup> устанавливает полномочия федеральных органов исполнительной власти (ч. 1) и региональных органов государственной власти (ч. 2) в сфере защиты несовершеннолетних от деструктивного контента. К полномочиям федеральных органов отнесено: разработка и реализация политики, перечня федеральных мероприятий<sup>409</sup>, федеральный государственный контроль (надзор) за соблюдением законодательства в данной сфере; регламентирование порядка экспертизы информационной продукции (отметим, что данная продукция размещается и в сети «Интернет»)<sup>410</sup>. У региональных органов государственной власти полномочия включают разработку и реализацию перечня региональных мероприятий в этой сфере и иные полномочия. При этом следует сказать, что Закон № 436-ФЗ не выстраивает систему государственных органов в сфере защиты несовершеннолетних от информации, причиняющей вред их здоровью и (или) развитию как в целом, так и непосредственно в сети «Интернет». Так, только в ч. 1 ст. 20 Закона № 436-ФЗ указаны конкретные федеральные органы исполнительной власти, осуществляющие функции государственного контроля (надзора) за соблюдением законодательства в области защиты несовершеннолетних от деструктивного

<sup>407</sup> Зоз В. А., Лагуточкина А. С. Об отдельных направлениях правового регулирования сетевой безопасности цифровой среды в условиях противодействия подростковой преступности // Вестник Саратовской государственной юридической академии. 2022. № 6 (149). С. 289-297.

<sup>408</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>409</sup> Приказ Минцифры России от 22.03.2022 № 226 «О перечне федеральных мероприятий, направленных на обеспечение информационной безопасности детей, производство информационной продукции для детей и оборот информационной продукции, на 2022 – 2027 годы» // СПС «КонсультантПлюс».

<sup>410</sup> Приказ Минкомсвязи России от 29.08.2012 № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей» (Зарегистрировано в Минюсте России 16.10.2012 N 25682) // Российская газета. 24.10.2012. № 245.

контента: 1) Роскомнадзор (сфера СМИ и связи, в том числе сеть «Интернет»); 2) Роспотребнадзор (сфера защиты прав потребителей); 3) Рособрнадзор (сфера образования и науки). Отметим, что в рамках нашего диссертационного исследования интерес представляет конкретно первое направление, осуществляемое Роскомнадзором.

Иными словами, ввиду отсутствия сформированной в Законе № 436-ФЗ системы органов власти в сфере защиты несовершеннолетних от деструктивного контента обозначим эту систему путем анализа подзаконных правовых актов, принятых в соответствии с Законом № 436-ФЗ. При анализе плана мероприятий, направленных на обеспечение информационной безопасности несовершеннолетних, утвержденного приказом Минцифры России<sup>411</sup>, можно сделать вывод, что в пределах своей компетенции полномочиями в сфере защиты несовершеннолетних от деструктивного контента, в систему органов власти, направленную на обеспечение информационной безопасности несовершеннолетних в сети «Интернет», может быть включен любой федеральный орган исполнительной власти. Так, согласно положениям Приказа Минцифры России от 01.12.2020 № 644, осуществляют функции по мониторингу законодательства РФ в исследуемой нами сфере отношений: рабочая группа «Безопасное информационное пространство для детей» при Координационном совете при Правительстве РФ, Минцифры России, МВД России, Министерство просвещения РФ (Минпросвещения), Министерство здравоохранения РФ (Минздрав), Роскомнадзор, Федеральное агентство по делам молодежи (Росмолодежь), Роспотребнадзор, Рособрнадзор, Автономная некоммерческая организация «Центр изучения и сетевого мониторинга молодежной среды» (эта организация будет рассмотрена в параграфе 2.3 данного диссертационного исследования), органы исполнительной власти субъектов РФ. При этом считаем правовым пробелом, что в вышеуказанном Приказе Минцифры РФ № 644 не указаны Уполномоченный по правам ребенка и органы прокуратуры РФ, хотя, на

---

<sup>411</sup> Приказ Минцифры России от 01.12.2020 № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021 – 2027 годы»// Вестник образования России. 2021. № 1 (январь).

наш взгляд, эти органы власти могут реализовывать свои полномочия в сфере обеспечения информационной безопасности несовершеннолетних.

Мониторинг в сети «Интернет» для выявления на публичных и закрытых ресурсах незаконного или деструктивного контента для несовершеннолетних (в целях снижения числа несовершеннолетних, оказавшихся под влиянием деструктивного контента) осуществляют: Роскомнадзор, МВД России, Росмолодежь, Автономная некоммерческая организация «Центр изучения и сетевого мониторинга молодежной среды».

Полномочия органов публичной власти, образующих систему обеспечения информационной безопасности несовершеннолетних от деструктивного контента, рассмотрим по принципу от частного к общему, то есть системообразующие органы будут более детально рассмотрены после краткой правовой характеристики органов, менее участвующих в этой сфере правоотношений.

Так, в соответствии с Постановлением Правительства РФ от 02.06.2008 № 418 Минцифры России является федеральным органом исполнительной власти, осуществляющим в том числе функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию<sup>412</sup>.

Важная задача у Минпросвещения России, направленная на снижение числа несовершеннолетних, оказавшихся под влиянием деструктивного контента посредством рекомендации в сети «Интернет» образовательного контента с помощью информационно-образовательной среды «Российская электронная школа»<sup>413</sup>. Как справедливо отмечено в коллективной монографии, «одной из важнейших задач системы образования является формирование у обучающихся умений и навыков работы с информацией, следовательно, и умений обеспечения

<sup>412</sup> Постановление Правительства РФ от 02.06.2008 № 418 (ред. от 27.03.2025) «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» // СЗ РФ. 2008. № 23. Ст. 2708; СЗ РФ. 2025. № 13. Ст. 1485.

<sup>413</sup> Официальный сайт «Государственная образовательная платформа «Российская электронная школа»». URL: <https://resh.edu.ru/> (дата обращения: 01.05.2025).

безопасности в ходе работы с цифровым пространством»<sup>414</sup>. Следует сказать, что из п. 15 ч. 3 ст. 28 Федерального закона № 273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации»<sup>415</sup> можно сделать вывод, что согласно необходимости «создания необходимых условий для охраны и укрепления здоровья» обучающихся, к компетенции образовательных организаций отнесен и вопрос информационной безопасности несовершеннолетних, которая непосредственно влияет на жизнь, здоровье и развитие несовершеннолетних. Например, образовательные организации проводят уроки и внеклассные программы, направленные на формирование у обучающихся навыков цифровой культуры, защиты своих персональных данных в сети «Интернет» и т. д.

Министерство культуры РФ осуществляет контроль, в соответствии с постановлением Правительства РФ от 20 июля 2011 г. № 590 «О Министерстве культуры Российской Федерации»<sup>416</sup>, за соблюдением требований законодательства РФ в сфере защиты несовершеннолетних от влияния деструктивного контента. Кроме того, Министерство культуры РФ является федеральным органом исполнительной власти, который осуществляет функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере культуры, искусства, культурного наследия, архивного дела.

Рособрнадзор, в соответствии с Постановлением Правительства РФ от 28.07.2018 № 885<sup>417</sup>, осуществляет государственный контроль (надзор) за соблюдением организациями, осуществляющими образовательную деятельность, требований законодательства РФ в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, за используемой в образовательном процессе информационной продукцией. В случае выявления

<sup>414</sup> Правовое регулирование защиты несовершеннолетних от деструктивной информационной среды : монография / Под общ. ред. С. Е. Титор. М. : РУСАИНС, 2025. С. 59.

<sup>415</sup> Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 28.02.2025) «Об образовании в Российской Федерации» // Российская газета. 31.12.2012. № 303; Российская газета. 05.03.2025. № 47.

<sup>416</sup> Постановление Правительства РФ от 20.07.2011 № 590 (ред. от 27.02.2025) «О Министерстве культуры Российской Федерации» (вместе с «Положением о Министерстве культуры Российской Федерации») // СЗ РФ. 2011. № 31. Ст. 4758; СЗ РФ. 2025. № 9. Ст. 964.

<sup>417</sup> Постановление Правительства РФ от 28.07.2018 № 885 (ред. от 07.03.2025) «Об утверждении Положения о Федеральной службе по надзору в сфере образования и науки и признании утратившими силу некоторых актов Правительства Российской Федерации» (с изм. и доп., вступ. в силу с 01.04.2025) // СЗ РФ. 2018. № 32 (Часть II). Ст. 5344; СЗ РФ. 2025. № 10. Ст. 1088.

нарушений принимает меры по их устранению, в том числе путем выдачи предписаний об устранении выявленных нарушений, а также осуществляет контроль за их исполнением.

Согласно нормам ст. 6 Федерального закона от 27.12.2018 № 501-ФЗ<sup>418</sup> Уполномоченный по правам ребенка в сфере защиты несовершеннолетних детей от информации, причиняющей вред их здоровью и (или) развитию, имеет следующий объем полномочий: 1) внесение предложений по совершенствованию государственной информационной политики, принятию, изменению или приостановлению нормативных актов; 2) рекомендации органам власти по устранению нарушений в исследуемой сфере и привлечению виновных к ответственности; 3) Уполномоченный по правам ребенка вправе обратиться в суд с административными исковыми заявлениями о признании незаконными решений, деяний органов государственной власти, органов местного самоуправления, иных органов, организаций. Как отмечают А. К. Полянина и В. А. Чистяков, «особенности полномочий и задач Уполномоченного по правам ребенка обуславливают его специфику как субъекта управления, заключающуюся в сочетании признаков формального и неформального контроля»<sup>419</sup>. И, по мнению О. Н. Булакова, именно Уполномоченный по правам ребенка является необходимым звеном во взаимодействии органов публичной власти и непосредственно общества, которое необходимо для повышения информационной защищенности несовершеннолетних<sup>420</sup>. Впрочем, достаточно интересен тот факт, что в тексте Федерального закона от 27.12.2018 № 501-ФЗ<sup>421</sup> нет ни одного упоминания «информационной безопасности» и сети «Интернет», что указывает на опережение развитием новых форм общественных отношений (а именно общественных

<sup>418</sup> Федеральный закон от 27.12.2018 № 501-ФЗ (ред. от 10.07.2023) «Об уполномоченных по правам ребенка в Российской Федерации» // СЗ РФ. 2018. № 53 (часть I). Ст. 8427; СЗ РФ. 2023. № 29. Ст. 5304.

<sup>419</sup> Полянина А. К., Чистяков В. А. Государственное управление и институт детского омбудсмена в сфере обеспечения информационной безопасности личности // Общество: политика, экономика, право. 2024. № 6 (131). С. 47-54.

<sup>420</sup> Булаков О. Н. Взаимодействие уполномоченного при президенте Российской Федерации по правам ребенка с институтами гражданского общества по вопросам защиты прав и законных интересов несовершеннолетних // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2021. № 1 (57). С. 47-53.

<sup>421</sup> Федеральный закон от 27.12.2018 № 501-ФЗ (ред. от 10.07.2023) «Об уполномоченных по правам ребенка в Российской Федерации» // СЗ РФ. 2018. № 53 (часть I). Ст. 8427; СЗ РФ. 2023. № 29. Ст. 5304.

отношений с участием несовершеннолетних в сети «Интернет») их правового регулирования.

МВД России проводит профилактические акции, размещение в сети «Интернет» мультимедийных и информационных материалов, направленных на предупреждение незаконного оборота и потребления наркотиков среди несовершеннолетних. МВД России и его структурные подразделения наравне являются постоянными участниками рабочих групп, целью деятельности которых выступают выработка и реализация безотлагательных мер, направленных на совершенствование механизма выявления, предупреждения и пресечения преступлений, связанных с деятельностью лиц, склоняющих несовершеннолетних к девиантному поведению посредством оказания психологического воздействия через «Интернет» и всевозможные социальные сети. В п. 4 ч. 1 ст. 12 Федерального закона «О полиции»<sup>422</sup> также указано о необходимости выявления и устранения причин и условий административных правонарушений; участия в профилактике безнадзорности и правонарушений несовершеннолетних; участия в пропаганде правовых знаний, в том числе в сфере информационной безопасности несовершеннолетних. Управление «К» МВД России, которое является подразделением по борьбе с преступлениями в сфере информационных технологий, занимается выявлением и устранением информационных угроз (деструктивного контента) в отношении несовершеннолетних.

На основе совокупности норм двух федеральных законов (№ 436-ФЗ от 29.12.2010 и № 120-ФЗ от 24.06.1999<sup>423</sup>) осуществляют свои полномочия по защите информационной безопасности несовершеннолетних комиссии по делам несовершеннолетних и защите их прав, которые в рамках своей деятельности обеспечивают защиту прав и законных интересов несовершеннолетних граждан; осуществление сбора, обобщения информации о несовершеннолетних, находящихся в социально опасном положении; участвуют в рассмотрении

<sup>422</sup> Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 28.12.2024) «О полиции» // СЗ РФ. 2011. № 7. Ст. 900; СЗ РФ. 2024. № 53 (Часть I). Ст. 8528.

<sup>423</sup> Федеральный закон от 24.06.1999 № 120-ФЗ (ред. от 01.04.2025) «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» // СЗ РФ. 1999. № 26. Ст. 3177; СЗ РФ. 2025. № 14. Ст. 1588.



административных дел, в которых фигурирует несовершеннолетний. Сотрудники полиции могут привлекать к ответственности лиц, вовлекающих несовершеннолетних в совершение противоправного деяния, а также информировать территориальный орган Роскомнадзора о выявлении страниц сайтов сети «Интернет», пропагандирующих суицид, а также противоправные действия, представляющие опасность для жизни и здоровья несовершеннолетнего<sup>424</sup>.

Согласно п. 1 ст. 17 Федерального закона «О прокуратуре Российской Федерации»<sup>425</sup>, а также в соответствии с п. 1.2 Приказа Генпрокуратуры России от 13.12.2021 № 744<sup>426</sup> предусмотрено проведение ежедневного мониторинга соблюдения прав и законных интересов несовершеннолетних, в том числе с использованием средств массовой информации и информационно-телекоммуникационных сетей, незамедлительное реагирование на все ставшие известными факты нарушения прав и законных интересов несовершеннолетних. Руководствуясь ч. 1 ст. 15.3 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»<sup>427</sup> генеральный прокурор РФ или его заместители в случае выявления сайта в сети «Интернет» с деструктивным контентом для несовершеннолетних вправе обратиться в Роскомнадзор с требованием об ограничении доступа к сайту. Отметим, что в ст. 20 Федерального закона № 436-ФЗ<sup>428</sup> нет упоминания прокуратуры как субъекта, который уполномочен осуществлять надзор за соблюдением законодательства РФ о защите детей от информации, причиняющей вред здоровью и (или) развитию несовершеннолетних. Федеральная служба по

<sup>424</sup> Динисламова А. З. Административно-правовой статус субъектов обеспечения информационно-психологической безопасности несовершеннолетних // Полиция и общество: проблемы и перспективы взаимодействия. 2023. № 5. С. 58-67.

<sup>425</sup> Федеральный закон от 17.01.1992 № 2202-1 (ред. от 03.02.2025) «О прокуратуре Российской Федерации» // СЗ РФ. 1995. № 47. Ст. 4472; СЗ РФ. 1995. № 47. Ст. 4472.

<sup>426</sup> Приказ Генпрокуратуры России от 13.12.2021 № 744 «Об организации прокурорского надзора за исполнением законодательства о несовершеннолетних, соблюдением их прав и законных интересов» // Законность. 2022. № 2; СПС «КонсультантПлюс».

<sup>427</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; СЗ РФ. 2024. № 48. Ст. 7218.

<sup>428</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)<sup>429</sup>, являясь ключевым органом в системе защиты детей от информации, способной принести вред жизни, здоровью и развитию несовершеннолетних, осуществляет масштабную работу по мониторингу информационного пространства и реагированию на выявленные нарушения. За последние годы значительно усовершенствованы технические средства выявления противоправного контента, налажено взаимодействие с операторами поисковых систем и хостинг-провайдерами. Особое внимание уделяется превентивным мерам, направленным на предотвращение распространения запрещенной информации<sup>430</sup>.

Структура Роскомнадзора определена согласно ч. 1 Приказа Роскомнадзора от 25.03.2022 № 53<sup>431</sup>, в нее входят восемь управлений (осуществляющих, к примеру, контроль и разрешительную работу в сфере СМИ, связи, электронных коммуникаций, защите прав субъектов персональных данных) и отдел по защите государственной тайны. В рамках темы нашего исследования представляют интерес полномочия Управления контроля и надзора в сфере электронных коммуникаций<sup>432</sup> и частично Управления по защите прав субъектов персональных данных<sup>433</sup>, которые направлены на обеспечение российского законодательства о персональных данных граждан<sup>434</sup> в целом, без учета возрастного критерия. Таким образом, структура Роскомнадзора не содержит подразделения (отдела, Управления), специализирующегося на обеспечении информационной безопасности несовершеннолетних. Роскомнадзор ведет реестр сетевых адресов

<sup>429</sup> Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 27.03.2025) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций») // СЗ РФ. 2009. № 12. Ст. 1431; СЗ РФ. 2025. № 13. Ст. 1482.

<sup>430</sup> Бегларян С. Д. К вопросу о правовом регулировании обеспечения безопасности детей в информационной среде // Актуальные проблемы права, экономики и управления : сб. материалов студенческой научной конф., посв. памяти заслуженного деятеля науки РФ, учёного-правоведа, д-ра юрид. наук, проф. М. Н. Марченко. М., 2022. С. 357-361.

<sup>431</sup> Приказ Роскомнадзора от 25.03.2022 № 53 «Об утверждении структуры и штатного расписания Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СПС «КонсультантПлюс».

<sup>432</sup> Положение об Управлении контроля и надзора в сфере электронных коммуникаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: <https://rkn.gov.ru/about/structure/> (дата обращения: 01.05.2025).

<sup>433</sup> Положение об Управлении по защите прав субъектов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: <https://rkn.gov.ru/about/structure/> (дата обращения: 01.05.2025).

<sup>434</sup> Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3451; СЗ РФ. 2024. № 33 (Часть I). Ст. 4929.

(доменных имен) сайтов, на которых размещен законодательно запрещенный контент (ч. 1, 2 ст. 15.1 Закона об информации № 436-ФЗ). Механизм блокировки Роскомнадзором сайтов в сети «Интернет» при выявлении противоправного контента детально регламентирован законодательством: в российском законе (в ч. 6 ст. 10 Закона № 436-ФЗ<sup>435</sup>) перечислены виды информации, которые запрещены к распространению в сети «Интернет»; в п. 1 ч. 5 ст. 15.1 Закона об информации № 436-ФЗ приведен подробный перечень запрещенной к распространению информации, при выявлении которой в сети «Интернет» уполномоченные органы публичной власти вправе обращаться для включения страниц сайтов в соответствующий Единый реестр, основанием для включения в который (то есть основанием для блокировки сайта) согласно ч. 5 ст. 15.1 Закона № 436-ФЗ и п. 5 Правилам, утвержденным Постановлением Правительства РФ от 26.10.2012 № 1101 (далее – «Правил об АИС «Единый реестр доменных имен»))<sup>436</sup>, являются:

1) решения уполномоченных органов в отношении распространяемых посредством сети «Интернет» материалов и информации, указанных в п. 1 ч. 5 ст. 15.1 Закона об информации № 436-ФЗ (например, порнографический и иной деструктивный контент). Органы, которые принимают такие решения, перечислены в пп. «а» п. 5 Правил об АИС «Единый реестр доменных имен, в том числе там перечислены МВД России, Роскомнадзор, Росздравнадзор, Росмолодежь. Виды информации, в отношении которых каждый из этих органов уполномочен принимать решение, также перечислены в пп. «а» п. 5 названных Правил. Также отметим, что причиной для принятия решения уполномоченным органом может стать обращение (через специальную форму на сайте Роскомнадзора<sup>437</sup>) органов публичной власти, общественных объединений, граждан. Обращение рассматривают уполномоченные органы и информацию о своем решении в

<sup>435</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>436</sup> Постановление Правительства РФ от 26.10.2012 № 1101 (ред. от 21.02.2025) «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-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // СЗ РФ. 2012. № 44. Ст. 6044.

<sup>437</sup> Форма для приёма обращений о наличии на сайтах в сети «Интернет» запрещённой информации. URL: <https://cais.rkn.gov.ru/feedback/> (дата обращения: 01.05.2025).

электронном виде направляют в Роскомнадзор и (или) оператору реестра в течение суток с учетом необходимости защиты сведений о защищаемом лице (п. 6–8 Правил об АИС «Единый реестр доменных имен»);

2) постановление судебного пристава-исполнителя об ограничении доступа в сети «Интернет» к информации, порочащей честь и достоинство гражданина, деловую репутацию лица (физического или юридического);

3) решение суда о признании распространяемой в сети «Интернет» информации незаконной (запрещенной). Уточним, что дела о признании информации запрещенной к распространению в сети «Интернет» рассматриваются в порядке гл. 27.1 КАС РФ<sup>438</sup>.

Обратиться в суд в этом случае могут прокурор, лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа (или иным неправомерным использованием такой информации) (ч. 1 ст. 265.1 КАС РФ, ч. 2 ст. 17 Закона об информации № 436-ФЗ).

Для обращения в суд потребуется подготовить административное исковое заявление (ч. 1 ст. 265.1 КАС РФ). Требования к нему приведены в ст. 265.2 КАС РФ. В нем следует указать обязательные сведения и приложить к нему необходимые документы, которые могут быть направлены в суд в электронной форме (ч. 3 ст. 265.2 КАС РФ). Заявление подается в районный суд по адресу административного истца либо по адресу или месту жительства административного ответчика (ч. 2 ст. 265.1 КАС РФ).

Особенности подготовки к судебному разбирательству по таким делам установлены в ст. 265.3 КАС РФ, а именно в этих случаях: в качестве заинтересованного лица всегда привлекается Роскомнадзор (ч. 2); возможно на основании ч. 4 ст. 265.3 КАС РФ применение мер предварительной защиты (ограничение (блокирование) доступа к запрещенному контенту); в резолютивной части решения обязательно указываются доменные имена и (или) указатели страниц сайтов, содержащих запрещенную информацию (ч. 2).

---

<sup>438</sup> Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ (ред. от 01.04.2025) // СЗ РФ. 2015. № 10. Ст. 1391; СЗ РФ. 2025. № 14. Ст. 1587.

После принятия решения его копия направляется в Роскомнадзор, иным лицам, участвующим в деле. В случае принятия решения о признании информации запрещенной оно подлежит немедленному исполнению (ч. 3, 4 ст. 265.5 КАС РФ). По общему правилу в процедуре блокировки задействованы Роскомнадзор или оператор реестра, связи, хостинг-провайдеры и владельцы сайтов. Возможен общий порядок блокировки сайта или же с особенностями, в случаях, предусмотренных (ст. 15.1-1 – 15.6-1 Закона об информации № 436-ФЗ). Ограничение (блокирование) доступа осуществляется в следующем общем порядке: 1) внесение оператором записи в реестр на основании полученной информации от уполномоченных органов, постановления судебного пристава-исполнителя или решения суда; Роскомнадзор и (или) оператор реестра вносят запись в реестр в течение суток со дня получения (п. 9 Правил об АИС «Единый реестр доменных имен»); 2) с момента получения уведомления провайдер хостинга, руководствуясь ч. 7 ст. 15.1 Закона об информации № 436-ФЗ, незамедлительно сообщает владельцу сайта о полученном уведомлении и о необходимости удаления запрещенной информации; 3) либо владелец сайта незамедлительно удаляет запрещенную информацию (интернет-страницу с запрещенной информацией), либо же в случае его бездействия или выражения отказа провайдер сайта обязан заблокировать доступ к сайту (ч. 8 ст. 15.1 Закона об информации № 436-ФЗ). По истечении суток с момента уведомления провайдера Роскомнадзор и (или) оператор реестра проверяет исполнение уведомления – то есть наличие или отсутствие на сайте запрещенной информации. В случае исполнения требования владельцем сайта и отсутствия на сайте запрещенной информации ввиду ее удаления, из реестра удаляются сведения с указанием причины, даты и времени исключения сведений (п. 12 Правил об АИС «Единый реестр доменных имен»). Если владельцем сайта и (или) провайдером хостинга проигнорированы требования об удалении запрещенной информации, то данный сайт (а точнее сетевой адрес сайта) вносится в реестр, вследствие чего в течение суток на основании ч. 9, 10 ст. 15.1 Закона об информации № 436-ФЗ оператор связи блокирует доступ к данному сайту. Исключением из общего порядка блокировки сайта является случай, когда субъектом выступает сетевое издание, при

этом законодательно установлены следующие особенности (ч. 11 ст. 15.1 Закона об информации): 1) срок принятия мер владельцем сайта (провайдера хостинга, оператора связи) составляет три дня с момента обращения; 2) при судебной отмене решения Роскомнадзора о включении в реестр, то есть в течение одних суток со дня его получения (пп. «а» п. 14 Правила об АИС «Единый реестр доменных имен»).

Достаточно важным является тот факт, что именно Роскомнадзор осуществляет контроль за возрастной маркировкой сайтов в сети «Интернет», отслеживает ее наличие и наказывает за отсутствие или неправильную маркировку. Напомним, что классификация информационной продукции согласно ст. 6 закона № 436-ФЗ<sup>439</sup> как оценка информации на предмет отнесения ее к определенной возрастной категории («0+», «6+», «12+», «16+», запрещенная для детей – то есть «18+») нами уже рассматривалась в параграфе 1.1 данного исследования. С учетом классификации информационной продукции проводится маркировка сайтов в сети «Интернет» по возрастному критерию. Однако если следовать терминологии закона № 436-ФЗ, правильнее сказать не «маркировка», а размещение «знака информационной продукции». И в этом случае возникают два взаимосвязанных вопроса: подлежат ли все сайты в сети «Интернет» размещению на них «знака информационной продукции» и как соотносятся требования размещения «знака информационной продукции» по Закону № 436-ФЗ и требования Закона о рекламе № 38-ФЗ<sup>440</sup>.

Так, на основании ч. 2 ст. 14 Закона № 436-ФЗ обязательной возрастной классификации подлежит только сайт, зарегистрированный в качестве СМИ. В случае, когда владелец сайта в добровольном порядке размещает знак информационной продукции (возрастной категоризации), данное лицо может либо выполнить это самостоятельно, либо имеет право обратиться к эксперту или организации, которые аккредитованы Роскомнадзором. Ответ на второй вопрос

<sup>439</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>440</sup> Федеральный закон от 13.03.2006 № 38-ФЗ (ред. от 26.12.2024) «О рекламе» // СЗ РФ. 2006. № 12. Ст. 1232; СЗ РФ. 2024. № 53 (Часть I). Ст. 8489.

раскрывается в правоприменительной и судебной<sup>441</sup> практике. Так, Приказ ФАС России от 28.12.2023 № 1079/23<sup>442</sup> устанавливает, что сайт в сети «Интернет» может рассматриваться как информационная продукция исключительно если такой сайт зарегистрирован в качестве сетевого издания. Необходимость возрастной категоризации информационной продукции предусмотрена ч. 1 ст. 12 закона № 436-ФЗ. Так, при системном анализе норм ст. 6, ч. 1 ст. 12 закона № 436-ФЗ и 10.1 ст. 5 Закона № 38-ФЗ можно сказать, что в случае распространения рекламы, объектом рекламирования в которой является сайт, зарегистрированный как СМИ, реклама подлежит маркировке. Однако если указание в рекламе на сайт в сети «Интернет» размещено с целью ознакомления потребителей рекламы с дополнительной информацией и такой сайт не выступает самостоятельным объектом рекламирования, то не требуется указание маркировки согласно ч. 10.1 ст. 5 Закона о рекламе № 38-ФЗ. Также следует учитывать, что, несомненно, деструктивный контент, указанный в ч. 2 ст. 5 Закона № 38-ФЗ<sup>443</sup>, запрещен для несовершеннолетних и отмечен как «18+». Следовательно, норма ч. 10.1 ст. 5 Закона о рекламе № 38-ФЗ о необходимости возрастной категоризации может быть применена только в отношении рекламы информационной продукции.

Также следует отметить, что ст. 14 Закона № 436-ФЗ<sup>444</sup> предусматривает возможность проведения экспертиз информационной продукции в целях определения наличия или отсутствия у нее признаков деструктивного влияния на несовершеннолетних. Как правило, проводятся психологические, санитарные, педагогические, социальные экспертизы. Порядок проведения подобных экспертиз регламентируется совокупностью правовых актов<sup>445</sup>, которые содержат перечень

<sup>441</sup> Например: Постановление Арбитражного суда Центрального округа от 25.04.2025 № Ф10-77/2025 по делу N A09-8618/2023 // СПС «КонсультантПлюс»; Постановление Арбитражного суда Дальневосточного округа от 26.02.2024 № Ф03-6598/2023 по делу № А51-3988/2023 // СПС «КонсультантПлюс»; Постановление Арбитражного суда Московского округа от 03.02.2022 N Ф05-34646/2021 по делу № А40-1845/2021 // СПС «КонсультантПлюс».

<sup>442</sup> Приказ ФАС России от 28.12.2023 № 1079/23 «Об утверждении руководств по соблюдению обязательных требований в сфере рекламы» // СПС «КонсультантПлюс».

<sup>443</sup> Федеральный закон от 13.03.2006 № 38-ФЗ (ред. от 26.12.2024) «О рекламе» // СЗ РФ. 2006. № 12. Ст. 1232; СЗ РФ. 2024. № 53 (Часть I). Ст. 8489.

<sup>444</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>445</sup> Приказ Минкомсвязи России от 29.08.2012 № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей» // Российская газета. 24.10.2012. № 245; Приказ Роскомнадзора от 05.10.2021 № 208 «Об установлении Требований к экспертам и

требований к экспертам. Отметим, что достаточно стандартных требований – образование, отсутствие конфликта интересов с заинтересованными лицами и судимости за преступления против личности, стаж по специальности не менее пяти лет общего и непрерывного по специальности не менее трех лет перед аккредитацией как эксперта и т. д.

Приказ Роскомнадзора от 05.10.2021 № 208 устанавливает профессиональные (только при условии нахождения в штате организации не менее трех экспертов) и экономические требования к экспертным организациям по информационной продукции. Проведение экспертизы осуществляется на договорной возмездной основе. Обратиться к эксперту могут органы публичной власти, общественные объединения, юридические или физические лица. В процессе проведения экспертизы оценивается информационная продукция, размещаемая в том числе в сети «Интернет», на наличие или отсутствие признаков деструктивного контента для несовершеннолетних; соответствие возрастной категории и знака информационной продукции. Роскомнадзором также привлекаются аккредитованные эксперты, однако к ним предъявляются дополнительные требования на основании приказа Роскомнадзора от 21.06.2016 № 174<sup>446</sup>: например, общий стаж должен быть не менее 10 лет (а не 5, как по стандартным требованиям к экспертам), также эксперт обладать должен определенными профессиональными знаниями и навыками (например, знаниями законодательства и современных научных подходов в исследуемой сфере и т. д.). Согласно положениям приказа Роскомнадзора от 14.10.2016 № 268<sup>447</sup> эксперты,

---

экспертным организациям, осуществляющим проведение экспертизы информационной продукции» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 14.01.2022; Приказ Роскомнадзора от 09.07.2024 № 125 «Об утверждении Порядка аккредитации экспертов и экспертных организаций на право проведения экспертизы информационной продукции» (Зарегистрировано в Минюсте России 06.09.2024 № 79408) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 09.09.2024.

<sup>446</sup> Приказ Роскомнадзора от 21.06.2016 № 174 «Об утверждении Критериев аттестации экспертов, привлекаемых Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций к проведению мероприятий по контролю» (Зарегистрировано в Минюсте России 24.08.2016 № 43381) // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>, 25.08.2016.

<sup>447</sup> Приказ Роскомнадзора от 14.10.2016 № 268 «Об утверждении Правил формирования и ведения реестра аттестованных экспертов, привлекаемых Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций к проведению мероприятий по контролю» // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>, 13.01.2017.



которые аттестованы для привлечения к проведениям экспертиз по инициативе Роскомнадзора, вносятся в соответствующий реестр.

Согласно нормам, указанным Минкомсвязи России в письме от 14.08.2012 № 52-165/ВА<sup>448</sup> и приказе от 29.08.2012 № 217<sup>449</sup>, если в СМИ, в том числе в сети «Интернета», заинтересованным лицом выявлена информационная продукция, которая может не соответствовать указанному производителем возрастному знаку, то это заинтересованное лицо обращается к заявлением о проведении экспертизы информационной продукции к эксперту (или экспертной организации), аккредитованным Роскомнадзором. Экспертиза осуществляется в срок до 30 дней с момента заключения договора о ее проведении и оплаты заинтересованным лицом (заказчиком).

В завершение изучения полномочий совокупности государственных органов в сфере обеспечения информационной безопасности несовершеннолетних можно сказать следующее. В России отсутствует специализированная структура власти, которая была бы направлена на обеспечение информационной безопасности несовершеннолетних в сети «Интернет»; отсутствует специализированная система подачи жалоб на информацию (материалы), содержащие деструктивный контент и адресованные несовершеннолетним.

Ежегодно возрастающее количество правонарушений и преступлений в изучаемой сфере наглядно иллюстрирует необходимость модернизации структуры органов публичной власти, реализующих обеспечение информационной безопасности несовершеннолетних. На наш взгляд, сегодня необходимым является внесение изменений в Приказ Роскомнадзора от 25.03.2022 № 53<sup>450</sup> в части создания в структуре Роскомнадзора Управления по информационной

---

<sup>448</sup> Письмо Минкомсвязи России от 14.08.2012 № 52-165/ВА «О применении норм Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс».

<sup>449</sup> Приказ Минкомсвязи России от 29.08.2012 № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей» (Зарегистрировано в Минюсте России 16.10.2012 № 25682) // Российская газета. 24.10.2012. № 245.

<sup>450</sup> Приказ Роскомнадзора от 25.03.2022 № 53 «Об утверждении структуры и штатного расписания Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СПС «КонсультантПлюс».

безопасности несовершеннолетних, в полномочия которого будут входить предлагаемые нами задачи, которые представлены в Приложении Б.

Введение профильного Управления по информационной безопасности несовершеннолетних в структуре Роскомнадзора позволит, во-первых, улучшить обеспечение информационной безопасности несовершеннолетних в сети «Интернет»; во-вторых, снизить нагрузку с МВД, в особенности с Комиссии по делам несовершеннолетних и защите их прав, как минимум в части профилактики правонарушений с участием несовершеннолетних в сети «Интернет». Напомним, что по состоянию на 2025 год нехватка кадрового обеспечения в структуре МВД составляет от 18,9 % до 30 %<sup>451</sup>.

Следует сказать, что указанный расширенный перечень полномочий Управления по информационной безопасности несовершеннолетних Роскомнадзора, который мы предложили, исходит из следующего научно-правового предложения по совершенствованию российского законодательства в сфере информационной безопасности несовершеннолетних.

Во-первых, нами предложена и обоснована в главе 1 данного исследования необходимость законодательно зафиксировать предложенные нами определения «малолетний» и «подросток»<sup>452</sup>, поскольку законодательное использование термина «подросток» отражает динамичное правовое положение «несовершеннолетних». Подростковый возраст, в отличие от детей как категории «малолетние», характеризуется быстрыми физическими, когнитивными и социальными изменениями, в том числе половым и репродуктивным созреванием; постепенным формированием способности иметь права и обязанности, требующие новых знаний и навыков, нести правовую ответственность. Таким образом, если правовое положение малолетних базируется на максимальной защите их прав и интересов ввиду их физиологической и социально-психологической беспомощности (недееспособности), то подростки уже отличаются частичной

<sup>451</sup> В российской полиции остро не хватает сотрудников (22 января 2025). URL: <https://lenta.ru/articles/2025/01/22/police/> (дата обращения: 01.05.2025).

<sup>452</sup> В главе 1 нами было обозначено, что легализовать определение «подросток» и уточнить термин «ребенок» возможно в абз. 2 ст. 1 ФЗ от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»<sup>452</sup>.

дееспособностью и деликтоспособностью (в том числе ответственностью в административном праве, уголовной ответственностью в определенных законом случаях).

Однако в России отсутствует правовой механизм контроля (надзора) возрастного критерия при регистрации в социальных сетях несовершеннолетних граждан. Если обратиться к пользовательскому соглашению социальной сети ВКонтакте, то согласно п. 5.2 Правил пользования сайтом ВКонтакте<sup>453</sup> – регистрация на сайте доступна с 14 лет. Согласно п. 3.4 Пользовательского соглашения Экосистемы VK<sup>454</sup>, «Пользователем Экосистемы VK является физическое лицо, зарегистрированное в соответствии с установленным настоящим Соглашением порядком, достигшее возраста, допустимого в соответствии с законодательством Российской Федерации для акцепта настоящего Соглашения, и обладающее соответствующими полномочиями. Отдельные Сервисы могут устанавливать иные возрастные ограничения для их использования, о чем указывается в Пользовательской документации такого Сервиса». Отметим, что минимальный возраст, который можно выбрать в этой социальной сети при регистрации, составляет 14 лет (уточним, что можно выбрать, но не обязательно подтверждать). При этом, согласно п. 5.4 Правил пользования сайтом ВКонтакте, «пользователь несет ответственность за достоверность, актуальность, полноту и соответствие законодательству Российской Федерации предоставленной при регистрации информации и ее чистоту от претензий третьих лиц». Порядок регистрации установлен п. 5.5 рассматриваемых Правил, согласно которому после предоставления информации Пользователю необходимо пройти ряд удостоверяющих процедур, а именно:

- подтвердить регистрацию путем распознавания автоматизированного теста, предназначенного для различия компьютеров и людей («капчи»);
- подтвердить регистрацию путем введения в соответствующую форму на сайте кода, полученного пользователем в виде sms-сообщения от администрации

<sup>453</sup> Правила пользования сайтом ВКонтакте. URL: <https://vk.com/terms> (дата обращения: 01.05.2025).

<sup>454</sup> Пользовательское соглашение Экосистемы VK. URL: <https://id.vk.com/terms> (дата обращения: 01.05.2025).

сайта на мобильный телефон пользователя, номер которого предоставляется самим пользователем.

Таким образом, для регистрации в социальной сети ВКонтакте пользователю необходимо иметь номер телефона, который может быть зарегистрирован на любое лицо. Однако, как показывают результаты социальных опросов, личный телефон, который имеет функционал принимать sms-сообщения, у несовершеннолетних в среднем появляется в возрасте 6,6–8 лет (то есть, как правило, в возрасте начала обучения в общеобразовательной школе)<sup>455</sup>. Так как самостоятельно при наличии присутствия родителя или иного законного представителя приобрести sim-карту несовершеннолетний может с 14 лет, то логично предположить, что для первоклассника sim-карту оформляют его родители или иные законные представители на свое имя. Таким образом, непосредственно социальная сеть ВКонтакте, согласно системному анализу положений Правил пользования сайтом ВКонтакте, не проверяет и не несет ответственности за достоверность данных, указанных при регистрации, в том числе за сведения о возрасте лица, которое регистрируется. Более того, согласно п. 5.6 Правил пользования сайтом ВКонтакте при регистрации пользователь соглашается с настоящими Правилами и принимает на себя указанные в них права и обязанности, связанные с использованием и функционированием сайта. Пользователь соглашается на получение посредством сервисов администрации сайта и/или сервисов третьих лиц электронных сообщений, sms и иных видов рассылок информационного, в т. ч. рекламно-информационного содержания, в том числе от партнеров администрации сайта, а также согласно им пользователь несет личную ответственность за любую информацию, которую размещает на сайте, сообщает другим пользователям, а также за любые взаимодействия с другими пользователями, осуществляемые на свой риск (п. 6.4). Иными словами, социальная сеть, по сути, не обеспечивает информационную безопасность несовершеннолетнего.

---

<sup>455</sup> Россияне рассказали, в каком возрасте пора покупать ребенку телефон. URL: <https://www.kp.ru/daily/27581/4851382/> (дата обращения: 01.05.2025).

При этом, согласно Постановлению Правительства РФ от 28.12.2024 № 1963<sup>456</sup>, утверждены правила для персональной страницы в социальной сети, у которой аудитория более 10 тысяч пользователей, например, правила предоставления сведений в Роскомнадзор о данном пользователе, в том числе позволяющих его идентифицировать. Однако эти правила носят общий характер для всех возрастных категорий пользователей социальных сетей.

Следует также сказать, что понятие «социальные сети» (точнее – «социальные Интернет-сети») определено в ч. 12.1 ГОСТ Р 56824-2015<sup>457</sup> как информационные системы, обеспечивающие возможности: 1) организационные (формирование устойчивых социальных связей между лицами, подключившимися к системе в сети «Интернет» в форме групп и сообществ на основе этических и правовых норм в пределах ограничений, наложенных системой); 2) коммуникативные (возможность определять список других пользователей, с которыми они могут общаться в рамках трансграничного виртуального общения); 3) информационные (возможность обмениваться информацией).

Согласно ч. 12.2 ГОСТ Р 56824-2015 различают общие и профессиональные социальные сети. Обратим внимание, что в Постановлении Правительства РФ от 28.12.2024 № 1963 используется понятие «социальные сети»<sup>458</sup>, в ГОСТ Р 56824-2015 – «социальные Интернет-сети» и «социальные сети».

Таким образом, на наш взгляд, целесообразно учесть опыт зарубежных стран и предусмотреть обязанность социальных сетей не только в декларационном порядке регистрировать пользователей по достижении ими подросткового возраста, но и законодательно предусмотреть это требование и ответственность за его неисполнение. На основании вышесказанного считаем целесообразным дополнить Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующей статьей:

<sup>456</sup> Постановление Правительства РФ от 28.12.2024 № 1963 «Об отдельных вопросах распространения информации в социальных сетях» // СЗ РФ. 2025. № 1. Ст. 23.

<sup>457</sup> ГОСТ Р 56824-2015. Национальный стандарт Российской Федерации. Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет (утв. и введен в действие Приказом Росстандарта от 03.12.2015 N 2103-ст). М. : Стандартинформ, 2017.

<sup>458</sup> Постановление Правительства РФ от 28.12.2024 № 1963 «Об отдельных вопросах распространения информации в социальных сетях» // СЗ РФ. 2025. № 1. Ст. 23.

«Статья 10.8. Обязанности владельца социальных сетей в информационно-телекоммуникационной сети «Интернет», предлагаемый текст которой приведен в Приложении В. Приведем обоснование используемой терминологии. Понятие «владелец социальной сети» введено в декабре 2020 года<sup>459</sup> в п. 1 ст. 10.6 Закона об информации № 149-ФЗ<sup>460</sup> и обозначает владельца сайта и (или) страницы сайта в сети «Интернет», информационной системы, программы для ЭВМ, которые предназначены для размещения (распространения) информации на государственном языке РФ или народов РФ, и доступ к которым в течение суток составляет более 500 000 российских пользователей сети «Интернет».

В целом, понятие «владелец социальной сети» в российском праве является устоявшимся и применяется также в ст. 13.50 КоАП РФ<sup>461</sup> («Неисполнение обязанностей владельцем социальной сети»), в Постановлении Правительства РФ от 28.12.2024 № 1963 («2. Владелец социальной сети по запросу предоставляет следующие сведения:») и т. д. Дискуссионной, но на наш взгляд правильной, является формулировка «*принимает разумные меры*» в отношении действий, которые будут приняты социальными сетями, так как опыт Австралии, Великобритании, Германии показывает, что подобные онлайн-платформы находят технологические решения для соответствия социальных сетей требованиям законодательства.

Конструкция «*влечет за собой административную и иную ответственность в соответствии с законодательством Российской Федерации*» использована вместо «*юридической ответственности*» для единообразного подхода в тексте Федерального закона от 27.07.2006 № 149-ФЗ<sup>462</sup>, так как именно такая лексическая конструкция применяется законодателем: часть 16 статьи 10.2-2. «Особенности предоставления информации с применением рекомендательных технологий»; ч. 13

<sup>459</sup> Федеральный закон от 30.12.2020 № 530-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2021. № 1 (часть I). Ст. 69.

<sup>460</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; СЗ РФ. 2024. № 48. Ст. 7218

<sup>461</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404.

<sup>462</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; СЗ РФ. 2024. № 48. Ст. 7218.

ст. 10.4. «Особенности распространения информации новостным агрегатором»; ч. 17 ст. 10.5. «Обязанности владельца аудиовизуального сервиса»; ч. 15 ст. 10.7. «Обязанности владельца сервиса размещения объявлений».

В этом предложении нами выбран возрастной критерий в виде достижения подросткового возраста (14 лет) согласно следующему: 1) согласно представленному в параграфе 1.1 данной диссертационной работы обоснованию возрастной категории «подросток» и представленного авторского понятия этого термина; 2) с 14 лет в России несовершеннолетнее лицо: получает паспорт гражданина РФ; обладает дееспособностью несовершеннолетних в возрасте от 14 до 18 лет (статья 26 ГК РФ<sup>463</sup>); имеет право создавать учетную запись (иными словами, регистрироваться) на портале Госуслуг<sup>464</sup>; имеет возможность в присутствии родителей оформить sim-карту оператора сотовой связи на свое имя; в настоящее время с этого возраста осуществляется регистрация в отечественных социальных сетях (без подтверждения возраста). Таким образом, на наш взгляд, этот возрастной критерий является обоснованным.

Согласно п. 7 Федерального закона от 29.12.2022 № 572-ФЗ<sup>465</sup> идентификация представляет собой совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению этих сведений с идентификатором. Верификация подразумевает под собой проверку, подтверждение правильности. Аутентификация является составляющей верификации. Но если верификация в большей степени относится к контролю физического доступа, то аутентификация – к доступу в информационные системы. Нами предложено исключение – «случаев регистрации в государственных и (или) муниципальных образовательных социальных сетях, регистрация в которых

<sup>463</sup> Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024, с изм. от 31.10.2024) // СЗ РФ. 1994. № 32. Ст. 3301; СЗ РФ. 2024. № 33 (Часть I). Ст. 4933.

<sup>464</sup> Как подтвердить учётную запись ребёнку с 14 лет. URL: [https://www.gosuslugi.ru/help/faq/login\\_child/252144](https://www.gosuslugi.ru/help/faq/login_child/252144) (дата обращения: 01.05.2025).

<sup>465</sup> Федеральный закон от 29.12.2022 № 572-ФЗ (ред. от 26.12.2024) «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // СЗ РФ. 2023. № 1 (часть I). Ст. 19; СЗ РФ. 2024. № 53 (Часть I). Ст. 8504.

разрешена с 6,6 лет с согласия родителей (законных представителей) регистрируемого несовершеннолетнего лица», так как в России набирают популярность образовательные детские социальные сети, однако в настоящее время все они относятся к социальным сетям, учредителем которых являются физические или юридические лица, которые не проводят в должной мере контроль за контентом, не осуществляют проверку возраста пользователей.

Наиболее популярная в РФ сеть «Сферум» («учебный профиль Сферум в VK Мессенджере»<sup>466</sup>) позиционирует себя как закрытое сообщество, в которое можно вступить по ссылке-приглашению, и предназначено для несовершеннолетних, их родителей, учителей. Вход в «Сферум» возможен: 1) через VK ID с использованием данных из сервиса (то есть «ВКонтакте»); 2) через номер телефона или e-почты; 3) через профиль на портале ГосУслуги. Отметим, что при регистрации в «Сферум» предлагается Пользовательское соглашение Экосистемы VK<sup>467</sup>, согласно п. 3.4 которого: пользователем Экосистемы VK является физическое лицо, зарегистрированное и достигшее возраста, допустимого в соответствии с законодательством РФ для акцепта настоящего Соглашения, и обладающее соответствующими полномочиями». Таким образом, выявляется, что возраст для регистрации как в «детском» «Сферум», так и в самой социальной сети «ВКонтакте» согласно указанному соглашению одинаковый.

Федеральные органы власти – не единственные, кто отвечает за защиту детей от вредной информации. Субъекты РФ (регионы) тоже имеют такие полномочия. Это связано с тем, что вопросы защиты детей отнесены к совместному ведению Российской Федерации и ее субъектов: то есть и центр, и регионы участвуют в решении этих задач.

Органы государственной власти субъектов РФ организывают и реализуют в основном самостоятельно и за счет средств соответствующего бюджета национальные проекты в масштабах региона. Так, «Дорожные карты» профилактики деструктивного поведения и правонарушений несовершеннолетних

---

<sup>466</sup> Учебный профиль Сферум в VK Мессенджере. URL: <https://sferum.ru> (дата обращения: 01.05.2025).

<sup>467</sup> Пользовательское соглашение Экосистемы VK. URL: <https://id.vk.com/terms> (дата обращения: 01.05.2025).



принимают на уровне муниципальных образований и, как правило, они содержат перечень мероприятий, направленных на формирование и повышение цифровой грамотности; на профилактику правонарушений в сфере информационной безопасности и разъяснений по возможной ответственности в случаях, когда несовершеннолетний будет являться лицом, совершившим правонарушение в этой сфере правоотношений. На более локальном уровне, например, на уровне образовательных учреждений принимаются положения об использовании сети «Интернет» в образовательном учреждении, в которых для несовершеннолетних отражают памятки о правилах безопасного использования сети «Интернет»<sup>468</sup>. Л. В. Шварц читает, что «нет четкого регламента меры и степени задействованности как региона, так и Федерации в процессе решения общих задач, что влечет несогласованность действий сторон <...> в сфере защиты детей от информации, причиняющей вред их здоровью и развитию»<sup>469</sup>. Четкая регламентация и разграничение полномочий между федеральным и региональным уровнями государственной власти с указанием конкретного перечня совместных полномочий в сфере информационной безопасности несовершеннолетних в сети «Интернет» способствовали бы повышению эффективного административно-правового регулирования этой сферы отношений.

### **2.3. Частные лица в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в России и зарубежных государствах**

Значительный вклад в защиту несовершеннолетних от информационных угроз вносят общественные организации и объединения. Их деятельность включает мониторинг информационного пространства, выявление противоправного

<sup>468</sup> Например: «Положение об использовании сети Интернет в образовательном учреждении» Отдела образования Администрации Белокалитвинского района. URL: <https://sosh12.bkobr.ru/deyatelnost/informatsionnaya-bezopasnost/dokumenty-shkoly/2333-polozhenie-ob-ispolzovanii-seti-internet-v-obrazovatelnom-uchrezhdenii> (дата обращения: 01.05.2025); Положение об использовании сети «Интернет» в МБОУ «Столбовская СОШ». URL: [https://shkolastolbovskaya-r22.gosweb.gosuslugi.ru/netcat\\_files/30/69/polozhenie\\_ob\\_ispol\\_zovanii\\_seti\\_Internet\\_podpisano.pdf](https://shkolastolbovskaya-r22.gosweb.gosuslugi.ru/netcat_files/30/69/polozhenie_ob_ispol_zovanii_seti_Internet_podpisano.pdf) (дата обращения: 01.05.2025).

<sup>469</sup> Шварц Л. В. Проблемы нормативно-правового регулирования распределения полномочий Российской Федерации и ее субъектов в сфере обеспечения информационной безопасности детей // Вестник Санкт-Петербургской юридической академии. 2021. № 4 (53). С. 70-76.

контента, организацию просветительских мероприятий, оказание психологической помощи пострадавшим несовершеннолетним и их родителям. Особенно эффективной является работа специализированных организаций, занимающихся вопросами кибербезопасности и защиты прав несовершеннолетних в цифровой среде. Одной из современных тенденций развития механизмов публичного управления в условиях становления правового государства в России является привлечение организаций гражданского общества к содействию в осуществлении функций, возложенных на органы государственной власти<sup>470</sup>.

Статья 21 Закона № 436-ФЗ<sup>471</sup> закрепляет возможность общественного контроля общественными и (или) некоммерческими организациями, гражданами в сфере информационной безопасности несовершеннолетних. Следует уточнить, что, выделив два основных направления контроля (надзора) в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет» – государственное и общественное, российский законодатель совершенно упустил главное – механизм взаимодействия между ними, который в полном объеме реализован в зарубежных, прежде всего европейских, государствах. В существующей сегодня в РФ институциональной среде уполномоченные органы государства и общественные объединения формально действуют обособленно, что существенно осложняет достижение целей и теми, и другими.

Закон № 436-ФЗ о защите детей от деструктивной информации имеет ряд правовых проблем. Как указали в своих правовых изысканиях С. Л. Банщикова<sup>472</sup> и И. Ю. Гольяпина<sup>473</sup>, этот закон недостаточно полно регламентирует (по сути, декларирует) обязанности родителей (лиц, заменяющих родителей) по обеспечению информационной безопасности несовершеннолетних в сети

<sup>470</sup> Зеленцов А. Б., Гацолати В. Э. Административно-правовые аспекты взаимодействия правоохранительных органов и организаций гражданского общества // Вестник Сургутского государственного университета. 2020. № 3(29). С.78-87.

<sup>471</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>472</sup> Банщикова С. Л. Административная ответственность за неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по их содержанию и воспитанию : автореф. дис. ... канд. юрид. наук // Омский государственный университет им. Ф. М. Достоевского. Омск, 2017. 35 с.

<sup>473</sup> Банщикова С. Л., Гольяпина И. Ю. Обязанности родителей по обеспечению информационной безопасности несовершеннолетних детей и административная ответственность за неисполнение обязанности // Вестник Сибирского института бизнеса и информационных технологий. 2018. № 1 (25). С. 95-100.

«Интернет», отсутствует обязанность информационных платформ, распространяющих деструктивный контент для несовершеннолетних в сети «Интернет». Напомним, что в Пояснительной записке «К проекту Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» указано «добровольное исполнение закона»<sup>474</sup>.

В своей статье К. А. Шуликов справедливо отмечает, что только властных полномочий органов государственной власти недостаточно для защиты несовершеннолетних в сфере информационной безопасности в сети «Интернет»<sup>475</sup>. Следует согласиться и с позицией Н. А. Фроловой о том, что «эффективное решение этой задачи [обеспечения безопасности личности, общества и государства] вряд ли возможно без «встречного» движения, без осознания ценности безопасности каждым гражданином»<sup>476</sup>.

В настоящее время можно наблюдать тенденцию увеличения роли «иных субъектов, которые не наделены конкретными властными полномочиями, а лишь выступают в качестве исполнителей решений органов власти»<sup>477</sup>. Субъекты с властными полномочиями нами рассмотрены выше. Рассмотрим теперь невластные субъекты, осуществляющие общественный контроль в исследуемой сфере правоотношений: общественные и добровольческие (волонтерские) объединения, в том числе киберволонтеры<sup>478</sup>; провайдеры хостингов, операторы

<sup>474</sup> Пояснительная записки «К проекту Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс».

<sup>475</sup> Шуликов К. А. Субъекты противодействия распространению деструктивного контента в сети Интернет и административно-правовая характеристика их деятельности // Административное право и процесс. 2024. № 8. С. 69-73.

<sup>476</sup> Фролова Н. А., Фархутдинов И. З., Панченко В. Ю. Фролова Н. А. Диалектическое единство развития и безопасности – платформа будущего // Евразийский юридический журнал. 2018. № 5 (120). С. 13.

<sup>477</sup> Шуликов К. А. Административно-правовые основы противодействия распространению деструктивного контента в сети «Интернет»: дис. ... канд. юрид. наук. СПб., 2024. С. 111-112.

<sup>478</sup> Термин «киберволонтер» встречается в научно-правовых статьях: Венцель С. В. Особенности мониторинга противоправного контента в интернете в рамках киберволонтерской деятельности // Обзор. НЦПТИ. 2021. № 1 (24). С. 30-37; Маскальцова О. В. Формирование добровольных кибердружин как проявление гражданской инициативы противодействия распространения негативной и противоправной информации в сети «Интернет» // В сб.: Культура открытого города: волонтерство как ресурс городских проектов. Материалы Международной научно-практической конференции студентов, аспирантов и молодых ученых. Управление культуры Администрации города Екатеринбурга, Муниципальное бюджетное образовательное учреждение высшего образования «Екатеринбургская академия современного искусства» (институт). 2020. С. 23-27; Лаптев А. С. Роль негосударственных субъектов в осуществлении регионального криминологического планирования // Бизнес и общество. 2023. № 2 (38); Мазова В. Д. Административно-правовой статус кибердружин // Правопорядок в России: проблемы совершенствования. Сборник научных трудов XVIII Всероссийской научно-практической конференции. Москва, 2024. С. 135-137; Матюшенков Д. М. Деятельность кибердружин в сфере охраны общественного порядка // Современный юрист. 2021. № 1 (34). С. 34-42.

связи и доменных имен, то есть лица, которые осуществляют блокирование запрещенного контента; владельцы социальных сетей, организаторы распространения информации в сети «Интернет», которых государство наделило полномочиями по осуществлению мониторинга за размещением и распространением запрещенного контента в сети «Интернет». Так, владельцем сайта является администратор доменного имени, переадресующего на соответствующий сайт. Отметим, что некоторые авторы относят владельцев социальных сетей, организаторов распространения информации в сети «Интернет» к информационным посредниками<sup>479</sup>. Однако есть позиция ВС РФ<sup>480</sup>, согласно которой не каждый владелец социальной сети является информационным посредником, а только в случае, если такое лицо осуществляет деятельность согласно 1253.1 ГК РФ<sup>481</sup>. Возникновение информационных посредников обусловлено огромными объемами контента, который размещается на онлайн-платформах, поэтому появилась необходимость передачи государством полномочий по контролю (надзору) владельцам онлайн-платформ в целях оперативного и совместного с государственными органами обеспечения информационной безопасности в сети «Интернет» путем мониторинга, выявления и передачи сведений о вредоносной для несовершеннолетних информации в соответствующие органы.

Общественные и добровольческие (волонтерские) объединения имеют основной целью своей деятельности противодействие размещению и распространению в сети «Интернет» деструктивного контента для несовершеннолетних, повышение навыков цифровой грамотности у детей и подростков. Так, в 2018 году по поручению Президента РФ была создана ИТ-компания – автономная некоммерческая организация «Центр изучения и сетевого мониторинга молодежной среды» (АНО «ЦИСМ») для защиты

<sup>479</sup> Например: Чубукова С. Г. Проблемы правового статуса информационного посредника // Вестник Академии права и управления. 2017. № 2 (47). С. 39-44.

<sup>480</sup> Подробнее: Обзор судебной практики рассмотрения гражданских дел, связанных с нарушением авторских и смежных прав в информационно-телекоммуникационной сети «Интернет» (утв. Президиумом Верховного Суда РФ 29.05.2024) // СПС «КонсультантПлюс».

<sup>481</sup> Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 22.07.2024) // Российская газета. 22.12.2006. № 289; Российская газета. 29.07.2024. № 165.

подростающего поколения от воздействия деструктивного контента<sup>482</sup>. Однако более активным и известным российским участником общественных отношений в изучаемой сфере является некоммерческое партнерство «Лига безопасного Интернета».

«Лига безопасного Интернета» как институт гражданского общества была создана относительно поздно применительно к уровню развития сети «Интернет» в России и мире, в 2011 году, став результатом государственно-частного партнерства. В дело защиты несовершеннолетних в Интернете и обеспечения их сетевой безопасности были вовлечены МВД России, Минкомсвязи РФ и Комитет Государственной Думы РФ по вопросам семьи, женщин и детей<sup>483</sup>.

В настоящее время, согласно открытым сведениям ФНС<sup>484</sup>, форма организации этого юридического лица – ассоциация участников рынка интернет-индустрии «Лига безопасного интернета» (сокращенно – ассоциация «Лига безопасного Интернета»). В 2012–2024 гг. волонтеры Лиги провели в образовательных организациях разного уровня свыше 14 500 уроков «безопасного Интернета»; в деле противодействия распространению противоправного контента в Рунете «Лига безопасного Интернета» (далее – Лига) организовывала «горячие линии» по приему обращений, в основном о распространении детской порнографии и наркотиков. Лига отчиталась о своем содействии блокировке и (или) удалению по обращениям волонтеров в 2011–2024 гг. опасного контента с 152 103 ресурсов, а также о закрытии 23 680 страниц в сети «Интернет», на которых шло распространение наркотиков<sup>485</sup>. Лига участвовала в разработке Концепции информационной безопасности детей в РФ 2023 году<sup>486</sup>. Однако являясь не просто разработчиком, а заинтересованным институтом гражданского общества, Лига должна была бы контролировать реализацию положений Концепции информационной безопасности детей в РФ 2023 г., что на практике не происходит.

<sup>482</sup> Официальный сайт АНО «ЦИСМ». URL: <https://cism-ms.ru/poleznye-materialy> (дата обращения: 01.05.2025).

<sup>483</sup> Официальный сайт Лига безопасного Интернета. URL: <https://ligainternet.ru/o-nas/> (дата обращения: 01.05.2025).

<sup>484</sup> Официальный сайт ФНС. URL: <https://egrul.nalog.ru/index.html> (дата обращения: 01.05.2025).

<sup>485</sup> Слово директора. Лига безопасного интернета. URL: <https://ligainternet.ru/direktor/> (дата обращения: 01.05.2025).

<sup>486</sup> Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СЗ РФ. 2023. № 19. Ст. 348.

Анализ деятельности Лиги показывает ее ситуативный характер с признаками неопределенности и несистемности действий. Так, 5 декабря 2024 г. информационные агентства сообщили, что глава Лиги безопасного интернета Е. Мизулина «уточнила информацию» о блокировке порталов с аниме, которые содержали ЛГБТ-пропаганду<sup>487</sup>. Немногим ранее она же «планировала попросить Генеральную прокуратуру РФ проверить детскую литературу...»<sup>488</sup>. Тогда же глава Лиги в своем Telegram-канале (не обращаясь в правоохранительные органы в порядке ст. 140 УПК РФ<sup>489</sup>) опубликовала «сообщение со ссылкой на анонимное обращение» о появлении в Перми «банды педофилов»<sup>490</sup>. СК возбудил уголовное дело, однако сам подход главы Лиги, создание резонансного информационного повода на основе анонимных сообщений, представляется не вполне соответствующим задачам организации, если рассматривать их в сопоставлении с зарубежными аналогами и глобальными задачами по безопасности в интернет-пространстве. Проведенный в рамках настоящего исследования анализ деятельности Лиги выявил проблему неопределенности статуса организации, на официальном сайте которой отсутствует информация об учредителях, регистрации Лиги, нет устава или заменяющего его документа, нет формализованной миссии, что существенно затрудняет понимание официального статуса организации, а соответственно, ее полномочий и возможностей сотрудничества. В этом смысле Лига отличается от британского Internet Watch Foundation (IWF)<sup>491</sup>, который формулирует, декларирует и публикует свои официальные видение и миссию<sup>492</sup>. Исходя из того, что (по данным ИСИЭЗ НИУ ВШЭ) в Интернет с разной степенью регулярности выходят 99 % российских подростков 14–17 лет, а 97 % из них имеют

<sup>487</sup> Роскомнадзор подтвердил блокировку порталов с аниме-контентом // РИА Новости. 2024. 5 декабря. URL: <https://ria.ru/20241205/roskomnadzor-1987599452.html> (дата обращения: 01.05.2025).

<sup>488</sup> Мизулина попросит Генпрокуратуру проверить детские книги // РИА Новости. 2024. 14 ноября. URL: <https://ria.ru/20241114/kultura-1983783129.html> (дата обращения: 01.05.2025).

<sup>489</sup> Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 21.04.2025) // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921; СЗ РФ. 2025. № 17. Ст. 2130.

<sup>490</sup> Мизулина попросит Генпрокуратуру проверить детские книги // РИА Новости. 2024. 14 ноября. URL: <https://ria.ru/20241114/kultura-1983783129.html> (дата обращения: 01.05.2025).

<sup>491</sup> Официальный сайт Internet Watch Foundation. URL: <https://www.iwf.org.uk/> (дата обращения: 01.05.2025).

<sup>492</sup> IWF Our mission. URL: <https://www.iwf.org.uk/about-us/why-we-exist/our-vision-and-mission/> (дата обращения: 01.05.2025).

как минимум один аккаунт в социальных сетях<sup>493</sup>, это вопрос национальной безопасности. Лига не прикладывает достаточных усилий, не имеет концепции системного вхождения информационной грамотности и безопасности в сети «Интернет» в школьную программу для формирования уже в младших классах базы для более глубоких познаний и навыков, которые на следующей ступени дадут уже специалисты. Свой смартфон у российского ребенка появляется рано, у каждого третьего – еще до школы. В этой же возрастной категории каждый восьмой ребенок имеет планшет, а каждый двадцатый – ноутбук или «умные» часы<sup>494</sup>. К 12–14 годам смартфоны (не считая планшетов и ноутбуков) имеют уже 90 % детей, что формирует интернет-зависимость<sup>495</sup>, растущие риски, которые в семьях не нивелируются. В то же время дети и подростки в онлайн-среде общаются, учатся, ищут информацию и т. д. Следовательно, в процессе нахождения в сети «Интернет» дети и подростки взаимодействуют с разным контентом, в том числе деструктивным для них.

Лига активно ведет работу с родителями несовершеннолетних с целью повышения их цифровой грамотности. Опубликованы «10 главных советов родителям по безопасности детей в Интернете»<sup>496</sup>, а также основные положения так называемого «семейного соглашения об использовании цифровых устройств»<sup>497</sup>, типовой бланк которого прилагается на сайте организации<sup>498</sup>. Обратная связь в этом случае отсутствует, Лига не приводит данных о том, сколько российских родителей заключили со своими детьми такого рода письменное соглашение. В отличие от британской IWF российская Лига не формирует единую

<sup>493</sup> Дети в Интернете. ИСИЭЗ НИУ ВШЭ. URL: <https://issek.hse.ru/news/837320649.html?ysclid=m4schi9m1400480739> (дата обращения: 01.05.2025).

<sup>494</sup> Там же.

<sup>495</sup> Акимова А. Н., Афанасьева Л. И. Особенности интернет-зависимости подростков // Проблемы современного педагогического образования. 2024. № 84-1. С. 390-392; Dong H., Yang F., Lu X., Hao W. Internet Addiction and Related Psychological Factors Among Children and Adolescents in China During the Coronavirus Disease 2019 (COVID-19) Epidemic / Frontiers in Psychiatry. 2020. № 11.

<sup>496</sup> URL: <https://ligainternet.ru/10-sovetov-roditelyam-po-bezopasnosti-v-seti/?ysclid=m500syuezp674323284> (дата обращения: 01.05.2025).

<sup>497</sup> Смартфон и ребенок. Почему думающие родители составляют семейное соглашение об использовании цифровых устройств. URL: <https://ligainternet.ru/semejnoe-soglashenie-ob-ispolzovanii-gadzhetov/>.

<sup>498</sup> Семейное соглашение об использовании гаджетов. URL: <https://ligainternet.ru/wp-content/uploads/2022/09/semejnoe-soglashenie-ob-ispolzovanii-gadzhetov-web.pdf> (дата обращения: 01.05.2025).

базу опасных ресурсов<sup>499</sup> для их последующей блокировки провайдерами, не налаживает сотрудничество с мессенджерами (для контроля контента) и платформами (системами) электронного обучения для производства и размещения учебных материалов. В целом, анализ деятельности Лиги показал потребность в существенном ее совершенствовании. Необходимо:

- максимально прозрачно, с привлечением всех заинтересованных лиц выработать миссию и видение организации; разработать и принять научно обоснованную концепцию развития Лиги, в которой обосновать и закрепить переход от разовых мероприятий к системной работе для создания эффективных институтов превенции угроз и рисков для несовершеннолетних в Интернете;
- опубликовать уставные документы Лиги;
- добиваться от интернет-провайдеров, операторов сотовой связи и их организаций выраженной, активной и непримиримой позиции к любому проявлению насилия в сети «Интернет» в целом и в отношении несовершеннолетних в частности;
- наладить (насколько это возможно в текущей ситуации) сотрудничество с аналогичными организациями за рубежом.

В 2011 году Лига создала межрегиональное общественное молодежное движение «Кибердружина», основной целью которого является недопущение распространения в сети «Интернет» информации, которая имеет противоправный характер, в том числе причиняющей вред здоровью и развитию несовершеннолетних. Основной задачей «Кибердружины» является поиск сайтов, распространяющих запрещенные материалы, и уведомление Лиги о них.

В Приказе Минобрнауки РФ от 24.01.2024 № 35<sup>500</sup>, а именно в утвержденном «Аналитическом отчете по результатам осуществления мониторинга реализации молодежной политики в РФ...», обозначено такое направление деятельности, как

<sup>499</sup> Роскомнадзор РФ ведёт Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. РКН РФ. URL: <https://eais.rkn.gov.ru/> (дата обращения: 01.05.2025).

<sup>500</sup> Приказ Минобрнауки России от 24.01.2024 № 35 «Об утверждении форм аналитических отчетов по результатам осуществления мониторинга реализации молодежной политики в Российской Федерации» (Зарегистрировано в Минюсте России 26.02.2024 № 77345) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 29.04.2025).



«327 – информационная безопасность (кибердружины)»<sup>501</sup>. Киберволонтерство (онлайн-волонтерство, виртуальное волонтерство, медиаволонтерство) – разновидность волонтерской деятельности, которая осуществляется дистанционно с помощью интернет-технологий.

Рассмотрим примеры. В 2021 году в РФ создан «Альянс по защите детей в цифровой среде» для создания безопасной онлайн-среды для несовершеннолетних пользователей сети «Интернет»<sup>502</sup>. К основным его задачам относятся: решения для усиленной защиты от нежелательной информации; поиск и удаление противоправных материалов; повышение цифровой грамотности детей и родителей. Этот альянс представляет собой объединение девяти крупных технологических, цифровых и медиакомпаний России. Каждый участник подписал Хартию «Цифровая этика детства»<sup>503</sup> в целях создания защищенной и благоприятной цифровой среды для детей и обязуется прилагать максимум усилий для создания безопасной и благоприятной цифровой среды, делиться лучшими практиками и новейшими разработками. На сайте «Альянса по защите детей в цифровой среде» по аналогии с «Safer Internet Day»<sup>504</sup> (общеевропейской инициативой по продвижению безопасного интернета для всех пользователей, особенно для несовершеннолетних) сделаны разделы «Для преподавателей», «Для детей», «Для родителей». Отметим, что на официальном сайте отсутствует информация о правовом статусе, документах – основаниях деятельности и т. д.

«Киберпатруль»<sup>505</sup> – проект, направленный на решение проблем информационной безопасности несовершеннолетних с привлечением общественного ресурса (киберволонтеров), поиск потенциально опасного контента в сети «Интернет». Его основная цель – выявление незаконного контента в сети «Интернет», а также проведение профилактических мероприятий в школах, вузах и сузах. «Киберпатруль» активно функционирует в РФ, например, в Тюменской,

<sup>501</sup> Там же.

<sup>502</sup> Официальный сайт «Альянс по защите детей в цифровой среде». URL: <https://internetforkids.ru/> (дата обращения: 01.05.2025).

<sup>503</sup> Хартия «Цифровая этика детства». URL: <https://internetforkids.ru/upload/docs/charter.pdf> (дата обращения: 01.05.2025).

<sup>504</sup> Safer Internet Day. URL: <https://www.webwise.ie/saferinternetday/> (дата обращения: 01.05.2025).

<sup>505</sup> Киберпатруль. URL: <http://кибер-патруль.рф/> (дата обращения: 01.05.2025).

Курской областях, Забайкалье, Волгограде, Югорске и в Республике Коми уже получен положительный эффект от предупреждения преступлений при помощи инициативных граждан. Также создаются аналоги на платформе образовательных учреждений (например, «Киберпатруль МКОУ СОШ с. Голуметь», «КиберПатруль ГБПОУ Колледж полиции, Москва» и т. д.). Аналогично функционируют «Кибердружины»: «Кибердружина» Народного фронта<sup>506</sup>; «Кибердружина. Центр информационной безопасности и психологической помощи молодежи Ханты-Мансийского автономного округа – Югры»<sup>507</sup>. Онлайн-платформа цифровых консультаций и безопасности в сети «Интернет» «РосКибербезопасность»<sup>508</sup>, которая была создана для обеспечения безопасности в сети «Интернет» (отметим, что на официальном сайте отсутствует информация о правовом статусе, документах – основаниях деятельности и т. д.).

Интересен тот факт, что в 2018 году депутатами фракции «Единая Россия» был подготовлен проект закона о кибердружинах, который прошел обсуждения в Общественной палате и должен быть внесен в Государственную Думу<sup>509</sup>. Законопроект «О кибердружинах в Российской Федерации» разработан депутатами от партии «Единая Россия» в целях создания правовых условий для добровольного участия граждан в противодействии распространению противоправной информации в Интернете. Согласно документу, кибердружинники будут вместе с правоохранительными органами выявлять в Интернете информацию, нарушающую законодательство, в том числе экстремистского характера. Формироваться кибердружины будут по инициативе граждан РФ в формате общественной организации. О создании и деятельности кибердружины необходимо будет уведомить Роскомнадзор, после этого прокуратуры и правоохранительные органы должны будут сотрудничать с кибердружинниками. Вступать в

<sup>506</sup> Кибердружина. Народный Фронт. URL: <https://onf.ru/cyberguard> (дата обращения: 01.05.2025).

<sup>507</sup> Кибердружина. Центр информационной безопасности и психологической помощи молодежи Ханты-Мансийского автономного округа Югры. URL: <https://cybersquad.ru/> (дата обращения: 01.05.2025).

<sup>508</sup> Онлайн платформа цифровых консультаций и безопасности в сети «Интернет» «РосКибербезопасность». URL: <https://roskiber.ru/> (дата обращения: 01.05.2025).

<sup>509</sup> Сайт Государственной Думы РФ. Авторы проекта о кибердружинах выслушали мнение общественников и экспертов в рамках «нулевых чтений». URL: <http://duma.gov.ru/news/29944/> (дата обращения: 01.05.2025).

кибердружинники смогут лица старше 18 лет<sup>510</sup>. Несомненным минусом этого документа является отсутствие положений о необходимости обучения кибердружинников или требований об их образовании и (или) профессиональных навыках в информационной сфере. По мнению участников заседания, требуют внимания вопросы программно-технической и личной безопасности кибердружинников, поскольку, по их мнению, наверняка будут попытки добыть персональные данные кибердружинников, угрожать им. Вместе с тем заслуживает внимания вопрос, как правоохранители будут проверять желающих сотрудничать с ними волонтеров. Кроме того, прозвучали предложения повысить возраст для вступления в ряды кибердружинников: по мнению некоторых экспертов, 18 лет – недостаточный порог для такой работы. Вместе с тем эксперты подтвердили актуальность рассматриваемого вопроса и необходимость предложенной законодательной инициативы как ответа на те вызовы, с которыми сталкивается сегодня наше общество и государство. Они отметили, что деструктивный контент формируется не только внутри страны, но и идет извне. Законопроект по состоянию на ноябрь 2025 года не принят.

Можно выделить следующие наиболее встречаемые формы волонтерства в сети «Интернет»: 1) некоммерческие организации и общественные движения, которые помимо мониторинга в сети проводят общие встречи, участвуют в профилактических мероприятиях с различными целевыми аудиториями; 2) кибердружины и киберотряды, создающиеся на базе образовательных организаций (школ, техникумов, колледжей или университетов). Как отмечает О. В. Маскальцова, «добровольцы проходят специальное обучение, делятся опытом в рамках тематических массовых мероприятий, соревнуются в своем мастерстве»<sup>511</sup>. Отметим, что Закон № 135-ФЗ уравнивает понятия «добровольчество» и «волонтерство», так как в ст. 1 обозначено, что под этой деятельностью «понимается добровольная деятельность в форме безвозмездного

<sup>510</sup> В Госдуме разработали законопроект о «кибердружинах». URL: <https://otr-online.ru/news/v-gosdume-razrabotali-zakonoproekt-o-kiberdruzhinah-114027.html> (дата обращения: 01.05.2025).

<sup>511</sup> Маскальцова О. В. Формирование добровольных кибердружин как проявление гражданской инициативы противодействия распространения негативной и противоправной информации в сети «Интернет». С. 23.

выполнения работ и (или) оказания услуг в целях, указанных в пункте 1 статьи 2 настоящего Федерального закона»<sup>512</sup>. Часть 1 ст. 2. закона устанавливает закрытый перечень целей благотворительной и добровольческой (волонтерской) деятельности, в том числе: содействие деятельности в сфере образования, науки, культуры, искусства, просвещения, духовному развитию личности, волонтерства; содействие правоохранительным органам и деятельности в сфере профилактики здоровья граждан, а также по профилактике безнадзорности и правонарушений несовершеннолетних. На наш взгляд, с учетом значимости и значительного развития добровольчества (волонтерства) в сфере обеспечения информационной безопасности в сети «Интернет» следует дополнить ч. 1 ст. 2. Закона от 11.08.1995 № 135-ФЗ еще одной целью, а именно «содействием в обеспечении информационной безопасности граждан, в том числе несовершеннолетних в сети «Интернет»». Считаем, необходимо закрепить повышенный уровень гарантий для волонтеров, деятельность которых направлена на повышение уровня информационной безопасности, в том числе несовершеннолетних в сети «Интернет», а именно поиск (выявление) противоправных материалов, в том числе информации, несущей вред здоровью и развитию несовершеннолетних, передача сведений о деструктивном контенте в правоохранительные органы.

В России отмечается существенный рост волонтерского движения. Так, помимо «крупных» объединений, таких как АНО «Цисм», Ассоциация «Лига безопасного интернета»<sup>513</sup>, «Альянс по защите детей в цифровой среде»<sup>514</sup>, «Киберпатруль»<sup>515</sup>, «Кибердружина» Народного фронта<sup>516</sup>, онлайн-платформа цифровых консультаций и безопасности в сети «Интернет» «РосКибербезопасность», существуют их аналоги в субъектах РФ, муниципальных образованиях, образовательных учреждениях. Однако в действующем

<sup>512</sup> Федеральный закон от 11.08.1995 № 135-ФЗ (ред. от 28.12.2024) «О благотворительной деятельности и добровольчестве (волонтерстве)» // СЗ РФ. 1995. № 33. Ст. 3340; СЗ РФ. 2024. № 53 (Часть I). Ст. 8564.

<sup>513</sup> Официальный сайт Ассоциация «Лига безопасного интернета». URL: <https://ligainternet.ru/o-nas/> (дата обращения: 01.05.2025).

<sup>514</sup> Официальный сайт «Альянс по защите детей в цифровой среде». URL: <https://internetforkids.ru/> (дата обращения: 01.05.2025).

<sup>515</sup> Киберпатруль. URL: <http://кибер-патруль.рф/> (дата обращения: 01.05.2025).

<sup>516</sup> Кибердружина. Народный Фронт. URL: <https://onf.ru/cyberguard> (дата обращения: 01.05.2025).

Федеральном законе «О благотворительной деятельности и добровольчестве (волонтерстве)» от 11.08.1995 № 135-ФЗ<sup>517</sup> такой важный и нужный, особенно сейчас, вид добровольческой (волонтерской) деятельности не находит должного отражения. Участие в обеспечении информационной безопасности граждан, в том числе несовершеннолетних, в цифровой среде не отнесено к целям добровольческой (волонтерской) деятельности.

Еще раз обозначим, что нормы ст. 21 Закона № 436-ФЗ<sup>518</sup> распространяются и на граждан, осуществляющих общественный контроль в сфере информационной безопасности несовершеннолетних в сети «Интернет». Достаточно часто к этой категории относятся родители несовершеннолетних. Однако в России далеко не все взрослые осуществляют «цифровой контроль» («родительский контроль»). По данным НИУ ВШЭ 44 % родителей никак не ограничивают действия своих детей в Интернете<sup>519</sup>. Отсюда следует, что повышение информационной грамотности в сети «Интернет» детей и подростков должно начинаться с дошкольного возраста. Как отмечает Г. Н. Захаров, «общая проблема российского общества заключается в том, что практически никто не занимается компьютерной грамотностью ни взрослых, ни детей в широком масштабе»<sup>520</sup>.

Разработка информационной системы родительского контроля ресурсов сети «Интернет» имеет особое значение в современном мире, где доступ к Интернету неограничен и дети могут столкнуться с деструктивным контентом<sup>521</sup>.

<sup>517</sup> Федеральный закон от 11.08.1995 № 135-ФЗ (ред. от 28.12.2024) «О благотворительной деятельности и добровольчестве (волонтерстве)» // СЗ РФ. 1995. № 33. Ст. 3340; СЗ РФ. 2024. № 53 (Часть I). Ст. 8564.

<sup>518</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

<sup>519</sup> Дети в интернете / ИСИЭЗ. 2023. 1 июня. URL: <https://issek.hse.ru/news/837320649.html?ysclid=m4schi9m1400480739> (дата обращения: 01.05.2025).

<sup>520</sup> Захаров Г. Н. Некоторые вопросы обеспечения безопасности детей в сети Интернет // Социально-правовые аспекты трансформации института современной семьи в контексте реализации государственной семейной политики : сб. статей по материалам международной научно-практической конференции, посв. 25-летию принятия Семейного кодекса Российской Федерации / Под общей редакцией О. Ю. Ильиной. 2020. С. 76-79.

<sup>521</sup> Шитов А. М. Анализ информационных систем родительского контроля web-ресурсов // Актуальные вопросы современной науки : сб. научных статей по материалам II Международной научно-практической конференции. Уфа, 2023. С. 200-205.

Принятая в 2023 г. Концепция информационной безопасности детей в РФ<sup>522</sup> делает акцент на ответственности родителей за воспитание и развитие своих детей. Это обосновано, однако просто дублирует положения ст. 63 СК РФ<sup>523</sup>, не формулируя никакой новизны в постановке и решении имеющихся проблем, то есть не в полной мере выполняя цель документа стратегического планирования. Кроме того, Концепция<sup>524</sup> также обоснованно указывает на приоритет в равном соотношении прав и обязанностей родителей в обеспечении информационной безопасности детей. С этим следует согласиться, но с существенным уточнением. Родители воспитывают будущих граждан, которые будут жить в развитом цифровом мире. Соответственно, родители не просто имеют право, но обязаны дать навыки сетевой безопасности, так как их отсутствие и совершение их детьми неосторожных или противоправных действий способно нарушить права третьих лиц, причинить вред общественным интересам, национальной безопасности.

Примером тому служат многочисленные примеры вовлечения (вербовки) несовершеннолетних через сеть «Интернет» в разного рода противоправные действия<sup>525</sup>. Для того чтобы прививать навыки безопасности в Интернете, родители не только сами должны обладать ими, но и быть в состоянии передать другим. Напомним, как выше уже отмечалось в данной диссертационной работе, что, к примеру, во Франции, согласно ст. 227-17 УК Франции<sup>526</sup>, для родителей, которые не в должной мере выполняют свои обязанности по воспитанию детей и подростков (например, не пресекли взаимодействие несовершеннолетнего и деструктивного

<sup>522</sup> Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СЗ РФ. 2023. № 19. Ст. 348.

<sup>523</sup> Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ (ред. от 23.11.2024, с изм. и доп., вступ. в силу с 05.02.2025) // СЗ РФ. 1996. № 1. Ст. 16; Российская газета. 27.11.2024. № 269.

<sup>524</sup> Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СЗ РФ. 2023. № 19. Ст. 348.

<sup>525</sup> Бошаева Л. Л. Интернет-технологии как способ вовлечения несовершеннолетнего лица в преступную деятельность // Право и государство: теория и практика. 2022. № 4 (208). С. 153-155; Кузина Л. С. «Сетевой наркомаркетинг» как один из факторов вовлечения несовершеннолетних в незаконный оборот наркотиков // Вестник Воронежского института МВД России. 2020. № 4. С. 285-290.

<sup>526</sup> Codepénal. URL: [https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006070719/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/) (дата обращения: 01.05.2025).

контента, что привело к ущербу его безопасности, здоровью, нравственности) предусмотрена уголовная ответственность.

В Австралии Управление комиссара по электронной безопасности – ключевой государственный орган, отвечающий за обеспечение информационной безопасности в сети «Интернет», член общественных организаций, участвующих в вопросах защиты детей в сети «Интернет», представлен организациями, которые не столько специализируются на онлайн-середе, сколько оказывают консультационную, психологическую помощь несовершеннолетним в целом. Australian Child Rights Taskforce – крупная организация по защите прав детей, которая активно участвует в обсуждении законодательных инициатив, выступает за разработку стандартов безопасности детей в социальных сетях<sup>527</sup>. Kids Helpline – служба поддержки детей и подростков, важный образовательный и консультационный ресурс: предоставляет поддержку малолетним и подросткам, включая консультации по вопросам безопасного поведения в сети «Интернет»<sup>528</sup>. Headspace – представляет собой созданную в 2006 году при поддержке правительства Австралии австралийскую некоммерческую организацию, специализирующуюся на поддержке психического здоровья несовершеннолетних<sup>529</sup>. В Австралии в разработке законодательства в сфере защиты детей в сети «Интернет» активно участвуют родители и родительские сообщества, педагогические организации и специалисты по воспитанию детей, экспертные сообщества. Таким образом, в Австралии большинство инициатив в сфере обеспечения информационной безопасности в сети «Интернет» реализуется на государственном уровне или через крупные общественные организации с широким спектром деятельности.

Действующая в Великобритании модель противодействия распространяемой в Интернете детской порнографии и контенту с насилием в отношении детей основана на законе 2003 г. The Protection of the Children Act, Sexual Offences Act

<sup>527</sup> Официальный сайт «The Australian Child Rights Taskforce». URL: <https://childrightstaskforce.org.au/> (дата обращения: 01.07.2025).

<sup>528</sup> Официальный сайт Kids Helpline. URL: <https://kidshelpline.com.au/> (дата обращения: 01.07.2025).

<sup>529</sup> Официальный сайт «Headspace». URL: <https://www.healthdirect.gov.au/> (дата обращения: 01.07.2025).

2003<sup>530</sup>, в соответствии с которым введен запрет копирования и распространения фото- и видеоматериалов с непристойными изображениями несовершеннолетних. Также в британском сегменте Интернета действует «Кодекс правил новых форм контента» (Code of Practise on New Form of Content<sup>531</sup>), в соответствии с которым операторы и провайдеры обязаны использовать программную блокировку опасного контента, включая создание единой базы «незаконных ресурсов», подлежащих блокировке провайдерами, что обеспечивает высокую степень защиты<sup>532</sup>.

Эту деятельность организует IWF – глобальная (действует в 51 стране) общественная организация со штаб-квартирой в Кембридже (Англия), деятельность которой направлена на минимизацию доступности в Интернете материалов о сексуальном насилии, в том числе над несовершеннолетними.

В отличие от российской Лиги безопасного интернета, бюджет IWF прозрачен. Доходы организации в 2023 г., по данным Благотворительной комиссии Англии и Уэльса, составили £6 011 992, а расходы – £4 913 399. Основные поступления (£5,92 млн) принесла благотворительная деятельность, включая два государственных гранта на £421 053<sup>533</sup>. Миссия организации состоит в выявлении, блокировке, удалении и предотвращении распространения материалов о сексуальном насилии над детьми в Интернете.

При этом IWF позиционирует себя как «технологическая организация по защите детей», ставящая целью обезопасить Интернет как для детей, так и для взрослых в глобальном масштабе. Что касается правового статуса, то она действует как некоммерческая организация, существующая при добровольной поддержке представителей интернет-индустрии, поставщиков услуг связи, в том числе интернет-провайдеров, операторов мобильной связи, производителей

<sup>530</sup> Sexual Offences Act 2003 // UK Public General Acts 2003. URL: <https://www.legislation.gov.uk/ukpga/2003/42/contents/enacted> (дата обращения: 01.05.2025).

<sup>531</sup> Code of Practise on New Form of Content. URL: <https://www.mobileuk.org/codes-of-practice> (дата обращения: 01.05.2025).

<sup>532</sup> «Лига безопасного интернета» готовит документ, призванный законодательно ограничить в России доступ к ресурсам, содержащим детское порно, пропаганду наркотиков и экстремистские материалы / Минцифры РФ. URL: <https://digital.gov.ru/ru/events/28870/> (дата обращения: 01.05.2025).

<sup>533</sup> Charity commission for England and Wales. URL: [https://register-of-charities.charitycommission.gov.uk/en/charity-search/?p\\_p\\_id=uk\\_gov\\_ccew\\_onereg\\_charitydetails\\_web\\_portlet\\_CharityDetailsPortlet&p\\_p\\_lifecycle=0&p\\_p\\_state=maximized&p\\_p\\_mode=view&\\_uk\\_gov\\_ccew\\_onereg\\_charitydetails\\_web\\_portlet\\_CharityDetailsPortlet\\_regId=1112398&\\_uk\\_gov\\_ccew\\_onereg\\_charitydetails\\_web\\_portlet\\_CharityDetailsPortlet\\_subId=0](https://register-of-charities.charitycommission.gov.uk/en/charity-search/?p_p_id=uk_gov_ccew_onereg_charitydetails_web_portlet_CharityDetailsPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_uk_gov_ccew_onereg_charitydetails_web_portlet_CharityDetailsPortlet_regId=1112398&_uk_gov_ccew_onereg_charitydetails_web_portlet_CharityDetailsPortlet_subId=0) (дата обращения: 01.05.2025).



оборудования и поставщиков программного обеспечения, а также «обычных граждан». Кроме того, IWF финансируется ЕС как третья часть Британского Национального центра кибербезопасности (National Cybersecurity Center, NCSC), созданной в 2016 г. правительственной организации, которая помогает органам государства в деле развития безопасной сети «Интернет», а также превенции киберугроз. При этом NCSC входит в структуру Правительственного центра связи – британского агентства по разведке информации и кибербезопасности (Government Communications Headquarters, GCHQ), т. е. службы государственной безопасности. Помимо этого IWF декларирует тесное сотрудничество с полицией, правительствами и неправительственными организациями. Руководит IWF попечительский совет в главе с независимым председателем. Члены Совета (10 человек) представляют общество (6), бизнес (информационную отрасль), а также (1) правозащитников. Совет контролирует и пересматривает полномочия, стратегию, политику и бюджет IWF, обеспечивая цели организации<sup>534</sup>. Важно, что IWF не просто уведомляет провайдеров, а разрабатывает технологии, услуги, продукты и наборы данных для превенции повторного появления изображений и усложнения противоправной деятельности<sup>535</sup>. Кроме приема обращений от пользователей сети, агенты IWF активно ищут в открытом и глубоком Интернете изображения и видео с сексуальным насилием над детьми, обращаясь затем к поставщикам услуг с требованием удалить такие веб-сайты или заблокировать их, если они находятся за пределами британской юрисдикции. Когда изображение найдено в открытом доступе в Интернете, IWF отслеживает его локацию и, если она в пределах Великобритании, от хостинговой компании требуют удаления изображения, а если за границей, то информирует местную полицию. Статистика IWF показывает, что свыше 99 % выявленных ими изображений сексуального насилия над детьми размещены за пределами Великобритании. В этом случае, пока выполняется работа по удалению, IWF заносит опасный веб-адрес в список URL-адресов для партнеров, чтобы они могли заблокировать контент. Кроме такого

<sup>534</sup> IWF. URL: Our contacts <https://www.iwf.org.uk/contact-us/> (дата обращения: 01.05.2025).

<sup>535</sup> IWF. Our mission. URL: <https://www.iwf.org.uk/about-us/why-we-exist/our-vision-and-mission/> (дата обращения: 01.05.2025).

перечня IWF ведет несколько сервисов, полезных для интернет-компаний в деле предотвращения распространения запрещенного контента. Также IWF активно строит неформальные партнерские отношения с правоохранительными и государственными органами, институтами гражданского общества. IWF не признает термин «детская порнография» («child pornography»), указывая на своем веб-сайте: «Мы используем термин «сексуальное насилие над детьми» («child sexual abuse»), <...> ребёнок не может дать согласие на собственное насилие»<sup>536</sup>. В Великобритании также функционирует волонтерская организация – Британский совет по безопасности детей в Интернете (UKCCIS) – группа из более чем 200 организаций, которые работают над обеспечением безопасности детей в сети «Интернет»; этот Совет был создан в 2008 году и призван объединить правительственные ведомства, правоохранительные органы, научные круги, частную промышленность и представителей третьего сектора, таких как благотворительные организации и добровольные группы. В настоящее время «Британский совет по безопасности детей в интернете» теперь называется «Британским советом по безопасности в интернете» (UKCIS), который представляет собой форум для сотрудничества, на котором правительство, технологическое сообщество и некоммерческие организации работают вместе над тем, чтобы Великобритания стала максимально безопасным местом для работы в сети «Интернет». UKCIS входит в состав Министерства образования, Министерства внутренних дел и Министерства науки, инноваций и технологий<sup>537</sup>.

Таким образом, в Великобритании функционируют:

- Британский совет по безопасности детей в Интернете (UKCCIS);
- Ассоциация по сертификации возрастных проверок (Age Check Certification Scheme, ACCS)<sup>538</sup>, которая сертифицирует компании, предоставляющие онлайн-сервисы, ориентированные на детей. ACCS тестирует системы идентификации личности и проверки возраста;

---

<sup>536</sup> Там же.

<sup>537</sup> Официальный сайт UKCIS. URL: <https://www.gov.uk/government/organisations/uk-council-for-internet-safety> (дата обращения: 01.05.2025).

<sup>538</sup> Официальный сайт Ассоциации по сертификации возрастных проверок (Age Check Certification Scheme, ACCS). URL: <https://avpassociation.com/> (дата обращения: 01.05.2025).

– IWF<sup>539</sup> – неправительственная саморегулируемая организация, созданная в Великобритании для надзора за Интернетом; можно сказать, что платформа предназначена для отправки сообщений о неправомерном содержимом в Интернете. Деятельность IWF в Великобритании активно критикуется по следующим направлениям: 1) неэффективность фильтрации, которая, по мнению критиков, препятствует законной интернет-активности и при этом неэффективна против злоумышленников<sup>540</sup>; 2) правовой статус благотворительной организации; 3) секретность внутренних процедур, слабая техническая реализация своей политики, которая ухудшает время отклика всего британского Интернета. В этом смысле показателен такой правовой прецедент. В феврале 2009 г. разработчик программного обеспечения из Йоркшира подал в Комиссию по благотворительности официальную жалобу на статус IWF как благотворительной организации, подчеркивая, что она действует в основном для обслуживания интересов поддерживающих ее интернет-провайдеров, а не общественности<sup>541</sup>; 4) секретность. IWF критикуют за внесение в черный список легального контента и за то, что она не сообщает веб-сайтам о том, что они блокируются. Таким образом, владелец заблокированной веб-страницы не уведомляется о том, что на его сайте есть вредный контент, в отношении которого ведется какая-то работа.

В целом, британская модель защиты несовершеннолетних в Интернете представляется заслуживающей внимания как пример результативной интеграции усилий государства, бизнеса и гражданского общества, как пример действующего института, чья деятельность системна, регулируема и, в целом, эффективна (в части минимизации бюджетных расходов). Позитивно и то, что деятельность IWF финансово прозрачна и остается в центре как государственного контроля, так и общественных обсуждений и критики.

<sup>539</sup> Официальный сайт Internet Watch Foundation. URL: <https://www.iwf.org.uk/> (дата обращения: 01.05.2025).

<sup>540</sup> «95% of UK internet is censored? 23 February 2009». Aaisp.net.uk. URL: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.76a79339-676433cc-d5666dd6-74722d776562/https/web.archive.org/web/20111101215616/http://aaisp.net.uk/news-censorship.html](https://translated.turbopages.org/proxy_u/en-ru.ru.76a79339-676433cc-d5666dd6-74722d776562/https/web.archive.org/web/20111101215616/http://aaisp.net.uk/news-censorship.html) (дата обращения: 01.05.2025).

<sup>541</sup> The IWF: Charity disparity? The Register. URL: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.76a79339-676433cc-d5666dd6-74722d776562/https/www.theregister.com/2009/02/20/iwf\\_charity/](https://translated.turbopages.org/proxy_u/en-ru.ru.76a79339-676433cc-d5666dd6-74722d776562/https/www.theregister.com/2009/02/20/iwf_charity/) (дата обращения: 01.05.2025)

На уровне ЕС существуют Центры безопасного Интернета (SIC), которые по всей Европе стремятся обеспечить безопасность детей и подростков в сети «Интернет» с помощью ряда действий и инициатив; SIC предоставляют множество услуг для поддержки детей и молодежи, а также для тех, кто заботится о них – родителям и опекунам, учителям, воспитателям и другим заинтересованным лицам. SIC включают в себя следующие компоненты, которые образуют европейскую сеть «Insafe»: горячие линии, организованные как Insafe, так и Международной ассоциацией горячих линий Интернета (INHOPE), а также национальный центр осведомленности. Insafe и INHOPE работают вместе через сеть SIC по всей Европе, которые обычно включают в себя центр информирования, телефон доверия, горячую линию и молодежную группу<sup>542</sup>. Национальные центры осведомленности сосредоточены на повышении осведомленности и понимания проблем и новых тенденций в области безопасного Интернета. Они проводят кампании по предоставлению детям, молодежи, родителям, опекунам и учителям навыков, знаний и стратегий для обеспечения безопасности в онлайн-пространстве и информирования о возможностях, которые предоставляют Интернет и мобильные технологии.

Горячие линии предоставляют информацию, советы и помощь детям, молодежи и родителям о том, как бороться с вредоносным контентом, деструктивной онлайн-интеракцией (такой как груминг), а также с разрушительным поведением в Интернете (например, кибербуллинг и секстинг). К горячим линиям все чаще можно получить доступ с помощью различных средств – телефона, электронной почты, веб-форм и онлайн-чатов. Горячие линии существуют для того, чтобы позволить членам общественности сообщать о незаконном контенте анонимно. Далее сведения о выявленном контенте передаются в соответствующие органы (интернет-провайдерам, правоохранительным органам) для принятия соответствующих мер. В целях повышения информационной безопасности детей и подростков, иных граждан в

---

<sup>542</sup> Официальный сайт Европейского союза. URL: <https://better-internet-for-kids.europa.eu/en/about/insafe-inhope> (дата обращения: 01.05.2025).

сети «Интернет» в мае 2016 года Европейская комиссия ЕС согласовала с Facebook, Microsoft, Twitter и YouTube «Кодекс поведения по противодействию противозаконным высказываниям, разжигающим ненависть, в Интернете». В течение 2018 года к Кодексу поведения присоединились Instagram, Snapchat и Dailymotion, в январе 2019 года – Jeuxvideo.com, в 2020 году – TikTok, а в 2021 году – LinkedIn. В мае и июне 2022 года о своем участии в Кодексе поведения объявили соответственно Rakuten, Viber и Twitch<sup>543</sup>. Кодекс поведения требует от ИТ-компаний следующее:

- иметь правила и общественные стандарты, запрещающие разжигание ненависти, а также внедрить системы и команды для проверки контента, который, как сообщается, нарушает эти стандарты. Все ИТ-компании, подписавшие Кодекс, теперь имеют и постоянно пересматривают условия обслуживания, правила или стандарты сообщества, запрещающие пользователям публиковать контент, разжигающий насилие или ненависть в отношении защищенных групп. Facebook (принадлежит Meta Platforms Inc.\*, признанной экстремистской организацией и запрещенной на территории Российской Федерации)<sup>544</sup> сообщает, что глобальная сеть насчитывает около 15 000 человек, работающих над всеми типами проверки контента, а в Google и YouTube более 10 000 человек работают над адресами контента, который может нарушать политику компании;

- отслеживать большую часть отмеченного контента в течение последних 24 часов в целях удаления или приостановления доступа к контенту, разжигающему ненависть, если необходимо;

- предоставлять регулярное обучение персоналу по поводу специфики «языка ненависти»;

- назначить национальные контактные пункты для получения уведомлений, в частности от национальных органов власти. Все ИТ-компании, подписавшие Кодекс поведения, организовали национальные пункты для обращений в целях

<sup>543</sup> Официальный сайт Европейской комиссии ЕС. URL: [https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online\\_en](https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en) (дата обращения: 01.12.2024)

<sup>544</sup> Официальный портал судов общей юрисдикции города Москвы. URL: <https://mosgorsud.ru/rs/tverskoj/services/cases/civil/details/de7ea6a0-a3ab-11ec-8a7e-51b31fb55b35> (дата обращения: 01.12.2024).

облегчения связи с соответствующими компетентными органами на национальном уровне.

Еще раз следует отметить, что для предотвращения кибербуллинга и защиты его жертв в Германии также действует ряд организаций и инициатив, поддерживаемых Федеральным правительством и регионами. Так, «jugendschutz.net» – это объединенный центр компетенции Федерального правительства и правительств земель для защиты детей и молодежи в Интернете, который организационно связан с КJM и помогает надзору в выполнении его обязанностей. В частности, орган контролирует предложения о нарушениях прав несовершеннолетних в СМИ и направляет дела в КJM для возбуждения судебного разбирательства. Некоммерческая организация с ограниченной ответственностью (gGmbH) «jugendschutz.net»<sup>545</sup> – это компания, которая на основании статьи 18 Государственного договора о защите детей и молодежи в сфере СМИ (JMStV)<sup>546</sup> занимается защитой молодежных СМИ в «телемедиа», то есть, в частности, в сети «Интернет». Согласно JMStV, «jugendschutz.net» представляет собой объединенный центр компетенции Федерального правительства и правительств земель для защиты детей и молодежи в Интернете, который связан с КJM и финансируется за счет региональных средств и средств Федерального министерства по делам семьи, пожилых граждан, женщин и молодежи. Эта организация исследует риски для молодежи в Интернете и привлекает к ним внимание владельцев ресурсов, родителей и молодых людей. Кроме того, на сайте организации есть онлайн-служба жалоб, куда родители, дети и молодые люди могут сообщать о нарушениях. Сайт jugendschutz.net отслеживает предложения в сети на предмет нарушений прав молодежи и принимает жалобы, а также проводит собственные исследования, чтобы определить, какие риски существуют для детей и подростков. Существует утвержденная процедура рассмотрения жалоб, согласно которой команда сайта jugendschutz.net просматривает представленный контент, оценивает содержание с

<sup>545</sup> Официальный сайт gGmbH «jugendschutz.net». URL: <https://www.jugendschutz.net/> (дата обращения: 01.05.2025).

<sup>546</sup> Jugendmedienschutz-Staatsvertrag (JMStV) vom 13. September 2002 (GVBl. 2003 S. 147, BayRS 02-21-S), der zuletzt durch Art. 2 des Vertrages vom 27. Februar 2024 (GVBl. S. 326) geändert worden ist. URL: <https://www.gesetze-bayern.de/Content/Document/JMStV> (дата обращения: 01.05.2025).

точки зрения юридических аспектов и выясняет, кто несет ответственность за него (известен ли владелец блога, публикации на веб-сайте или в социальных сетях и является ли поставщик услуг членом добровольного органа самоконтроля)<sup>547</sup>.

Выводы по главе 2 исследования.

1. Рассмотрены органы публичной власти, обеспечивающие информационную безопасность несовершеннолетних в сети «Интернет» в зарубежных государствах. Следует сказать, что в этих государствах действуют специальные нормы по защите несовершеннолетних от деструктивного контента и, как правило, в виде единого правового акта, обеспечивающего информационную безопасность несовершеннолетних. В Австралии до 2017 года функционировало Управление комиссара по электронной безопасности детей, в 2017 году его полномочия были расширены, в итоге его деятельность стала охватывать все возрастные категории, а должность была переименована в «Комиссар по электронной безопасности». Закон Online Safety Act 2021 регламентирует деятельность Управления по вопросам электронной безопасности (eSafety) как независимой государственной организации, деятельность которой поддерживается Австралийским управлением по коммуникациям и СМИ (АСМА) и непосредственно комиссаром по электронной безопасности, который является независимым статутным учреждением в составе АСМА, а также порядок привлечения нарушителей к юридической ответственности. Отметим, что в обязанности комиссара по электронной безопасности входит разработка рекомендаций по «разумным мерам», которые должны приниматься платформами социальных сетей с возрастными ограничениями.

В США как государстве – родоначальнике социальных сетей основным органом, который обеспечивает информационную безопасность несовершеннолетних в сети «Интернет», является Федеральная торговая комиссия (FTC), которая уделяет особое внимание вопросам конфиденциальности детей в Интернете; осуществляет надзор за соблюдением требований Закона COPPA,

---

<sup>547</sup> Beschwerdeverfahrenjugendschutz.net. URL: <https://www.jugendschutz.net/ueber-uns/beschwerdeverfahren> (дата обращения: 01.05.2025).

которые также распространяются на операторов, если они «фактически знают» («actual knowledge»), что собирают персональные данные пользователей другого сайта, ориентированного на детей младше 13 лет. Интересен тот момент, что понятие «фактически знают» легально не определено.

Во Франции функционирует Национальный совет по защите детей, в состав которого вошли представители различных органов власти (в том числе и мировых судей), а также представителей общественных организаций, занимающихся воспитанием и (или) защитой прав несовершеннолетних; также в ведении председателя окружного совета осуществляет свою деятельность Служба социальной помощи детям. Министерство внутренних дел Франции ведет борьбу со всеми формами киберпреступности, направленной в том числе и против детей. Национальная комиссия по информационным технологиям и гражданским свободам (CNIL) с 2022 года проводит исследования по вариантам онлайн-верификации возраста, результаты которого периодически публикуются на официальном сайте CNIL.

В Германии функционирует Федеральный центр защиты детей и молодежи (BzKJ), который является независимым федеральным надзорным органом в сфере деятельности Федерального министерства по делам семьи, пожилых людей, женщин и молодежи (BMFSFJ). Интересным является тот факт, что в 2022 году в Германии одобрено использование искусственного интеллекта (ИИ) для целей проверки возраста на онлайн-платформах.

В Великобритании функционирует Управление по коммуникациям (Ofcom), представляющее собой регулирующий и антимонопольный орган в сфере телекоммуникаций и связи Великобритании; Ofcom уполномочен блокировать доступ к конкретным веб-сайтам; штрафовать компании, которые не соблюдают обязанность по защите пользователей от вредоносного контента в Интернете. Ofcom обязан обеспечивать надлежащую защиту граждан (в том числе несовершеннолетних) от информации, причиняющей вред их здоровью или развитию. В 2023 году был учрежден Консультативный комитет по дезинформации и ложной информации в составе Ofcom; также следует сказать, что технологии



верификации возраста, которые не нарушали бы конфиденциальность пользователей, и предусмотренные законом, также разрабатываются.

В Ирландии в 2022 году учрежден Coimisiún na Meán в качестве национального регулирующего органа в соответствии со ст. 30 Директивы ЕС об аудиовизуальных медиауслугах (AVMSD); установлены полномочия Coimisiún na Meán в части обеспечения информационной безопасности несовершеннолетних, также Закон OSMR предусматривает назначение комиссара по безопасности в сети «Интернет» в Coimisiún na Meán, который отвечает за соблюдение обязательного кодекса безопасности в Интернете и несет ответственность не только за вредоносный онлайн-контент, но и контент, не соответствующий возрасту, в том числе порнографию и грубое и бессмысленное насилие.

2. Примеры из судебной практики, рассмотренные в параграфе 2.1, иллюстрируют проблему «сферы судебной юрисдикции»: при национальном законодательстве и решениях национальных судов об изъятии (запрете, блокировке) деструктивного контента для несовершеннолетних, непосредственно сама сеть «Интернет», а именно глобальные цифровые площадки, распространяющие деструктивный контент, носят наднациональный, международный характер. С учетом технологий Virtual Private Network (VPN), переездов несовершеннолетних граждан в разные государства (где деструктивный контент может быть не заблокирован по решению суда) и т. д. — возникает необходимость в постепенной гармонизации и унификации правовых норм в части понятий деструктивной информации для разных государств.

3. Органы публичной власти в сфере обеспечения информационной безопасности несовершеннолетних в России функционируют в виде комплексного механизма, который при этом не образует единую законодательно определенную систему.

4. Выявлено, что в ст. 20 Федерального закона № 436-ФЗ<sup>548</sup> нет упоминания МВД и прокуратуры как субъектов, которые уполномочены осуществлять контроль

<sup>548</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

(надзор) за соблюдением законодательства РФ о защите детей от вредоносного контента, а также проводить профилактику правонарушений среди несовершеннолетних в этой сфере.

5. В России отсутствует специализированная структура в органах публичной власти, деятельность которой была бы направлена конкретно на обеспечение информационной безопасности несовершеннолетних в сети «Интернет»; отсутствует специализированная система подачи жалоб на информацию (материалы), содержащие деструктивный контент и адресованные непосредственно несовершеннолетним. Ежегодно возрастающее количество правонарушений в изучаемой сфере наглядно иллюстрирует необходимость модернизации структуры органов публичной власти, реализующих обеспечение информационной безопасности несовершеннолетних. Считаем целесообразным внести изменения в Приказ Роскомнадзора от 25.03.2022 № 53<sup>549</sup> в части создания в структуре Роскомнадзора «Управления по информационной безопасности несовершеннолетних» с перечисленными в тексте исследования полномочиями.

6. В России отсутствует правовой механизм контроля (надзора) возрастного критерия при регистрации в социальных сетях несовершеннолетних граждан. На наш взгляд, целесообразно учесть опыт зарубежных государств и предусмотреть обязанность социальных сетей не только в декларационном порядке регистрировать пользователей по достижении 14 лет, но и законодательно предусмотреть это требование и ответственность за его неисполнение. Предложено и обосновано внесение в Закон об информации от 27.07.2006 № 149-ФЗ статьи 10.8, устанавливающей обязанности владельца социальных сетей в информационно-телекоммуникационной сети «Интернет». Контроль за выполнением этой обязанности владельцем социальных сетей возложить на Роскомнадзор.

7. Рассмотрены общественные (некоммерческие) объединения России, Австралии, Великобритании, наднациональные и национальные объединения государств – членов ЕС (Франции и Германии). Проведен сравнительный анализ

---

<sup>549</sup> Приказ Роскомнадзора от 25.03.2022 № 53 «Об утверждении структуры и штатного расписания Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СПС «КонсультантПлюс».

российской «Лиги безопасного интернета» и зарубежных общественных организаций.

8. Обоснована правовая позиция, что с учетом значимости и значительного развития добровольчества (волонтерства) в сфере обеспечения информационной безопасности в сети «Интернет» следует дополнить ч. 1 ст. 2 Федерального закона от 11.08.1995 № 135-ФЗ<sup>550</sup> еще одной целью: «содействие в обеспечении информационной безопасности граждан, в том числе несовершеннолетних, в информационно-телекоммуникационной сети «Интернет»».

---

<sup>550</sup> Федеральный закон от 11.08.1995 № 135-ФЗ (ред. от 28.12.2024) «О благотворительной деятельности и добровольчестве (волонтерстве)» // СЗ РФ. 1995. № 33. Ст. 3340; СЗ РФ. 2024. № 53 (Часть I). Ст. 8564.

### **ГЛАВА 3. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТВЕТСТВЕННОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ «ИНТЕРНЕТ» ПО ЗАКОНОДАТЕЛЬСТВУ РОССИИ И ЗАРУБЕЖНЫХ ГОСУДАРСТВ**

#### **3.1. Меры административного принуждения в сфере информационной безопасности несовершеннолетних в сети «Интернет» по законодательству зарубежных государств**

В любом государстве именно несовершеннолетние лица являются наиболее активными пользователями сети «Интернет», тем самым создавая опасность деструктивного воздействия на них информационного пространства ввиду возрастного, умственного, психологического развития несовершеннолетних. Поэтому государства, как российское, так и зарубежные, регламентируют отношения с участием несовершеннолетних в сетевом пространстве для защиты несовершеннолетних лиц от деструктивного информационного воздействия.

Административно-правовая ответственность за нарушения в сфере информационной безопасности несовершеннолетних в сети «Интернет» включает в себя не только административную ответственность, но и применение иных мер ответственности (наказаний), предусмотренных нормами административного права. Следует отметить, что в зарубежных государствах некоторые составы административных правонарушений, предусмотренные в КоАП РФ, можно встретить не только в административном, но и в уголовном законодательстве, по этой причине такие составы правонарушений и ответственность за их совершение нами относятся к административно-правовой ответственности, несмотря на то, что эти составы включены в уголовные кодексы зарубежных государств.

Рассмотрим ответственность за нарушения законодательных норм в сфере информационной безопасности несовершеннолетних в сети «Интернет» в Австралии.

Как отмечает Е. В. Муратова в своем диссертационном исследовании, «...созданная в Австралии система административной юстиции, представленная системой пересмотра административных решений в федеральных судах Австралии (judicial review) и системой пересмотра по существу административных решений в независимых административных трибуналах (merits review), деятельностью омбудсмана Австралийского Союза и иными средствами контроля за публичной администрацией, является одной из самых прогрессивных в мире»<sup>551</sup>.

В отличие от российского административного права в Австралии отсутствует единый кодифицированный кодекс, посвященный административным правонарушениям, административной ответственности. Австралийское административное право определяет объем полномочий и обязанностей административных органов правительства Австралии. По сути, это система общего права с растущим количеством законодательных актов, которые сместили акцент в сторону кодифицированного судебного контроля и судов с широкой юрисдикцией<sup>552</sup>. В соответствии с законодательством лица, принимающие административные и судебные решения, обязаны предоставлять письменные документы, как правило, письменное обоснование своих решений. Согласно закону, заявителю, подающему апелляцию в соответствии с законодательством Содружества, должны предоставляться письменные обоснования решений судов Содружества и лиц, принимающих административные решения, в соответствии с разделом 13 Закона об административных решениях (судебном пересмотре) Австралии от 16 июня 1977 г. (Administrative decisions (judicial review) Act 1977)<sup>553</sup>, а также в соответствии с разделом 269 Закона о трибунале по административным решениям 2024 года (Administrative Review Tribunal Act 2024)<sup>554</sup>. Как уже было обозначено выше, в Австралии действует Закон о безопасности в Интернете № 76

<sup>551</sup> Муратова Е. В. Административная юстиция в Австралии : автореф. дис. ... канд. юрид. наук. М., 2013. С. 3.

<sup>552</sup> Bateman W., McDonald L. The Normative Structure of Australian Administrative Law // Federal Law Review. 2017. № 45(2). P. 153-179.

<sup>553</sup> Закон об административных решениях (судебном пересмотре) Австралии от 16 июня 1977 г. (Administrative decisions (judicial review) Act 1977). URL: <https://www.legislation.gov.au/Details/C2013C00365> (дата обращения: 01.05.2025).

<sup>554</sup> Administrative Review Tribunal Act 2024. URL: <https://www.legislation.gov.au/C2024A00040/latest/text> (дата обращения: 01.05.2025).

от 23 июля 2021 г. (Online Safety Act 2021)<sup>555</sup>. Согласно ст. 64 этого закона при выявлении факта размещения в сети «Интернет» неправомерной информации оператору направляется уведомление, которое содержит требование удаления из общего доступа данной информации и предупреждение о неправомерности подобных действий, в случае необходимости – принести извинения за публикацию. При повторном опубликовании на виновное лицо налагается штраф в размере 500 штрафных единиц. Уточним, что согласно ст. 156 Online Safety Act 2021 при выявлении комиссаром по электронной безопасности неоднократности данного правонарушения он имеет право обратиться в Федеральный суд с требованием прекратить деятельность по предоставлению услуг в интернет-пространстве.

Понятие «cyber-bullying» (киберзапугивание или кибербуллинг) несовершеннолетнего по законодательству Австралии присутствует в законодательстве, но без легально закрепленной дефиниции.

Согласно ст. 1 Закона, содержащего определения, используемые в этом законе, сказано: материалы о кибербуллинге, предназначенные для австралийского ребенка, имеют значение, указанное в разделе 6 («cyber-bullying material targeted at an Australian child has the meaning given by section 6»)<sup>556</sup>. Так, уточним еще раз, что в разделе 6 Материалы о кибербуллинге, направленные против австралийского ребенка, нет непосредственно легального определения термина «cyber-bullying», но указаны следующие признаки:

- 1) материал должен быть размещен на сервисе социальных сетей; или соответствующем электронном сервисе; или определенном интернет-сервисе;
- 2) обычный здравомыслящий человек пришел бы к выводу, что: вполне вероятно, что материал был предназначен для воздействия на конкретного австралийского ребенка; материал, вероятно, будет представлять для австралийского ребенка серьезную угрозу, серьезно запугивать, серьезно беспокоить или серьезно унижать его достоинство;

<sup>555</sup> Online Safety Act 2021 No. 76. URL: <https://www.legislation.gov.au> (дата обращения: 30.03.2025).

<sup>556</sup> Там же.

3) другие условия (если таковые имеются), которые указаны в законодательных нормах; этот материал является кибер-травлей, направленной против австралийского ребенка; целью этого материала является австралийский ребенок.

Иными словами, кибербуллинг можно определить как использование социальных сетей, текстовых сообщений, электронной почты или телефонных звонков с любого электронного телекоммуникационного устройства для оскорбления, запугивания, преследования или угроз в адрес другого человека, его безопасности или для того, чтобы вызвать у него обоснованные опасения по поводу возможности насилия<sup>557</sup>. Такое поведение обычно повторяется и направлено на то, чтобы причинить боль, расстроить, смутить или напугать несовершеннолетнего. Другие формы кибербуллинга могут включать в себя сексуальное домогательство к несовершеннолетнему лицу, которое преследуется по закону в соответствии с уголовным законодательством.

В Австралии нет специального закона, предусматривающего уголовную ответственность за кибербуллинг, однако в существующие законы, которые мы рассмотрим далее, были внесены поправки, позволяющие криминализировать и наказывать за кибербуллинг. В Австралии о случаях кибербуллинга можно сообщить уполномоченному по вопросам кибербезопасности, а также в полицию. Уполномоченный по вопросам кибербезопасности имеет законодательные полномочия требовать от поставщиков онлайн-услуг удаления крайне опасного контента в течение 24 часов после получения официального уведомления. Комиссар также может оказать поддержку родителям и детям в выборе оптимальных действий при столкновении с кибербуллингом.

В Новом Южном Уэльсе в Законе о преступлениях (домашнее и личное насилие) № 80 2007 г. (Crimes (Domestic and Personal Violence) Act 2007 No 80) (Новый Южный Уэльс)<sup>558</sup> были внесены поправки, охватывающие такие виды кибербуллинга, как публикация угрожающих или оскорбительных сообщений,

<sup>557</sup> Cyberbullying. URL: <https://www.esafety.gov.au> (дата обращения: 01.05.2025).

<sup>558</sup> Crimes (Domestic and Personal Violence) Act 2007 No 80 (current version for 4 April 2025). URL: <https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2007-080#sec.13>

фотографий или видео в Интернете или неоднократная отправка нежелательных сообщений. Поправки к закону получили название «Закон Долли» в честь Эми «Долли» Эверетт, которая в возрасте 14 лет покончила с собой в 2018 году после продолжительного кибербуллинга со стороны сверстников в школе-интернате.

Так, ст. 7(1) фиксирует, что «запугивание лица» означает поведение (включая киберзапугивание), равносильное преследованию или приставанию к лицу, или пример поведения, которое может быть равносильно преследованию лица или преднамеренное разглашение или угроза разглашения любых из нижеследующих сведений о человеке без его согласия, известное как «outing»: сексуальная ориентация человека; гендерная история человека; наличие у человека различных половых признаков; то, что человек живет с ВИЧ; что данное лицо является или было работником секс-бизнеса. Примечание к этой статье устанавливает, что примером киберзапугивания может быть травля человека путем публикации или передачи оскорбительных материалов в социальных сетях или по электронной почте.

Статья 13 предусматривает уголовную ответственность за действия, которые можно расценить как преследование или запугивание человека если лицо, совершившее эти действия, намеревалось вызвать страх или причинить физический или моральный вред или, по крайней мере, знало, что его действия могут вызвать страх у жертвы; максимальное наказание – лишение свободы на срок 5 лет или штраф в размере 5500 долларов, или и то, и другое (ст. 13)<sup>559</sup>.

В серьезных случаях кибербуллинга может иметь место нарушение статьи 31C(2) Закона о преступлениях 1900 года (Новый Южный Уэльс)<sup>560</sup>, которая предусматривает уголовную ответственность за подстрекательство или советы другому лицу совершить самоубийство, если в результате этого другое лицо совершает или пытается совершить самоубийство. За подстрекательство или советы другому лицу совершить самоубийство предусмотрено наказание в виде лишения свободы на срок до 5 лет.

<sup>559</sup> Там же.

<sup>560</sup> Crimes Act 1900 (NSW) No. 40. URL: <https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1900-040#sec.31C> (дата обращения: 01.05.2025).



Также серийное онлайн-насилие и кибербуллинг считаются преступлением по ст. 474.17 Уголовного кодекса 1995 года<sup>561</sup>. Чтобы поведение преступника могло считаться уголовным правонарушением, оно должно серьезно повлиять на жертву (психически или физически). В соответствии с федеральным законодательством Австралии, ст. 474.17A(1) Уголовного кодекса Закона 1995 года, использование лицом услуг связи, таких как Wi-Fi, Интернет или телекоммуникационные услуги, таким образом, что это может быть расценено разумным человеком как оскорбительное или угрожающее при любых обстоятельствах, что включает в себя передачу, предоставление доступа, публикацию, распространение, рекламу или продвижение материалов сексуального характера, является преступлением, наказуемым лишением свободы на срок до 6 лет.

Уточним, что в Австралии один из самых низких возрастов уголовной ответственности в мире, который составляет 10 лет, за исключением Австралийской столичной территории (повышен возраст уголовной ответственности до 14 лет с 1 июля 2025 года с переходным периодом до 12 лет) и Виктории (правительство штата Виктория повысило возраст уголовной ответственности до 12 лет к концу 2024 года и повысит до 14 лет к 2027 году).

Интересен прецедент, согласно которому по решению Верховного суда Австралии медиакомпании в Австралии несут ответственность за комментарии, которые читатели оставляют на их страницах в соцсетях, если в комментариях содержится клевета и оскорбления<sup>562</sup>. По мнению суда, СМИ, создавая открытые страницы в соцсетях, поощряют появление комментариев, а значит, должны отвечать за них. Австралийские медиакомпании прогнозируют, что это решение суда приведет к тому, что СМИ будут закрывать комментарии под своими публикациями и в целом меньше публиковать тексты в соцсетях.

<sup>561</sup> Criminal Code Act 1995 No. 12. URL: <http://www5.austlii.edu.au/au> (дата обращения: 01.05.2025).

<sup>562</sup> Fairfax Media Publications Pty Ltd v Voller; Nationwide News Pty Limited v Voller; Australian News Channel Pty Ltd v Voller [2021] HCA 27 (8 September 2021) S236/2020, S237/2020 и S238/2020. URL: [https://www.hcourt.gov.au/cases/case\\_s236-2020](https://www.hcourt.gov.au/cases/case_s236-2020) (дата обращения: 01.05.2025).

Согласно Закону о клевете 2005 г. (Defamation Act 77 of 2005 (at 2 March 2025))<sup>563</sup> клевета может быть определена как ложное утверждение о человеке, порочащее его честь и достоинство. Для подачи иска истцу необходимо доказать три элемента: публикацию, идентификацию и клеветнический смысл. Заявление имеет клеветнический смысл, если оно может заставить обычного, здравомыслящего читателя хуже относиться к истцу или если оно может привести к тому, что истца будут избегать или подвергать более чем банальным насмешкам. При этом публикация понимается в широком смысле, включая любое сообщение кому-либо, кроме заявителя, как письменное, так и устное. Защититься от обвинений в клевете достаточно сложно, ведь истец не должен доказывать, что порочащие его сведения ложны, а единственное, что может сделать ответчик, это доказать, что все факты являются правдой.

Более того, в 2021 году австралийское правительство предложило законопроект Social Media (Anti-Trolling) Bill<sup>564</sup>, который должен заставить социальные сети раскрыть личности анонимных пользователей, публикующих клеветнические комментарии.

Согласно законопроекту социальные сети будут обязаны раскрывать персональные данные «онлайн-троллей» и клеветников. Граждане Австралии, в том числе несовершеннолетние, которые считают, что их оклеветали в Интернете, смогут получить судебные постановления, обязывающие онлайн-гигантов, таких как Twitter Inc. и Meta Platforms Inc. (ранее известна как Facebook), установить личности авторов постов. Если платформы социальных сетей не смогут этого сделать, им придется возместить ущерб от клеветы. Уточним, что действие правовых норм по рассматриваемому законодательству не предусматривает раскрытие личности «интернет-троллей» с территории других государств.

Кроме того, социальные сети планируют обязать создать специализированные формы, через которые пользователи смогут сообщать о том,

---

<sup>563</sup> Defamation Act 77 of 2005 (at 2 March 2025) Australia, New South Wales. URL: [https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/nsw/consol\\_act/da200599/](https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/nsw/consol_act/da200599/) (дата обращения: 01.05.2025).

<sup>564</sup> Exposure Draft of the Social Media (Anti-Trolling) Bill 2021, December 2021. URL: [https://www.uts.edu.au/globalassets/sites/default/files/2022-05/cmt-submission-to-attorney-generals-department-on-exposure-draft-of-anti-trolling-bill\\_0.pdf](https://www.uts.edu.au/globalassets/sites/default/files/2022-05/cmt-submission-to-attorney-generals-department-on-exposure-draft-of-anti-trolling-bill_0.pdf) (дата обращения: 01.05.2025).

что стали жертвой клеветы. Сначала пользователей, публикующих дискредитирующий контент, будут просить самостоятельно удалить записи с площадки и урегулировать вопрос. Если же просьба не будет удовлетворена, то у жертвы будет возможность подать судебный иск.

Согласно действующему законодательству компании, занимающиеся социальными сетями, не считаются издателями материалов, размещенных на их платформах. Например, если пользователь оставляет клеветнические комментарии на странице Facebook, юридическая ответственность ложится на владельца страницы. Этот законопроект на момент написания исследования не принят, при его обсуждении было указано, что клевета составляет лишь малую долю деструктивного («троллингового») воздействия в сети «Интернет», поэтому предложенный правовой механизм защиты лиц в социальных сетях от репутационного ущерба признан неэффективным.

Как уже указано выше, в ЕС с мая 2018 года действует GDPR, основной целью которого является обеспечение информационной безопасности граждан ЕС, в особенности защита их персональных данных и конфиденциальности. Статья 51 GDPR устанавливает обязанность для государств – членов создания независимых органов публичной власти, ответственных за исполнением норм GDPR, защиту физических лиц в части их персональных данных на территории ЕС и, в том числе, в сети «Интернет» (далее – надзорный орган). Национальные надзорные органы должны сотрудничать между собой, создавая устойчивую систему в рамках ЕС. Государства могут создавать несколько национальных надзорных органов, но при этом должны назначить одно из них контактным центром для взаимодействия с другими подобными органами государств – членов ЕС. Пункты a-h и j § 2 ст. 58 GDPR наделяют надзорный орган правом выносить контролеру или процессору (часто используется термин «обработчик») предупреждения за нарушение норм GDPR в случаях, если обработка персональных данных может: предположительно нарушать требования GDPR, если непосредственно обработка противоречит нормам GDPR, а также требовать, чтобы контролер сообщил лицу, чьи персональные данные (субъект) обрабатываются, о выявленных нарушениях в

обработке его данных; предоставить ответ на запрос субъекта персональных данных; исправить и (или) уничтожить данные в случаях, предусмотренных ст. 16–18 GDPR; также надзорный орган имеет право налагать временное или постоянное ограничение, запрет на обработку данных конкретным контролером, отзываться сертификат, позволяющий проводить обработку персональных данных. Согласно п. «h» § 2 ст. 58 и ст. 83 GDPR надзорный орган налагает административный штраф как в дополнение к предупреждению и иным мерам, указанным выше, так и вместо них. Уточним, что для определения степени наказания рассматривается каждый случай конкретно.

Таким образом, каждое государство – член ЕС имеет собственный орган для расследования предполагаемых нарушений и обеспечения соблюдения GDPR, эти независимые государственные учреждения известны как органы по защите данных (DPA).

Глава 8 GDPR посвящена средствам правовой защиты, ответственности и санкциям, а именно ст. 82 содержит нормы, регламентирующие ответственность и право на компенсацию, ст. 83 устанавливает общие условия для наложения административных штрафов, ст. 84 раскрывает санкции. Считаем важным отметить, что название статьи и термин в них «административный штраф» указаны согласно интерактивному справочнику проекта «GDPR-TEXT.COM», целью которого является наиболее точный перевод GDPR на разные языки, в том числе на русский<sup>565</sup>. Так, если контролером или обработчиком допущено нарушение положений GDPR, которое повлекло причинение ущерба (материального или нематериального) любому лицу, то такое лицо имеет право на получение компенсации. Следует уточнить, что законом предусмотрено освобождение от ответственности в случае, если контролер или обработчик сможет доказать, что ущерб был нанесен пострадавшему лицу не по вине контролера или обработчика. Нормы GDPR (ст. 83) содержат условия определения административного взыскания в виде штрафа с учетом: 1) эффективности наказания; 2) применения меры

---

<sup>565</sup> Общий регламент защиты персональных данных ЕС / Общ. ред. С. Воронкевич. URL: <https://gdpr-text.com/ru/> (дата обращения: 01.08.2025).

сдерживания; 3) соразмерности.

Часть 1 ст. 51 GDPR устанавливает обязанность национальных надзорных органов государств – членов ЕС гарантировать соблюдение не просто наложения административного штрафа, но обязательно с условием соблюдения при этом индивидуального подхода, соразмерности, сдерживания повторных совершений правонарушений и эффективности наказания. Для достижения этих условий учитываются: 1) характер, тяжесть и продолжительность нарушения (какие категории персональных данных, в каком объеме и как долго неправомерно обрабатывались), размер причиненного ущерба; 2) сознательно или по неосторожности допущены нарушения; 3) были ли предприняты ответственным лицом меры по избежанию или уменьшению ущерба при обработке персональных данных; 4) сообщил ли контролер или обработчик сам об утечке данных надзорному органу, степень взаимодействия; 5) повторяемость правонарушений в этой сфере правоотношений; 6) иные обстоятельства, смягчающие или отягчающие наказание.

Часть 3 ст. 51 GDPR устанавливает, что при совокупности правонарушений норм GDPR применяется правило, согласно которому общий размер штрафа не может быть выше, чем размер штрафа за наиболее тяжкое правонарушение.

Непосредственно размеры штрафов установлены п. 4–6 ст. 51 GDPR, при этом за правонарушения, указанные в ст. 8, 11, 25–39, 42, 41(4), 43, административный штраф составляет до 10 млн евро, а в случае субъекта хозяйствования – до 2 % от общего годового мирового оборота за предыдущий финансовый год (в зависимости от того, какая сумма больше); максимальный штраф до 20 млн евро, в случае субъекта хозяйствования – до 4 % от общего годового мирового оборота за предыдущий финансовый год назначается за нарушение основных принципов GDPR (ст. 5–7, 9) и обязательств контролеров (обработчиков), которые установлены главой IX, а также предусмотренные ст. 12–22 права субъектов персональных данных; за передачу третьим лицам (в иное государство или международной организации), что установлено ст. 44–49 GDPR. Также наказание в виде максимального штрафа предусмотрено за неисполнение

предписаний и (или) ограничений, которые выданы надзорным органом. Также стоит обратить внимание, что штрафы за нарушение GDPR поступают в национальный бюджет государства – члена ЕС, которое взыскало данный штраф, а не поступают субъектам персональных данных, чьи права и интересы были нарушены.

В рамках нашей темы исследования достаточно интересен п. 9 ст. 51 GDPR, который регламентирует те случаи, когда в государстве – члене ЕС не предусмотрены административные штрафы. Так, в этом случае положения GDPR национальным надзорным органом применяются таким образом, чтобы штраф налагался компетентными национальными судами (например, такая модель реализуется в Дании и Эстонии). Согласно примечаниям 148, 149 GDPR установлено, что в случаях незначительных правонарушений физических лиц надзорный орган может ограничиться вынесением наказания в виде выговора. А в случаях определения меры ответственности физического лица, которое не является субъектом хозяйствования, необходимо принимать во внимание его доход и материальное положение. Уточним, что согласно ст. 84 и (149) GDPR государства – члены ЕС имеют право также устанавливать уголовную ответственность за нарушение норм GDPR при условии соблюдения принципов соразмерности, эффективности и профилактики правонарушений. Кроме того, административные и (или) уголовные санкции должны быть определены национальным правом государства – члена ЕС.

Великобритания после официального выхода из ЕС 31.01.2020 приняла свой регламент, аналогичный GDPR. За соблюдение GDPR в Великобритании отвечает Управление комиссара по информации (ICO). Отметим, что принципы, права и обязанности субъекта персональных данных, контролеров (процессоров) максимально схожи с нормами GDPR; правовая ответственность аналогична первоначальному европейскому регламенту. В GDPR GB также предусматривается два уровня административных штрафов: 1) за менее серьезные правонарушения размер штрафа составляет ту величину, которая больше: до £8,7 млн или до 2 % от мирового годового дохода за предыдущий финансовый год; 2) за более серьезные

или повторные правонарушения размер штрафа составляет ту величину, которая больше: до £17,5 млн или до 4 % от мирового годового дохода за предыдущий финансовый год.

В Германии предусмотрена административная и уголовная ответственность за распространение деструктивного контента. Правовые системы России и Германии относятся к романо-германской (континентальной) правовой семье. Как отмечает Л. В. Гаврилова, в юридической науке «отсутствуют единый подход к отнесению правонарушения к уголовной или административной ответственности в Германии»<sup>566</sup>. В своей научной статье Т. Ф. Минязева и А.В. Серебренникова указывают, что согласно мнению одной части научно-юридического сообщества, все правонарушения в Германии следует отнести к предмету уголовного права, другая же часть полагает, что имеет место как «административная (которая считается специальной (*lex specialis*) по отношению к общему уголовному закону), так и уголовная ответственность»<sup>567</sup>. Отметим, что само понятие административной ответственности, закрепленное в § 2 Закона об административных правонарушениях (OWiG)<sup>568</sup> представляет собой «противоправное деяние, подлежащее обвинению, в совершении которого реализуется действие закона, разрешающего наказание в виде штрафа». Отметим, что возраст привлечения к ответственности физических лиц составляет 14 лет. Основным видом наказания, как следует из определения и непосредственно третьего раздела OWiG, является денежное взыскание в виде штрафа. Можно сказать, что в целом OWiG носит рамочный характер.

Нормами NetzDG<sup>569</sup> предусмотрен порядок рассмотрения жалоб владельцами сайтов в сети «Интернет» на выявление деструктивного контента (в особенности травлю в отношении несовершеннолетних), размещенного в социальных сетях, с

<sup>566</sup> Гаврилова Л. В. Разграничение преступления и административного правонарушения как научная и нормотворческая проблема в ФРГ // Академический юридический журнал. 2003. № 3.

<sup>567</sup> Минязева Т. Ф., Серебренникова А. В. Уголовная ответственность юридических лиц в России и Германии: к постановке проблемы // Lex russica. 2017. № 2 (123). С. 147-154.

<sup>568</sup> Gesetz über Ordnungswidrigkeiten (OWiG). URL: <https://www.buzer.de/gesetz/5827/index.htm> (дата обращения: 01.05.2025).

<sup>569</sup> Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) 2017. URL: <https://www.buzer.de/NetzDG.htm> (дата обращения: 01.05.2025).

целью удаления подобного контента. При этом у владельцев подобных сайтов есть обязанность хранения удаленного из общего доступа деструктивного контента, так как его предоставление может потребоваться для суда, если гражданин в судебном порядке будет защищать свои права и интересы. Также надзорный орган по защите несовершеннолетних обладает правом досудебного воздействия в отношении распространителей ненадлежащей информации. Таким образом, за распространением контента, деструктивно влияющего на несовершеннолетних в сети «Интернет», предусмотрена ответственность, в частности, для владельцев социальных сетей, которые обязаны после получения жалобы пользователей либо в течение 24 часов удалить (блокировать доступ) к незаконному контенту, либо в течение 7 дней в части контента, законность или незаконность которого необходимо определить в ходе проверки. Систематическое несоблюдение этого требования владельцами социальных сетей считается административным правонарушением и наказывается штрафом в размере до 500 тыс. евро (§ 4 (2) NetzDG). По официальной статистике, в Германии 800 000 несовершеннолетних в возрасте от 10 до 18 лет уже подвергались оскорблениям или издевательствам в сети «Интернет»; более трети молодых людей считают оскорбления и систематические издевательства одним из самых серьезных рисков в Интернете. При этом наиболее серьезно страдают от кибермоббинга<sup>570</sup> молодые люди в возрасте от 15 до 16 лет<sup>571</sup>.

В Законе об административных правонарушениях (OWiG)<sup>572</sup> имеется ст. «§ 118 Преследование широкой общественности», согласно которой правонарушителем является тот, кто совершает грубое непристойное деяние, способное причинить неудобства или поставить под угрозу общество в целом, а также нарушить общественный порядок; при этом согласно § 118(2)

<sup>570</sup> Кибермоббинг – форма групповой онлайн-травли, включающая тактику слухов, дискредитации и запугивания. Отличается от кибербуллинга участием нескольких агрессоров, действующих сообща и целенаправленно. Кибермоббинг может происходить в социальных сетях и других онлайн-сообществах. Подробнее: Абраменко Е. В. Кибермоббинг как глобальная интернет-проблема в молодежной среде // *Primo Aspectu*. 2024. № 2 (58). С. 31-39.

<sup>571</sup> На страже интересов онлайн-пользователей: борьба с кибербуллингом в Германии. Сайт Федерального министерства иностранных дел Германии. URL: <https://germania-online.diplo.de/ru-dz-ru/gesellschaft/neuerordner/2419918-2419918> (дата обращения: 01.05.2025).

<sup>572</sup> Gesetz über Ordnungswidrigkeiten (OWiG). URL: <https://www.buzer.de/gesetz/5827/index.htm> (дата обращения: 01.05.2025).



административное правонарушение может быть наказано штрафом, если действие не может быть наказано в соответствии с другими правилами.

Согласно «§ 119 Грубо оскорбительные и оскорбительные действия» Закона об административных правонарушениях (OWiG) заключаются в публичной форме, подходящей для преследования других, или в грубо оскорбительной форме путем распространения или обнародования содержания ((3) § 11 УК Германии), предлагая, рекламируя возможность совершения сексуальных действий или делая заявления такого содержания ((1) § 119). Согласно (2) § 119 административным правонарушителем также является тот, кто предлагает, рекламирует средства или предметы, предназначенные для сексуального использования, публичными способами. Такое административное правонарушение может быть наказано штрафом в размере до 1000 евро в случаях, предусмотренных п. (1) § 119, и штрафом в размере до 10 000 евро в остальных случаях.

С развитием технологий и социальных сетей общение в Интернете стало неотъемлемой частью нашей жизни, однако с ростом популярности социальных сетей также увеличилось количество случаев, когда пользователи становятся жертвами оскорблений, угроз и клеветы.

Оскорбление – одно из самых распространенных правонарушений в Интернете. Оно может проявляться в разных формах: от резких комментариев и нецензурных выражений до распространения ложных обвинений, которые могут повредить репутации человека. Важно учитывать, что в Германии это деяние подпадает под действие уголовного законодательства.

В Уголовном кодексе Германии имеется конкретная статья, регулирующая оскорбления (Beleidigung). Так, § 185 Уголовного кодекса Германии (StGB) устанавливает, что любое оскорбление личности, в том числе публичное, является уголовным правонарушением. За такие действия предусмотрены штрафы или тюремное заключение сроком до одного года. В случае если оскорбление сопровождается угрозой насилия, наказание может быть более серьезным. Правонарушители, впервые совершившие это правонарушение, или в сети «Интернет», чаще всего получают денежные штрафы. Если потерпевший хочет

привлечь оскорбившего к ответственности, то он должен подать заявление в полицию в течение трех месяцев. Две статьи StGB посвящены сплетням (§ 186 Üble Nachrede) и клевете (§ 187 Verleumdung). Уточним, что перевод названия статей процитирован по научно-практическому комментарию и переводу текста закона, подготовленному П. В. Головненковым<sup>573</sup>. Так, согласно § 186 StGB «Сплетня (Üble Nachrede)» - это деяние лица, утверждающего в отношении другого лица сведения, которые носят неуважительный или унижающий достоинство такого лица характер, подлежит наказанию в случаях, когда данное лицо не смогло подтвердить подлинность сведений. Этой статьей предусмотрено наказание в виде денежного штрафа или лишения свободы до 1 года, а в случаях, когда распространение сведений проходило публично (в том числе с использованием сети «Интернет». — *Авт.*), то лишением свободы на срок до 2-х лет или денежным штрафом. Согласно § 187 «Клевета (Verleumdung)» отличается от «Сплетни (Üble Nachrede)» тем, что распространяются заведомо ложные сведения; за клевету предусмотрено наказание в виде лишения свободы до 2-х лет или штрафом, а в случае публичной клеветы (распространения клеветы неограниченному кругу лиц) предусмотрено наказание в виде лишения свободы на срок до 5 лет или штрафом. Следует уточнить, что если в сети «Интернет» пользователь скрывается за фальшивым именем или анонимным аккаунтом, то в случае юридического разбирательства его можно найти, особенно если оскорбления касаются конкретных людей или компаний, что упрощает задачу для следствия. Важно помнить, что правоохранительные органы могут использовать данные о пользователях, включая их IP-адреса, для идентификации.

Таким образом, законодательство Германии устанавливает уголовную и административную ответственность за распространение деструктивного для несовершеннолетних контента.

---

<sup>573</sup> Головненков П. В. Уголовное уложение Федеративной Республики Германия – Strafgesetzbuch (StGB). Научно-практический комментарий и перевод текста закона. Universitätsverlag Potsdam, 2021. С. 306.

Во Франции нет понятия административного правонарушения в российском понимании, однако административные санкции существуют (спору по ним подведомственны как общим, так и административным судам)<sup>574</sup>.

Нормами закона № 78-17 от 06.01.1978<sup>575</sup>, регламентирующего обработку данных, установлена уголовная ответственность лиц за изготовление, распространение незаконного контента, содержащего порнографию, жестокость, насилие и т. д., когда лицо, совершившее деяние, осознаёт, что такой контент будет доступен несовершеннолетним.

Статьей 222-37-1 УК Франции (Code penal)<sup>2</sup> предусмотрен запрет на вовлечение несовершеннолетнего лица в транспортировку, хранение, передачу (продажу) наркотических и психотропных веществ, в том числе с использованием сети «Интернет», за это деяние предусмотрен либо штраф до 150 тыс. евро, либо лишение свободы до 7 лет.

Раздел 5 Code penal (ст. 226-16 – 226-24), посвященный нарушениям прав человека в результате использования компьютерных файлов или их обработки, гармонизирован с нормами GDPR ЕС. Защита несовершеннолетних в этом разделе не имеет каких-либо особенностей от основных лиц, чьи права защищены этим разделом.

Интересной нормой является ст. 227-17 Code penal, согласно которой предусмотрена достаточно серьезная ответственность родителей несовершеннолетнего лица в случае, если их действие или бездействие повлекло причинение несовершеннолетнему лицу ущерб физическому, психическому, нравственному состоянию: наказание предусматривает лишение свободы до 2-х лет или штраф до 30 тыс. евро.

Также считаем важным отметить, что полиция Франции на региональном уровне в своей структуре имеет отделы, деятельность которых направлена на

<sup>574</sup> Les pouvoirs de l'administration dans le domaine des sanctions. Etude adoptée par l'Assemblée Générale du Conseil d'Etat le 8 décembre 1994, Paris, La Documentation française, coll. Les études du Conseil d'Etat, 1995; Талапина Э. В. Административное право Франции сегодня // Ежегодник сравнительного правоведения. 2004 // Общество сравнительного правоведения. М., 2005. С. 136-151.

<sup>575</sup> Loi № 78-17 du 6 janvier 1978 relative a l'informatique, aux fichiers et aux libertés. URL: [https://www.legifrance.gouv.fr/loda/article\\_lc/LEGIARTI000037822807/](https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037822807/) (дата обращения: 10.08.2025).

борьбу с преступлениями, совершаемыми с помощью сети «Интернет» и в том числе против несовершеннолетних лиц. Как отмечено в коллективной монографии под редакцией С. Е. Титор, «законодательство Франции содержит ряд специальных норм о защите несовершеннолетних от деструктивной информационной среды и данные законы устанавливают меры ответственности (преимущественно уголовной) при нарушении прав и законных интересов несовершеннолетних»<sup>576</sup>.

Закон № 2020-766 (Loi n°2020-766 du mercredi 24 juin 2020 visant à lutter contre les contenus haineux sur internet)<sup>577</sup>, который направлен на борьбу с ненавистническим контентом в сети «Интернет», направлен на усиление вклада цифровых операторов в борьбу с определенным явно ненавистническим контентом в сети «Интернет».

Закон изначально предполагал, чтобы сайты социальных сетей, работающие во Франции, удаляли оскорбительный контент в течение 24 часов после уведомления, в противном случае им грозит штраф в размере до 1,25 млн евро. Конкретный незаконный контент, связанный с детской порнографией и терроризмом, должен быть удален в течение 1 часа после обнаружения. Такие провайдеры могут также удалять контент до того, как он будет обнаружен, без каких-либо штрафов. Этот закон похож на принятый в 2017 году в Германии Закон об улучшении правоприменения в социальных сетях (NetzDG)<sup>578</sup>. Хотя ЕС попросил Францию отложить принятие законов до тех пор, пока не будет принят собственный Закон о цифровых услугах ЕС (Digital Services Act)<sup>579</sup>, Франция приняла собственную версию закона из-за более строгих законов против разжигания ненависти. Однако если обратиться к действующей редакции закона, то значительная часть статей будет исключена ввиду «[Положений, признанных

<sup>576</sup> Правовое регулирование защиты несовершеннолетних от деструктивной информационной среды : монография / Под общ. ред. С. Е. Титор. М. : РУСАИНС, 2025. С. 36-37.

<sup>577</sup> Loi n°2020-766 du mercredi 24 juin 2020 visant à lutter contre les contenus haineux sur internet (Publiée au Journal Officiel du jeudi 25 juin 2020). URL: <https://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSX1913052L> (дата обращения: 01.05.2025).

<sup>578</sup> Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) 2017. URL: <https://www.buzer.de/NetzDG.htm> (дата обращения: 01.05.2025).

<sup>579</sup> European Digital Services Act (DSA) (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC) (the DSA). URL: <http://eur-lex.europa.eu/> (дата обращения: 30.03.2025).

несоответствующими Конституции решением Конституционного совета № 2020-801 от 18 июня 2020 г.]]. Также отметим, что «Глава V: Повышение эффективности уголовного преследования в отношении авторов материалов, разжигающих ненависть, в Интернете (статьи 10–12)» рассматривает опять-таки уголовную ответственность, а не административную.

### **3.2. Общая характеристика административной ответственности за правонарушения в области информационной безопасности несовершеннолетних в российском сегменте сети «Интернет»**

Развитие и распространение информационно-телекоммуникационной сети «Интернет» предоставили возможность несовершеннолетним для непрерывного развития, самообучения, повышения квалификации, обретения полезных навыков, заведения новых друзей, ведь с психологической точки зрения коммуникации со сверстниками в раннем возрасте, будь то в офлайн- или онлайн-формате, положительно сказывается на развитии в физическом и духовном плане.

В условиях непрерывного совершенствования информационных и коммуникационных технологий и развития информационного общества человечество сталкивается с девиантными проявлениями в цифровой среде, которые зачастую носят деструктивный характер. Особенно этому влиянию в силу несформировавшейся психики и недостатка жизненного опыта подвержены несовершеннолетние граждане. При реализации политики в сфере применения информационных и коммуникационных технологий, наряду с обеспечением прав граждан на доступ к информации и обеспечением свободы выбора средств получения знаний при работе с информацией, нужно учитывать необходимость обеспечения государственной защиты интересов граждан в информационной сфере, в частности, обеспечения безопасной информационной среды для несовершеннолетних<sup>580</sup>. Ответственность за нарушения, носящие деструктивный

---

<sup>580</sup> Правовое регулирование защиты несовершеннолетних от деструктивной информационной среды : монография / Под общ. ред. С. Е. Титор. М. : РУСАИНС, 2025. С. 7.

характер, классифицируются различными статьями УК РФ<sup>581</sup> и КоАП РФ<sup>582</sup>. Несмотря на то, что сфера уголовной ответственности выходит за рамки диссертационного исследования, считаем важным для разграничения и наглядности видов ответственности перечислить статьи и УК РФ<sup>583</sup>, и КоАП РФ в исследуемой теме. Так, *уголовная ответственность в изучаемой сфере правоотношений предусмотрена следующими нормами УК РФ*: ст. 205.2; ст. 207.1; ст. 207.2; ст. 207.3; ст. 272; ст. 280; ст. 280.1; ст. 280.3; ст. 280.4; ст. 282; ст. 282.4; ст. 284.2; ст. 354; ст. 354.1. Анализируя нормы КоАП РФ, можем выделить следующие статьи, в которых содержатся правонарушения, совершенные с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», а также ответственность, предусмотренная за данные деяния. Так, *административная ответственность предусмотрена следующими составами Кодекса РФ об административных правонарушениях*: ст. 6.17; ст. 5.61; ст. 5.62; ст. 6.13; ст. 6.13.1; ст. 6.20; ст. 6.21; ст. 6.21.1; ст. 6.21.2; ст. 5.35. Вышесказанное наглядно показывает, что сфера информационной безопасности в целом и несовершеннолетних в частности регламентируется российским законодателем на высоком уровне, при этом большая часть деяний отнесены к уголовным деяниям, что подчеркивает их степень общественной опасности.

Рассмотрим более детально административное законодательство в исследуемой сфере отношений. Статья 6.17 КоАП РФ охватывает обязанности по защите несовершеннолетних от информации, способной нанести вред их здоровью и развитию. В этом контексте ключевым направлением является регулирование распространения информационной продукции и соблюдение установленных норм, направленных на защиту несовершеннолетних от деструктивного контента. Эта статья включает в себя ряд предписаний и требований, касающихся как физических, так и юридических лиц.

<sup>581</sup> Уголовный кодекс Российской Федерации" от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) // СЗ РФ. 1996. № 25. Ст. 2954; Российская газета. 25.04.2025. № 93.

<sup>582</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404.

<sup>583</sup> Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) // СЗ РФ. 1996. № 25. Ст. 2954; Российская газета. 25.04.2025. № 93.

Важно отметить, что административная ответственность, предусмотренная ст. 6.17, применяется в случаях, когда действия не подпадают под определение уголовно наказуемых деяний. В исключительных случаях, когда правонарушение может быть квалифицировано как более серьезное, применяются другие статьи КоАП РФ: например, 6.20 и 6.21<sup>584</sup>, которые устанавливают более строгие меры наказания. Такое разграничение позволяет адекватно реагировать на различные случаи нарушения законодательства о защите несовершеннолетних, при этом учитывая тяжесть проступка и последствия для несовершеннолетних.

Согласно ст. 6.17 КоАП РФ предусмотрена административная ответственность за несоблюдение требований распространения среди детей и подростков информационной продукции с признаками деструктивного контента; размещение (в том числе в сети «Интернет») на такой продукции объявления о привлечении несовершеннолетних к участию в создании информационной продукции с деструктивным контентом для несовершеннолетних; несоблюдение административных, технических, организационных средств обеспечения информационной безопасности детей и подростков в сети «Интернет» от деструктивного контента; размещение на информационной продукции для детей и подростков. Следовательно, объектом правонарушения выступают общественные отношения, связанные с защитой детей и подростков от деструктивного контента, в том числе размещенного непосредственно на информационной продукции. Отметим, что согласно Российскому агентству правовой и судебной информации средняя сумма штрафа за данное правонарушение по ст. 6.17 КоАП РФ составила 8 тыс. рублей<sup>585</sup>. Так, прокурор Невского района Санкт-Петербурга, действующий в защиту неопределенного круга лиц, обратился в Невский районный суд Санкт-Петербурга с административным исковым заявлением, в котором просит признать информацию, распространяемую на интернет-сайтах по сетевым адресам:

---

<sup>584</sup> «Статья 6.20. Изготовление юридическим лицом материалов или предметов с порнографическими изображениями несовершеннолетних и оборот таких материалов или предметов» и «Статья 6.21. Пропаганда нетрадиционных сексуальных отношений и (или) предпочтений, смены пола, отказа от деторождения».

<sup>585</sup> Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере : монография / Н. С. Волкова, А. А. Ефремов, С. М. Зырянов и др.; отв. ред. Л. К. Терещенко. М. : Инфотропик Медиа, 2024. 352 с. // СПС «КонсультантПлюс».

[https://www.\\*\\*\\*.me](https://www.***.me), [https://f.pornolomka\\*\\*\\*.com/](https://f.pornolomka***.com/) информацией, распространение которой на территории РФ запрещено. В ходе проверки проведен осмотр вышеуказанных интернет-сайтов. На интернет-ресурсе размещены в свободном доступе видеоизображения, демонстрирующие сцены половых актов, о чем свидетельствует копирование изображения, отображенного на экране монитора, при помощи клавиши «PrintScreen». Размещение на данном интернет-сайте видеоизображений наружных половых органов следует расценивать как информацию порнографического характера, действия владельцев интернет-сайта – как публичную демонстрацию порнографических материалов, поскольку она не имеет научного, медицинского или учебного предназначения, а осуществляется для удовлетворения сексуальных потребностей посетителей. Посещение данного сайта свободно для всех без исключения граждан, сайт не содержит ограничений к доступу по кругу лиц, в том числе в зависимости от возраста либо профессии. В силу изложенного информация, размещенная на сайтах [https://www.\\*\\*\\*.me](https://www.***.me), [https://f.pornolomka\\*\\*\\*.com/](https://f.pornolomka***.com/), является информацией, запрещенной для распространения как противоречащая законодательству РФ. На основании выявления данного факта Роскомнадзору согласно ч. 1, 2, 5 ст. 15.1 Закона № 149-ФЗ «Об информации»<sup>586</sup> следует внести сведения о данном сайте (страницы сайта) в сети «Интернет» в Единый реестр доменных имен и его блокировке.

Так, в 2021 г. к административной ответственности было привлечено юридическое лицо, осуществлявшее продажу футболок, товаров, надписи на которых содержали нецензурную брань, нецензурные слова и выражения. В процессе судебного разбирательства было установлено, что реализация указанного товара производится в свободной форме в торговом зале без каких-либо информационных обозначений возрастного ограничения. Судом было признано, что подобные действия являются нарушением Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»<sup>587</sup>, поскольку

<sup>586</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; СЗ РФ. 2024. № 48. Ст. 7218.

<sup>587</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.



нецензурная брань отнесена к информации, запрещенной для распространения среди детей, а информация, содержащая бранные слова и выражения, не относящиеся к нецензурной брани, является информацией, имеющей возрастные ограничения по распространению. Нарушение указанных требований и стало основанием для привлечения юридического лица к административной ответственности<sup>588</sup>.

Согласно ст. 6.17 КоАП РФ субъектами административной ответственности выступают физические, должностные, юридические лица, ИП. Также следует сказать, что правонарушение может быть совершено умышленно и по неосторожности. Иными словами, к административной ответственности могут быть привлечены как организации, так и индивидуальные предприниматели, что подчеркивает общую ответственность перед обществом за создание безопасной информационной среды. Процедура обжалования решений о привлечении к ответственности предусмотрена для граждан и организаций, которые считают, что их права были нарушены. Это позволяет создавать эффективную систему защиты, где каждая сторона может отстоять свою позицию в рамках действующего законодательства. Обжалование включает процесс подачи жалобы в вышестоящие инстанции, что позволяет избежать произвольности в применении административных мер и обеспечивает справедливое разбирательство.

Отметим, что поведение несовершеннолетних в сети «Интернет» требует постоянного мониторинга и адаптации правовых норм. Ключевым моментом в эффективности применения ст. 6.17 КоАП РФ является не только юридическая ответственность, но и просветительская работа с населением, направленная на формирование понимания важности защиты несовершеннолетних от потенциально вредного контента. Работы в этом направлении активизируются как государственными органами, так и некоммерческими организациями, что способствует более комплексному подходу к решению проблемы.

---

<sup>588</sup> Решение Московского городского суда от 15.11.2021 по делу № 7-17345/2021 О привлечении к ответственности по ч. 1 ст. 6.17 КоАП РФ за нарушение законодательства о защите детей от информации, причиняющей вред их здоровью и развитию // СПС «КонсультантПлюс».

В рамках административной ответственности, предусмотренной ст. 6.17, важно учитывать и культурные аспекты, касающиеся восприятия информации несовершеннолетними. Традиционные подходы к рейтингованию и классификации контента должны быть адаптированы к меняющимся реалиям современного мира, где информационные потоки становятся все более разнообразными и сложными. Поэтому соблюдение норм, установленных законом, требует от различных субъектов не только приверженности к правовым стандартам, но и активной позиции в распространении безопасных практик использования информационных технологий. Помимо этого стоит отметить, что система административных мер должна включать как проактивные, так и реактивные механизмы. Проактивные механизмы должны быть направлены на предотвращение распространения вредной информации, включая усиление контроля за контентом, в то время как реактивные механизмы должны обеспечивать ответ на уже произошедшие нарушения законодательства. Это требует комплексных усилий со стороны государственных и общественных структур, чтобы создать безопасную интернет-среду для несовершеннолетних.

Таким образом, ст. 6.17 КоАП РФ является значимым инструментом защиты прав несовершеннолетних, позволяющим адаптировать юридические меры к постоянно меняющемуся состоянию информационной безопасности в России. Установленные нормы и правила должны быть поддержаны адекватными мерами внедрения и контроля, чтобы обеспечить реальную защиту детской и подростковой аудитории и минимизировать риски, связанные с использованием сети «Интернет». В последние годы наблюдается рост правонарушений в области информационной безопасности, непосредственно затрагивающих несовершеннолетних. В Российской Федерации такие правонарушения проявляются в разнообразных формах, начиная от распространения вредоносного программного обеспечения и заканчивая кибербуллингом и распространением запрещенной информации. Важно отметить, что административная ответственность по КоАП РФ устанавливает ряд мер, направленных на пресечение таких деяний и защиту детей

в цифровом пространстве<sup>589</sup>. К числу основных правонарушений, с которыми сталкиваются несовершеннолетние, можно отнести распространение вредоносных вирусов, кражу личных данных и осуществление неправомерного доступа к информации. Например, в результате действий злоумышленников могут быть украдены банковские данные, что имеет серьезные последствия для финансовой безопасности не только отдельных граждан, но и общества в целом<sup>590</sup>. Способы совершения таких правонарушений разнообразны, и, как показала статистика, число случаев увеличивается: в 2020 году зафиксирован рост на 75,1 % по сравнению с предыдущим годом, что является тревожным сигналом для общества и правоохранительных органов.

Часть 1 ст. 5.61 КоАП РФ содержит официальное определение такому правонарушению, как «оскорбление», которое представляет собой «унижение чести и достоинства лица, выраженное в неприличной или иной противоречащей общепринятым нормам морали и нравственности форме»<sup>591</sup>. Оскорбление – одно из самых распространенных административных правонарушений. Так, за 2024 год по ст. 5.61 КоАП рассмотрено 18 237 дел, подвергнуто наказанию 14 903 (81,0 %) человек<sup>592</sup>. Цифровизация общественных отношений послужила основанием для внесения корректировок в данную статью, согласно которым в ч. 2 ст. 5.61 КоАП РФ установлена административная ответственность за оскорбление конкретного человека или неограниченного круга лиц, выраженное в форме, не соответствующей общепринятым нормам морали и нравственности<sup>593</sup>. Отметим, что квалифицирующим признаком правонарушения по этой статье КоАП РФ, влекущим ужесточение наказания, является использование сети «Интернет». Полномочия по возбуждению дел об административном правонарушении по ст.

<sup>589</sup> Прокуратура Саратовской области. URL: [https://epp.genproc.gov.ru/web/proc\\_64/mass-media/news?item=85499501](https://epp.genproc.gov.ru/web/proc_64/mass-media/news?item=85499501) (дата обращения: 01.05.2025).

<sup>590</sup> Преступления, совершаемые в сети «Интернет». URL: <https://prokuratura-zo-krd.ru/pravovoe-prosveshchenie/prestupleniya-sovershaemye-v-seti-internet-0> (дата обращения: 01.05.2025).

<sup>591</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404.

<sup>592</sup> Судебная статистика. Официальный сайт Агентства правовой информации. URL: <https://stat.api-пресс.рф/stats/adm/t/31/s/65> (дата обращения: 01.05.2025).

<sup>593</sup> Федеральный закон от 30 декабря 2020 г. № 513-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СЗ РФ. 2021. № 1 (часть I). Ст. 52.

5.61 КоАП РФ отнесены прокуратуре (ч. 1 ст. 28.4 КоАП РФ), а по рассмотрению дел – мировым судьям (абз. 6 ч. 3 ст. 23.1 КоАП РФ). Объективная сторона выражена понятиями «честь» и «достоинство», при этом «честь – внешняя оценка действий человека со стороны других лиц и общества, а достоинство выражается в личностных ценностях, формируемых из понимания своей значимости»<sup>594</sup>. Следовательно, унижение чести и достоинства – это отрицательная оценка личности в обобщенном виде, направленная на ее дискредитацию<sup>595</sup>. При этом непристойность формы высказывания является объективной стороной оскорбления<sup>596</sup> и оценивается судом<sup>597</sup>. Объективная сторона оскорбления заключается в действиях, которые унижают честь и достоинство определенного лица в неприличной форме (циничной, противоречащей установленным правилам поведения, требованиям общечеловеческой морали). При этом объективная сторона ст. 5.61 КоАП РФ может состоять в публикации оскорбления, в том числе в СМИ и в сети «Интернет». В разъяснениях высших судов имеется важный фактор разграничения правонарушений путем опубликования оскорбления в сети «Интернет», в том числе в социальных сетях: если оскорбление опубликовано в личном сообщении, то это деяние подлежит квалификации по ч. 1 ст. 5.61 КоАП РФ; а при условии опубликования оскорбления на публичных интернет-ресурсах (то есть доступных неограниченному кругу лиц) – по ч. 2 ст. 5.61 КоАП РФ<sup>598</sup>.

При этом следует учитывать, что правонарушения (ч. 1 ст. 5.61 КоАП РФ) с учетом незначительной степени общественной опасности и (или) вреда могут быть признаны малозначительными (ст. 2.9 КоАП РФ). Например, если оскорбление

<sup>594</sup> Аратова А. А. Квалификация оскорбления // Административное право и процесс. 2012. № 11. С. 60.

<sup>595</sup> Постатейный комментарий к Кодексу РФ об административных правонарушениях. Часть первая / Р. В. Амелин, А. В. Колоколов, М. Д. Колоколова и др.; под общ. ред. Л. В. Чистяковой. М.: ГроссМедиа, 2019. Т. 1. 1343 с.

<sup>596</sup> Необходимо иметь в виду, что «к нормам морали и нравственности» в философском понимании отнесены нормы поведения, обычаи, постоянно повторяемые в однотипных поступках множества людей и выступающие как нравственный закон, обязательный для каждого человека в отдельности. Они формируются из осмысления обобщенных моральных представлений «о добре и зле», «справедливости и своенравности», «добродетели и пороке» (Словарь по этике / Под ред. И. С. Кона. М.: Политиздат, 1984. С. 211).

<sup>597</sup> Решение Верховного суда Республики Алтай от 30.11.2017 № 21-81/2017 (Жалоба на определение об отказе в возбуждении дела об административном правонарушении по ст. 5.61 КоАП РФ (оскорбление) оставлена без изменения) // СПС «КонсультантПлюс».

<sup>598</sup> Решение Череповецкого городского суда Вологодской области от 22 декабря 2021 г. по делу № 12-1016/2021 «Об отмене актов о привлечении к административной ответственности по ст. 5.61 КоАП РФ (оскорбление)» // СПС «КонсультантПлюс».

было высказано в личной переписке в социальной сети с использованием сети «Интернет» при обмене оскорблениями обеими сторонами. Также отметим, что оскорбление нескольких лиц следует считать одним правонарушением (одним оскорбительным действием по ч. 2 ст. 5.61 КоАП РФ)<sup>599</sup>.

Для определения факта наличия или отсутствия оскорбительного содержания информации (материала) назначается судебная лингвистическая экспертиза, объектом которой являются тексты (на бумажном или электронном носителе), аудиозапись, видеозапись. Определяется наличие или отсутствие признаков публичности, наличия унижения чести и достоинства, формы высказывания и т. д.<sup>600</sup> При публичном оскорблении максимальный размер административного штрафа двукратно увеличен по сравнению с непубличным оскорблением и составляет для лиц: физических – 10 тыс. руб., должностных – 100 тыс. руб., юридических – 700 тыс. рублей. Кратное увеличение штрафа за публичные оскорбления обусловлены как анонимностью в онлайн-среде, так и значительной степенью распространения сети «Интернет», что влечет распространение контента с оскорблениями, которые, как отмечает Д. А. Новгородов, «ежеминутно наносят психологическую травму, оставаясь в большинстве случаев, по мнению отдельных исследователей, безнаказанными»<sup>601</sup>. Обозначим, что, исходя из п. 7 Постановления Пленума Верховного Суда РФ от 24 февраля 2005 г. № 3, достаточно даже одного лица, который узнал об оскорблении, размещенном на публичном ресурсе в сети «Интернет»<sup>602</sup>. Субъектами правонарушения по ст. 5.61 КоАП РФ являются лица физические, должностные, юридические, а субъективная сторона характеризуется умышленной виной. Также следует обозначить, что, исходя из практики правоприменения, разграничением правонарушений, совершенных публично в

<sup>599</sup> Обзор судебной практики Верховного Суда Российской Федерации № 2 (2021) (утв. Президиумом Верховного Суда РФ 30.06.2021) // Бюллетень Верховного Суда РФ № 10, октябрь. 2021.

<sup>600</sup> Стернин И. А., Антонова Л. Г., Карпов Д. Л., Шаманова М. В. Выявление признаков унижения чести, достоинства, умаления деловой репутации и оскорбления в лингвистической экспертизе текста. Ярославль, 2013. С. 28.

<sup>601</sup> Новгородов Д. А. Административные наказания за правонарушения, совершаемые посредством сети Интернет, и практика их применения // Научный портал МВД России. 2017. № 4. С. 11.

<sup>602</sup> Постановление Пленума Верховного Суда Российской Федерации от 24 февраля 2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» // СПС «КонсультантПлюс».

сети «Интернет», согласно ч. 3 ст. 20.1 КоАП РФ<sup>603</sup> и ч. 2 ст. 5.61 КоАП РФ выступает мотив правонарушения (как факультативный признак субъективной стороны). Иными словами, «суды оценивают характер высказываний как определяющих мотив правонарушителя»<sup>604</sup>. Например, диспозиция правонарушения по двум вышеуказанным статьям КоАП РФ имеет сходства, однако, как считают А. П. Стуканов и А. К. Соловьева, в случае деяния по ч. 3 ст. 20.1 КоАП РФ мотив в этом случае будет только хулиганский<sup>605</sup>.

Несомненный научный интерес для анализа представляют выявленные И. А. Зайцевым в ряде его научных работ<sup>606</sup> следующие две правовые проблемы:

1) в отличие от ст. 25 УПК РФ ст. 24.5 КоАП РФ не содержит такого основания исключения производства по делу об административном правонарушении, как примирение сторон. Во всех государствах, которые ранее были в составе СССР, имеется в КоАП институт примирения с потерпевшим, в том числе в Республике Беларусь (ст. 8.5)<sup>607</sup>, Республике Казахстан (ст. 64)<sup>608</sup> и Республике Узбекистан (ст. 21.2)<sup>609</sup>. На наш взгляд, с учетом позиции Президиума Верховного суда РФ (п. 50)<sup>610</sup>, это предложение обоснованное и позволило бы снизить нагрузку на судебную систему;

2) И. А. Зайцев предлагает: «с целью предупреждения лицами, достигшими

<sup>603</sup> «Распространение в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации, за исключением случаев, предусмотренных статьей 20.3.1 настоящего Кодекса, если эти действия не содержат уголовно наказуемого деяния». – Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404.

<sup>604</sup> Соловьева С. В. Механизм реализации административной ответственности за возбуждение ненависти или вражды // Право и практика. 2020. № 3. С. 72-77.

<sup>605</sup> Стуканов А. П., Соловьева А. К. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства: проблемы привлечения к административной ответственности // Законность. 2019. № 8. С. 29-33.

<sup>606</sup> Зайцев И. А. Административная ответственность за оскорбление, совершенное публично с использованием информационно-телекоммуникационных сетей, включая сеть Интернет // Административное право и процесс. 2023. № 8. С. 54-60.

<sup>607</sup> Кодекс Республики Беларусь об административных правонарушениях от 6 января 2021 г. № 91-З (с изм. и доп. по сост. на 20.02.2025) // Национальный правовой Интернет-портал Республики Беларусь. URL: <https://pravo.by/document/?guid=11031&p0=НК2100091> дата обращения: 01.05.2025).

<sup>608</sup> Кодекс Республики Казахстан от 5 июля 2014 года № 235-V ЗПК (с изм. и доп. по сост. на 09.04.2025 г.). URL: <https://adilet.zan.kz/rus/docs/K1400000235> (дата обращения: 01.05.2025).

<sup>609</sup> Кодекс Республики Узбекистан об административной ответственности (утв. Законом Республики Узбекистан от 22 сентября 1994 г. N 1015-XII (с изм. и доп. по сост. на 28.04.2025 г.). URL: <https://lex.uz/ru/docs/97661> (дата обращения: 01.05.2025).

<sup>610</sup> Обзор судебной практики ВС РФ № 2 (2021) (утв. Президиумом ВС РФ 30.06.2021) // СПС «КонсультантПлюс».

возраста 14 лет, совершения новых правонарушений (ч. 1 ст. 3.1 КоАП РФ), а также недопустимости использования сети «Интернет» для совершения оскорблений в подростково-молодежной среде, понизить возраст административной ответственности за оскорбление с 16 до 14 лет, внося соответствующие изменения в ст. 2.3 КоАП РФ»<sup>611</sup>.

Второе предложение И. А. Зайцев, безусловно, интересное, но в то же время и дискуссионное.

С одной стороны, вопросы снижения возраста до 14 лет действительно активно обсуждаются в научном сообществе длительное время<sup>612</sup>. Отметим, что согласно ст. 4.2 КоАП РФ к административной ответственности привлекаются лица, достигшие 14 лет за ряд правонарушений (в том числе за оскорбления (ст. 10.2 КоАП РФ)), при общем возрасте привлечения лиц к ответственности по КоАП РФ – с 16 лет. Так, по мнению Н.Е. Красновой, «необходимо снизить возраст административной ответственности несовершеннолетних, это также будет носить воспитательный характер»<sup>613</sup>. Как отмечают Е. В. Ильгова, А.И. Сметанникова, «несовершеннолетние в возрасте от 14 до 16 лет, совершившие административное правонарушение, уже способны отдавать себе отчет в неприемлемости своих поступков, однако остаются безнаказанными, что воспитывает в них чувство вседозволенности»<sup>614</sup>. Г. Г. Михалева отмечает, что не достигший 16 лет «правонарушитель не всегда в ответе за свое деяние, а это означает, что, в данном случае, принцип неотвратимости административной ответственности может быть не учтен»<sup>615</sup>. Дифференцированный подход предлагают А. В. Омельченко,

<sup>611</sup> Зайцев И. А. Административная ответственность за оскорбление, совершенное публично с использованием информационно-телекоммуникационных сетей, включая сеть Интернет // Административное право и процесс. 2023. № 8. С. 54-60.

<sup>612</sup> Куликов В. Почему предлагают снизить возраст наказания подростков в новом КоАП // Российская газета. Столичный выпуск. № 110 (7868). URL: <http://rg.ru/2019/05/22/pochemu-predlagaiut-snizit-vozrast-nakazaniia-podrostkov-v-novom-koap.html> (дата обращения: 01.05.2025); Шкагулов К. О. К вопросу о снижении возрастного порога для привлечения к административной ответственности // Молодой ученый. 2020. № 21(311). С. 418-421.

<sup>613</sup> Краснова Н. Е. Перспективы реформирования законодательства привлечения несовершеннолетних к административной ответственности // E-Scio. 2020. № 2 (41). С. 60-68.

<sup>614</sup> Ильгова Е. В., Сметанникова А. И. К вопросу о снижении возраста административной ответственности // Вестник Саратовской государственной юридической академии. 2018. № 5 (124). С. 58-61.

<sup>615</sup> Михалева Г. Г. Вопросы совершенствования административно-юрисдикционной деятельности полиции по привлечению несовершеннолетних к административной ответственности // Аграрное и земельное право. 2023. № 6 (222). С. 72-74.

А.А. Седова: «... альтернатива, которая предполагает административную ответственность физическим лицам с шестнадцати лет по общему правилу и с четырнадцати – за отдельные административные правонарушения»<sup>616</sup>. Схожей точки зрения придерживается и Г. Ю. Каримова, предлагая помимо снижения возраста за отдельные административные правонарушения также и «целесообразность создания нового раздела в КоАП РФ «Административная ответственность несовершеннолетних»<sup>617</sup>. Вопросы снижения возраста ответственности за правонарушения несовершеннолетних в России исследуются многими правоведами (например, такими как С. Б. Беликова, С. О. Туаева<sup>618</sup>, Т. А. Недоступенко<sup>619</sup>, М. А. Гезгиев<sup>620</sup> и др.).

Однако дискуссионным в анализируемом предложении И. А. Зайцева<sup>621</sup>, на наш субъективный взгляд, является следующее: самый главный критерий понижения возраста административной ответственности – это степень общественной опасности. В то же время, несмотря на актуальность обеспечения информационной безопасности несовершеннолетних в сети «Интернет», ч. 2 ст. 5.61 КоАП РФ не имеет настолько значимой степени общественной опасности, чтобы исключительно для этой части или статьи в целом вводить исключение в виде привлечения к административной ответственности с 14 лет. Для примера приведем, что ст. 15.27.1 КоАП РФ «Оказание финансовой поддержки терроризму, распространению оружия массового уничтожения» имеет наказание в виде административного штрафа для юридических лиц – от 10 млн до 60 млн руб. и, несомненно, степень общественной опасности намного выше, чем

<sup>616</sup> Омельченко А. В., Седова А. А. К вопросу о снижении возраста привлечения к административной ответственности // *Европейский юридический журнал*. 2023. № 37. С. 103-107.

<sup>617</sup> Каримова Г. Ю. Некоторые проблемные аспекты административной ответственности несовершеннолетних // *Евразийский юридический журнал*. 2021. № 4 (155). С. 119-120.

<sup>618</sup> Беликова С. Б., Туаева С. О. К вопросу о снижении возраста привлечения к административной ответственности // *Инновации. Наука. Образование*. 2021. № 29. С. 508-514.

<sup>619</sup> Недоступенко Т. А. Предупреждение противоправных действий со стороны несовершеннолетних и в отношении них: новые подходы и перспективы внедрения // *Проблемы в российском законодательстве*. 2021. Т. 14. № 4. С. 218-222.

<sup>620</sup> Гезгиев М. А. Ответственность несовершеннолетних за административные правонарушения // *Право и управление*. 2023. № 7. С. 298-302.

<sup>621</sup> Зайцев И. А. Административная ответственность за оскорбление, совершенное публично с использованием информационно-телекоммуникационных сетей, включая сеть Интернет // *Административное право и процесс*. 2023. № 8. С. 54-60.



рассматриваемый выше состав административного правонарушения. Также в главе 12 КоАП РФ «Административные правонарушения в области дорожного движения», на наш взгляд, имеют более высокую степень общественной опасности, чем правонарушения главы 6, поскольку транспортное средство уже представляет собой источник повышенной опасности.

Иными словами, целесообразней рассмотреть возможность либо по общему правилу снижать возраст привлечения к административной ответственности (с 14 лет), либо вводить дифференцированный подход в зависимости от степени общественной опасности. В этом контексте предлагаем обратиться к исследованию законопроектов по исследуемому вопросу.

Так, в 2014 году в Госдуму РФ был внесен законопроект, который предполагает снижение возраста (с 16 до 14 лет), с которого наступает ответственность за административные правонарушения<sup>622</sup>. Согласно пояснительной записке к нему законопроектом предлагается определить, что административная ответственность наступает для лиц с 14 лет. Авторы документа отмечают, что в возрасте от 14 до 16 лет ребенок уже отдает отчет своим поступкам, в состоянии оценить деструктивный характер своих действий, а также принять и оценить неблагоприятные последствия, наступающие в случае привлечения к уголовной ответственности; при этом принятие разработанного законопроекта не исключает применения комиссией по делам несовершеннолетних освобождения от административной ответственности с применением к ним меры воздействия, предусмотренной законодательством о защите прав несовершеннолетних<sup>623</sup>. Отметим, что законопроект был отклонен.

В 2019 году на официальном интернет-портале «Российской газеты» была размещена статья, согласно которой специальная правительственная группа должна представить концепцию нового Кодекса об административных правонарушениях; к

<sup>622</sup> Законопроект № 442510-6 «О внесении изменений в главу 2 Кодекса Российской Федерации об административных правонарушениях (в части уточнения возраста, по достижении которого наступает административная ответственность)» (17.06.2014 отклонен) // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество». URL: <https://sozd.duma.gov.ru/bill/442510-6> (дата обращения: 01.05.2025).

<sup>623</sup> Официальный сайт Уполномоченного по правам ребенка в ЯНАО. URL: <https://yamalchild.ru/?p=1683> (дата обращения: 01.05.2025).

работе тогда подключилось широкое научное сообщество, в том числе ведущие юридические вузы страны и представители науки, которые выдвинули предложение сократить до 14 лет возраст привлечения к административной ответственности за некоторые нарушения, например, мелкое хулиганство и побои. Одним из обоснований выступал тот фактор, что возрастная группа с 14 до 16 лет оказывается в некой «темной» зоне: трудные подростки уже способны совершать проступки, представляющие серьезную общественную опасность, но из сферы законодательства об административных правонарушениях они выпадают. Это подчас порождает у них чувство безнаказанности, а безнаказанность ведет к намного более страшным преступлениям<sup>624</sup>. Предложенные нормы по состоянию на ноябрь 2025 не получили законодательного закрепления.

Законопроектом № 1112019-7 в 2021 году предлагалось ввести понятие «уголовный проступок» при условии, что деяние совершено впервые; у лица, его совершившего, отсутствует судимость (неснятая/непогашенная) и отсутствует освобождение от уголовной ответственности в годовой период, который предшествовал моменту уголовного проступка<sup>625</sup>. При этом законопроектом устанавливалось, что общественная опасность уголовного проступка должна быть минимальной (малозначительной). Достаточно интересны в этом контексте научные работы, посвященные соотношению уголовного проступка, норм УК РФ и КоАП РФ, а также «перемещение законодателем запрещенных деяний<sup>626</sup> из УК РФ в КоАП и обратно»<sup>627</sup>. В этом случае возраст привлечения к административному проступку составлял бы 14 лет или же был возможен для обсуждения вариант

<sup>624</sup> Почему предлагают снизить возраст наказания подростков в новом КоАП (22.05.2019) // Интернет-портал «Российской газеты». URL: <https://rg.ru/2019/05/22/pochemu-predlagaiut-snizit-vozrast-nakazaniia-podrozkov-v-novom-koap.html> (дата обращения: 01.05.2025).

<sup>625</sup> Проект Федерального закона № 1112019-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с введением понятия уголовного проступка» // СПС «КонсультантПлюс».

<sup>626</sup> Номоконов В. А. «Криминализация» административного права или административный произвол криминализации? // Библиотека криминалиста. 2013. № 2. С. 208-213.

<sup>627</sup> Голикова А. В. Обоснование формирования перечня уголовных проступков посредством перераспределения деяний в КоАП РФ и УК РФ // Право и практика. 2020. № 3. С. 77-83; Леонов Р. А. Общественно опасные деяния (проступки), совершаемые лицами, не достигшими возраста уголовной ответственности (уголовно-правовой и криминологический аспекты) : дис. ... канд. юрид. наук. Саратов, 2011. 194 с.; Картавенко У. А. Квалификация мелкого хищения как административного правонарушения // Международный журнал гуманитарных и естественных наук. 2024. № 12-1 (99). С. 128-130.

переноса ряда статей из КоАП РФ в УК РФ с учетом, что за уголовный проступок возможна была бы ответственность (с учетом соответствующих изменений в ст. 20 УК РФ) с 14 лет. Однако законопроект отклонен.

Также в контексте нашего исследования считаем необходимым рассмотреть проект закона, предусматривающего модернизацию норм КоАП РФ и введения Процессуального кодекса РФ об административных правонарушениях<sup>628</sup>. Согласно ч. 1 ст. 2.6 проекта обновленного КоАП РФ была предусмотрена административная ответственность граждан, достигших к моменту совершения административного правонарушения возраста 16 лет. Иными словами, разработанный проект в редакции 2020 года не содержит ни понижения возраста, ни возрастной градации. Таким образом, наглядно проиллюстрировано, что научное сообщество в последнее десятилетие обосновывает необходимость снижения возраста привлечения к административной ответственности, но законодатель придерживается устойчивой позиции отклонения подобных проектов или научных предложений. В то же время мы согласны с тем, что в исследуемой нами сфере правовых отношений с учетом масштабного распространения сети «Интернет» и активным использованием его несовершеннолетними возникают правовые проблемы в пресечении, наказании и профилактике таких правонарушений, как оскорбление, запугивание, травля несовершеннолетних. Целенаправленные и систематические подобные деяния в отношении детей и подростков приводят к психическим и физическим проблемам несовершеннолетних, в том числе к самоубийствам или попыткам их совершения несовершеннолетними<sup>629</sup>.

Административная ответственность за действия, составляющие объективную сторону буллинга (травли), установлена ст. 5.61, 20.1 КоАП РФ<sup>630</sup>. Учитывая, что потерпевший (жертва буллинга) под воздействием агрессора также получает

<sup>628</sup> Проект Федерального закона «О введении в действие Кодекса Российской Федерации об административных правонарушениях и Процессуального кодекса Российской Федерации об административных правонарушениях» (подготовлен Минюстом России, ID проекта 02/04/01-20/00099058) // СПС «КонсультантПлюс».

<sup>629</sup> Подробнее: Карауш И. С., Куприянова И. Е., Кузнецова А. А. Кибербуллинг и суицидальное поведение подростков // Суицидология. 2020. Т. 11. № 1(38). С. 117-129.

<sup>630</sup> На основании ст. 20.1 КоАП РФ возможно привлечение к ответственности за мелкое хулиганство, то есть за распространение в информационно-телекоммуникационных сетях, в том числе в сети Интернет, информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность.

травмы психологического характера (неуверенность в себе, стыд и т. п.), последствия выражаются в нанесении морального вреда, который тоже подлежит компенсации. Моральный вред за подобные действия, совершенные лицами, не достигшими возраста 14 лет или в возрасте от 14 до 18 лет, не имеющими дохода, подлежит взысканию с их родителей либо других лиц, осуществляющих воспитательную деятельность на законных основаниях. Анонимность и простота размещения любого сообщения (комментария) приводит к тому, что распространение заведомо ложных сведений, порочащих честь и достоинство другого лица (в том числе и несовершеннолетнего), встречается достаточно часто<sup>631</sup>.

Стоит обратить внимание также на ст. 5.62 КоАП РФ<sup>632</sup>, которая содержит определение дискриминации: дискриминация представляет собой посягательство на права, свободы и интересы человека и гражданина, в том числе несовершеннолетнего, по ряду признаков (возраст, национальность, религия и т. д.). Дискриминация в отношении детей и подростков требует к себе особого внимания, ведь проблема дискриминации в сети «Интернет» стоит остро, особо часто она проявляется в среде именно несовершеннолетних, одни из которых, к сожалению, в силу отсутствия должного контроля со стороны родителей, а также правильного воспитания, используют нецензурную брань в отношении сверстников, распространяют информацию дискриминационного характера. Стоит отметить, что часто сами же несовершеннолетние становятся жертвами виртуальной дискриминации со стороны третьих лиц. Объективная сторона правонарушения по ст. 5.62 КоАП РФ выражается в действиях (либо в бездействии), нарушающих права, свободы и законные интересы человека и гражданина в зависимости от его пола, расы, цвета кожи, национальности, языка, происхождения, имущественного, семейного, социального и должностного положения, возраста, места жительства, отношения к религии, убеждений,

<sup>631</sup> Фетисов П. И. Преступления против личности, совершаемые с использованием информационно-телекоммуникационных технологий (включая сеть Интернет) // Известия Юго-Западного государственного университета. Серия: История и право. 2024. Т. 14. № 2. С. 119-130.

<sup>632</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404.

принадлежности или непринадлежности к общественным объединениям или каким-либо социальным группам. Для квалификации деяния как дискриминации достаточно факта нарушения права гражданина по признакам дискриминации, возможные последствия или их отсутствие не учитываются при квалификации данного деяния<sup>633</sup>. Согласно ст. 5.62 КоАП РФ субъектами правонарушения могут быть физические или юридические лица, совершившие деяние умышленно или по неосторожности.

Отметим, что глава 6 КоАП РФ включает в себя семь статей в сфере информационной безопасности несовершеннолетних в сети «Интернет». В целях упорядочивания и более детального раскрытия состава административных правонарушений по КоАП РФ в сфере информационной безопасности несовершеннолетних в сети «Интернет» представлены в Приложении Г.

Так, в ст. 6.13 КоАП РФ обозначены санкции за пропаганду наркотических средств, психотропных веществ и их прекурсоров, в том числе с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет». Это деяние влечет «административный штраф в размере от пяти тысяч до тридцати тысяч рублей; на должностных лиц – от пятидесяти тысяч до ста тысяч рублей; на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, – от пятидесяти тысяч до ста тысяч рублей либо административное приостановление деятельности на срок до девяноста суток; на юридических лиц – от одного миллиона до одного миллиона пятисот тысяч рублей либо административное приостановление деятельности на срок до девяноста суток»<sup>634</sup>. Также относительно недавно КоАП РФ был дополнен статьями, предусматривающими ответственность за оборот и пропаганду наркотических средств, психотропных веществ (ч. 1.1 ст. 6.13 КоАП РФ) и закиси азота (ст. 6.13.1 КоАП РФ) в целях охраны здоровья граждан, в том числе несовершеннолетних.

<sup>633</sup> Постатейный комментарий к Кодексу РФ об административных правонарушениях. Часть первая / Р. В. Амелин, А. В. Колоколов, М. Д. Колоколова и др.; под общ. ред. Л. В. Чистяковой. М. : ГроссМедиа, РОСБУХ, 2019. Т. 1. URL: <https://rulaws.ru> (дата обращения: 21.08.2025).

<sup>634</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404.

Под пропагандой<sup>635</sup> наркотических средств, психотропных веществ в сети «Интернет», являющейся квалифицированным составом вышеобозначенных статей КоАП РФ, Верховный Суд РФ<sup>636</sup> понимает деятельность в сети «Интернет» физических или юридических лиц, в результате которой распространяются сведения о запрещенных веществах и средствах, местах их приобретения, изготовления, употребления, создание побуждающего интереса и рекламы эффекта от их употребления. Срок давности привлечения к административной ответственности за совершение административного правонарушения, предусмотренного названной нормой, составляет один год и исчисляется со дня обнаружения административного правонарушения. Деяния, выраженные в том, что размещены материалы, пропагандирующие запрещенные вещества, в публичном доступе в сети «Интернет», подлежат квалификации по ч. 1.1 ст. 6.13 КоАП РФ. К примеру, размещение в социальной сети фотографии с одеждой, на которой есть изображение листьев конопли, может быть квалифицировано по ч. 1 ст. 6.13 КоАП РФ. Так, одна из пользователей социальных сетей разместила на своих страницах в «Инстаграм» и «ВКонтакте» фотографию своих новых носочков с нарисованными на них листьями конопли. Фото заметили сотрудники УМВД (подразделения наркоконтроля) и составили протоколы по упомянутой статье, по фотографии в «Инстаграм», и второй – по той же самой фотографии, размещенной во «ВКонтакте». В результате рассмотрения дела суд ограничился наложением штрафа в 4 тысячи рублей, ввиду того, что имелись смягчающие обстоятельства – признание вины, раскаяние в содеянном, молодой возраст<sup>637</sup>.

<sup>635</sup> «Под пропагандой в Большой советской энциклопедии понимается распространение политических, философских, научных, художественных и других взглядов и идей с целью их внедрения в общественное сознание и активизации массовой практической деятельности. Иными словами, отличие пропаганды от распространения какой-либо информации заключается в побудительном мотиве для осуществления какой-либо деятельности либо формирования каких-то установок». Цит. по: Пресняков М. В. Ментальные права: конституционное содержание и допустимость ограничений // Конституционное и муниципальное право. 2024. № 9. С. 45-53.

<sup>636</sup> Пункт 42 Обзора судебной практики Верховного Суда Российской Федерации № 4 (2021) применения судами общей юрисдикции ч. 1.1 ст. 6.13 КоАП РФ, утвержденного Президиумом Верховного Суда Российской Федерации 16.02.2022 // СПС «КонсультантПлюс».

<sup>637</sup> Селфи в одежде с «конопляным» принтом: осторожно штраф! // Официальный сайт Министерства внутренних дел Российской Федерации. URL: <https://238.56.мвд.рф/document/21128094> (дата обращения: 01.05.2025), а также Постановление Второго кассационного суда общей юрисдикции от 29 апреля 2022 г. № 16-2483/2022 «О привлечении к ответственности по ч. 1.1 ст. 6.13 КоАП РФ за пропаганду наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства»; Постановление Чусовского городского суда

На основании ст. 1 Федерального закона от 29.12.2020 № 472-ФЗ<sup>638</sup> в целях обеспечения безопасности жизни и здоровья населения с 1 января 2021 года на территории РФ ограничивается оборот закиси азота, так как закись азота является одурманивающим веществом («Закись азота (оксид азота (I), динитрогена оксид)» согласно перечню, утвержденному Постановлением Правительства РФ от 24.07.2021 № 1259)<sup>639</sup>. Согласно ст. 6.13.1 КоАП РФ правонарушением является пропаганда, в том числе в сети «Интернет», использования (потребления) закиси азота либо распространение информации о местах ее приобретения, изготовления, потребления, создание побуждающего интереса и рекламы эффекта от ее употребления<sup>640</sup>.

Административная ответственность согласно ст. 6.21 КоАП РФ предусмотрена за действия, выразившиеся в пропаганде нетрадиционных сексуальных отношений и (или) предпочтений, смены пола, так как эти действия рассматриваются как проявления запрещенной в РФ экстремистской организации ЛГБТ. Санкции ст. 6.21 КоАП РФ устанавливают административные штрафы на граждан – от 200 000 руб. до 400 000 руб., на должностных лиц – от 400 000 руб. до 800 000 руб., для юридических лиц – от 2 млн до 5 млн руб. или административным приостановлением деятельности на срок до 90 суток. Административная ответственность согласно ст. 6.21 КоАП РФ установлена за действия, в результате которых деструктивный контент, содержащий обоснование и (или) оправдание педофилии (действия сексуального характера с лицами, не достигшими 16 лет). Сама идеология педофилии и ее распространение, в том числе и среди несовершеннолетних с использованием сети «Интернет», является средством негативного воздействия на их благополучное развитие и нравственные установки. Законодатель, согласно п. 2 ст. 6.21.1, устанавливает следующую ответственность

---

Пермского края от 13 июля 2022 г. по делу N 5-194/2022 «О привлечении к административной ответственности по статье 6.13 КоАП РФ» // СПС «КонсультантПлюс».

<sup>638</sup> Федеральный закон от 29.12.2020 № 472-ФЗ «Об ограничении оборота закиси азота в Российской Федерации» // Российская газета. 11.01.2021. № 1.

<sup>639</sup> Постановление Правительства РФ от 24.07.2021 № 1259 «Об утверждении перечня одурманивающих веществ» // СЗ РФ. 2021. № 31. Ст. 5922.

<sup>640</sup> Постановления Советского районного суда города Липецка от 19 января 2022 г. по делу N 5-22/2022 и от 26 июля 2022 г. по делу № 5-321/2022 «О привлечении к административной ответственности по статье 6.13.1 КоАП РФ (пропаганда закиси азота)» // СПС «КонсультантПлюс».

за вышеобозначенные деяния: административный штраф: на граждан – от 400 000 руб. до 800 000 руб., на должностных лиц – от 800 000 руб. до 2 млн руб., для юридических лиц – от 4 млн до 10 млн руб. или приостановлением деятельности на срок до 90 суток.

В сфере информационной безопасности детей и подростков в сети «Интернет» административная ответственность не только регламентируется на законодательном уровне, но и активно исполняется на практике. Примером может служить активизация работы органов прокуратуры, которые регулярно публикуют данные о правонарушениях в сфере информационных технологий и принимают меры для их предотвращения. Важно, что такие меры охватывают не только криминальные аспекты, но также направлены на просвещение и информирование граждан о рисках и способах защиты<sup>641</sup>. Однако для достижения реальных результатов в защите несовершеннолетних необходимо продолжать мониторинг правонарушений, развивать образовательные программы и повышать уровень осведомленности среди всех участников процесса – от родителей и их детей до органов власти и правоохранительных структур.

Вопросы безопасности несовершеннолетних в Интернете становятся все более актуальными в условиях современного цифрового мира. Социальные сети, онлайн-игры и различные платформы открывают множество возможностей, однако вместе с тем представляют существенные риски, которые могут угрожать безопасности несовершеннолетних. Роль родителей в этом контексте является ключевой, поскольку именно они несут ответственность за защиту своих детей от возможных угроз в цифровой сфере.

Концепция административной ответственности за правонарушения в области информационной безопасности, касающиеся несовершеннолетних, является неотъемлемой частью правовой системы России. На фоне динамичного развития цифровых технологий и возрастания уязвимости несовершеннолетних в Интернете

---

<sup>641</sup> Преступления, совершаемые в сети «Интернет» / Прокуратура... : сайт. URL: <https://prokuratura-zo-krd.ru/pravovoe-prosveshchenie/prestupleniya-sovershaemye-v-seti-internet-0> (дата обращения: 01.05.2025).



необходима систематизация законодательства, направленного на защиту этой категории пользователей от различных форм киберугроз и правонарушений.

В русле нашего исследования также представляет интерес ст. 19.7.10-4 КоАП РФ, которая устанавливает административную ответственность владельцев социальных сетей, если они не выполняют предписания Роскомнадзора по мониторингу деструктивного контента в сети «Интернет» и уведомления о таком контенте Роскомнадзора. Данное деяние влечет административный штраф: на граждан – от 100 000 до 200 000 руб.; на должностных лиц – от 500 000 до 800 000 руб.; на юридических лиц – от 4 млн до 6 млн рублей. В целом по этой норме, введенной в 2023 году, на сегодня отсутствует судебная практика или спорные правовые ситуации.

Напомним: в предыдущей главе нами была обозначена правовая проблема, что в РФ отсутствует правовой механизм контроля (надзора) возрастного критерия при регистрации в социальных сетях несовершеннолетних граждан, в результате чего социальные сети, например, «ВКонтакте», не проверяет и не несет ответственность за достоверность данных, указанных при регистрации, в том числе за сведения о возрасте лица, которое регистрируется, то есть не обеспечивает информационную безопасность несовершеннолетнего. В результате нами было предложено дополнить Закон об информации № 149-ФЗ<sup>642</sup> статьей 10.8, в которой кроме обязанности владельца социальной сети также предусмотрена административная ответственность. Поэтому в продолжение реализации данного научного тезиса нами предлагается дополнить КоАП РФ статьей 6.17.1 (см. ее текст в Приложении Д), которая устанавливает административную ответственность за неисполнение владельцем социальной сети обязанности по идентификации и (или) аутентификации достижения пользователем 14 лет при регистрации, за исключением случаев регистрации в государственных и (или) муниципальных образовательных социальных сетях, регистрация в которых разрешена с 6,6 лет с

---

<sup>642</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; СЗ РФ. 2024. № 48. Ст. 7218.

согласия родителей (законных представителей) регистрируемого несовершеннолетнего лица.

Роль родителей в обеспечении безопасности детей в Интернете не может быть переоценена. Они должны не только контролировать доступ несовершеннолетних к интернет-ресурсам, но и активно участвовать в формировании у них навыков безопасного онлайн-поведения. Обсуждение с детьми возможных рисков, связанных с использованием сети «Интернет», а также обучение их критическому восприятию информации являются важными шагами на пути к созданию безопасного интернет-пространства. Следует отметить, что ст. 5.35 КоАП РФ предусмотрена административная ответственность за неисполнение родителями или иными законными представителями малолетних и подростков обязанностей по содержанию и воспитанию несовершеннолетних. Однако взаимодействие несовершеннолетних с деструктивным контентом в сети «Интернет» осуществляется в том числе и в результате попустительства со стороны их родителей (законных представителей). Так, родители (законные представители) сами предоставляют доступ несовершеннолетним к цифровым платформам, не предназначенным для несовершеннолетних; не проводят предусмотренный для граждан в соответствии со ст. 21 Федерального закона от 29 декабря 2010 г. № 436-ФЗ<sup>643</sup> контроль за соблюдением требований данного закона проводить мониторинг оборота информационной продукции и доступа своих детей к информации. Родителями (законными представителями) не устанавливается или не используется «родительский контроль» на технических средствах с доступом в сеть «Интернет»; не проводятся воспитательные, обучающие беседы с разъяснением, какой информации следует избегать в сети «Интернет», о каких деструктивных сообществах и пользователях, пишущих несовершеннолетним, следует сразу сообщать родителям. К сожалению, привести статистику по ст. 5.35 КоАП РФ не представляется возможным, так как статистика МВД по рассматриваемой статье не публикуется, поскольку привлечение к административной ответственности по ст.

<sup>643</sup> Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48; СЗ РФ. 2024. № 49 (часть IV). Ст. 7429.

5.35 КоАП РФ находится в компетенции территориальных комиссий по делам несовершеннолетних и защите их прав. Но санкция по ч. 1 ст. 5.35 достаточно наглядна: предупреждение или штраф в размере от 500 до 2000 рублей, что, несомненно, является ничтожно малым размером штрафа, если учесть, что сумма МРОТ по состоянию на 2025 год – 22 440 рублей.

Проиллюстрируем вышесказанное примером из судебной практики. Так, две несовершеннолетние девочки (ФИО1 и ФИО2) осуществляли звонки и сообщения третьей несовершеннолетней девочке (ФИО3) с целью вынуждения ее путем запугивания совершать определенные действия, связанные с самоповреждением. В результате рассмотрения данного административного дела комиссия по делам несовершеннолетних и защите их прав привлекла родителя ФИО1 по ст. 5.35 КоАП РФ и вынесла предупреждение, ввиду отсутствия контроля родителей за осуществлением досуга своего ребенка<sup>644</sup>. Несомненно, что с учетом ментально-психологических и возможных физических повреждений ФИО3 наказание по рассмотренному примеру крайне незначительное и не служит профилактическим целям недопущения подобных правонарушений среди малолетних и подростков.

Как мы считаем, следует учесть, что размер административного штрафа по ч. 1 ст. 5.35 КоАП РФ был неизменен с 2007 года до 31.07.2025, однако увеличение административного штрафа с «от 100 до 500 руб.» на «от 500 до 2000 руб.» требует и дальнейшего кратного увеличения.

Далее, в векторе нашего исследования и предложений в части возрастного критерия для ограничения регистрации несовершеннолетних в социальных сетях (предложенное нами в данном диссертационном исследовании дополнение в Закон об информации № 149-ФЗ статьей 10.8), считаем целесообразным дополнить ст. 5.35 «Неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по содержанию и воспитанию несовершеннолетних» КоАП РФ<sup>645</sup> частями 4 и 5, устанавливающими

<sup>644</sup> Решение № 12-115/2017 от 26 апреля 2017 г. по делу № 12-115/2017 Ленинского районного суда г. Саратова. URL: <https://actofact.ru/case-64RS0046-12-115-2017-2017-04-03-1-1/> (дата обращения: 01.05.2025).

<sup>645</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404.

ответственность родителей (законных представителей) малолетних и подростков за выявленный факт регистрации детей в социальных сетях: как сам факт непосредственно регистрации детей в социальных сетях родителями, предоставления документов (СНИЛС, паспортные данные, биометрические данные, номер телефона, которые зарегистрированы на совершеннолетнее лицо и т. д.), так и факт допущения родителями регистрации малолетнего ребенка в социальной сети как неисполнение родителями (законными представителями) своих обязанностей по воспитанию детей.

Отметим, что специальный мониторинг не предусмотрен. Предложение данной статьи является коррелирующей мерой со статьей об административной ответственности непосредственно социальных сетей (10.8). Например, если выявлен факт регистрации лица младше 14 лет – малолетнего, то платформа предоставляет данные, согласно которым регистрация происходила совершеннолетнего лица, что подтверждается его предъявленными данными. И при выявлении факта, что родители зарегистрировали ребенка с использованием подложных (не принадлежащих ему данных) – наступает их ответственность. Может возникнуть вопрос: почему мы рассматриваем ответственность именно родителей (законных представителей), а не любого лица? По сути, почти все регистрации в сети «Интернет» связаны с кодом, который приходит по sms указанного при регистрации номера телефона. Но уже принят закон<sup>646</sup>, вступивший силу с 01.06.2025, согласно которому законодательно запрещено передавать свои sim-карты лицам, которые не являются близкими родственниками.

Приведем обоснования предложенного нами размера штрафа в ч. 4 и ч. 5 ст. 5.35 КоАП РФ. Так, при изучении составов правонарушений в сфере информационной безопасности несовершеннолетних, а также в целом с использованием сети «Интернет» и размеров административного штрафа, предусмотренного по ним, мы рассмотрели размеры административных штрафов

---

<sup>646</sup> Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 01.04.2025 (дата обращения: 21.08.2025).

ст. 5.61, ст. 5.62, ч. 1.1 ст. 6.13, ст. 6.13.1, ст. 6.17, ч. 3 ст. 6.21, ч. 2 ст. 6.21.1, ч. 2 ст. 6.21.2, ст. 13.49, ст. 13.50 КоАП РФ в отношении граждан (Приложение Е).

При анализе представленных в приложении размеров административных штрафов можно сделать вывод, что в действующей редакции КоАП РФ в исследуемой сфере правоотношений предусмотрен административный штраф от 1000 до 800 000 рублей. Следует уточнить, что размер административного штрафа сильно коррелирует с годом введения наказания или годом внесения изменений: так, за 2023 год отсутствует размер штрафа менее 50 000 рублей.

Разумеется, размер административного штрафа будет связан со следующим:

- 1) степень общественной опасности деяния;
- 2) субъект правонарушения;
- 3) первичность или повторность свершения правонарушения.

Анализ показывает, что минимальный штраф предусмотрен за такие правонарушения, как дискриминация, пропаганда запрещенных веществ и закиси азота, а также неисполнение родителями малолетних и подростков обязанностей по их воспитанию. То есть эти нормы обусловлены профилактическими целями либо же защитой чести и достоинства лица. Так, пропаганда смены пола, нетрадиционных сексуальных отношений, отказа от деторождения, педофилии, распространения деструктивного контента, содержащего оправдания подобных отклонений, наказываются уже штрафами от 100 000 до 800 000 руб., что подчеркивает принципиальную позицию законодателя по пресечению подобных правонарушений. Следует обозначить, что если субъект правонарушения – владелец социальных сетей, то согласно санкциям ст. 13.41 и ст. 19.7.10-4: минимальный штраф от 50 000, максимальный до 200 000 руб. на гражданина; если же родители или иные законные представители – то размер штрафа по ст. 5.35 КоАП РФ крайне незначителен и составляет от 500 до 2000 руб., что делает данный специальный субъект правоотношений потенциально более девиантным, так как административные санкции не служат предупреждающим (профилактическим) целям, что не соответствует ч. 1 ст. 3.1 КоАП РФ.

Степень общественной опасности по предлагаемому нами составу правонарушения (ч. 4 и ч. 5 ст. 5.35) в сравнении с похожими составами

заключается в том, что при неправомерном доступе малолетнего к социальным сетям, в силу возраста, умственного и психического уровня развития, данное лицо находится в опасности от воздействия информации, которая деструктивно влияет или может повлиять на жизнь, здоровье, развитие малолетнего лица. В связи с этим считаем возможным предложить размер административного штрафа от десяти тысяч рублей до пятидесяти тысяч рублей.

В отношении нормы ч. 4–5 ст. 5.35 КоАП РФ не предусмотрен специальный мониторинг. Предложенное ч. 4–5 ст. 5.35 КоАП РФ является коррелирующей мерой со статьей об административной ответственности непосредственно социальных сетей (6.17.1 КоАП РФ). Например, выявлен факт регистрации малолетнего ребенка в социальной сети в Интернете, при этом владелец социальной сети предоставляет данные, согласно которым происходила регистрация совершеннолетнего лица, что подтверждается его персональными данными. И при выявлении факта, что родители зарегистрировали малолетнего ребенка с использованием подложных (не принадлежащих ему данных) – наступает их административная ответственность. Следует обозначить, что нами предлагается ответственность именно родителей (законных представителей), а не любого лица ввиду следующего: 1) по сути, почти все регистрации связаны с кодом, который приходит по sms указанного при регистрации номера телефона; 2) согласно нормам закона от 01.04.2025 № 41-ФЗ<sup>647</sup> законодательно запрещено передавать свои sim-карты лицам, которые не являются близкими родственниками.

В результате анализа административной ответственности в сфере информационного обеспечения несовершеннолетних в сети «Интернет» можно сказать, что российское законодательство в этой сфере активно развивается, вводятся новые составы правонарушений для пресечения распространения деструктивного контента для малолетних и подростков в онлайн-среде.

---

<sup>647</sup> Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2025. № 14. Ст. 1574.

В сфере информационной безопасности детей и подростков в сети «Интернет» КоАП РФ предусматривает составы административного правонарушения, в которых объектом правонарушений выступают общественные отношения, связанные с защитой малолетних и подростков от деструктивного контента в сети «Интернет», а также общественные отношения в области защиты их прав и законных интересов, защиты их здоровья, морали и нравственности, в том числе в сфере информационной безопасности в сети «Интернет».

Объективные стороны правонарушений составляют деяния согласно ст. 6.17, 5.61, 5.62, 6.13, 6.13.1, 6.20, 6.21, 6.21.1, 6.21.2, 5.35, 19.7.10-4 КоАП РФ.

Субъектами правонарушений по перечисленным статьям (за исключением ст. 6.20 КоАП РФ, где субъектами являются только юридические лица) являются граждане; должностные лица субъектами выступают по ст. 6.17, 5.61, 6.13, 6.13.1, 6.21, 6.21.1, 6.21.2 КоАП РФ; юридические лица субъектами правоотношений выступают по ст. 6.17, 5.61, 5.62, 6.13, 6.13.1, 6.20, 6.21, 6.21.1, 6.21.2 КоАП РФ; индивидуальные предприниматели субъектами правоотношений выступают по ст. 6.17, 6.13, 6.13.1 КоАП РФ; иностранные граждане, лица без гражданства выступают субъектами по ст. 6.13, 6.21, 6.21.1, 6.21.2 КоАП РФ; специальными субъектами правоотношений являются родители и иные законные представители несовершеннолетнего (ст. 5.35), владельцы социальной сети (ст. 19.7.10-4). Субъективная сторона правоотношений по ст. 6.17, 5.62, 6.13, 6.21.2, 5.35, 19.7.10-4 КоАП РФ может быть выражена как умышленной формой вины, так и по неосторожности; по ст. 5.61, 6.13.1, 6.20, 6.21, 6.21.1 возможна только умышленная форма вины.

В условиях стремительного развития цифровых технологий и увеличения времени, проводимого несовершеннолетними в Интернете, необходимость защиты их прав и интересов становится особенно актуальной.

Выводы по главе 3 диссертационного исследования.

1. В главе рассмотрены правонарушения и мера ответственности в сфере информационной безопасности несовершеннолетних и в сети «Интернет» по российскому и зарубежному законодательствам.

2. В то же время в зарубежных государствах, в отличие от российского законодательства, предусмотрена мера юридической ответственности (в виде штрафов) цифровых платформ, например, за деяния при идентификации возраста пользователя.

3. Отличительной чертой зарубежного законодательства в исследуемой теме является достаточно проработанный подход к обеспечению информационной безопасности несовершеннолетних в сети «Интернет», например, выделение таких составов противоправных деяний, как кибербуллинг, киберпреследования (Австралия). Так, российское законодательство не выделяет отдельно такое противоправное деяние, как кибербуллинг (то есть «травля в сети «Интернет»»), привлекая за подобные действия лицо, достигшее 16-летнего возраста либо к административной ответственности за действия, установленные ст. 5.61, 20.1 КоАП РФ<sup>648</sup>, либо к уголовной ответственности в соответствии со ст. 128.1, 213 УК РФ<sup>649</sup>. Несомненно, что выделение данного действия в отдельный административный состав – дискуссионное, но интересное, с учетом его систематического и деструктивного влияния на здоровье и развитие несовершеннолетнего.

4. В диссертации проведено исследование научных трудов, посвященных вопросу снижения возраста административной ответственности в России, законопроектов и их обсуждений по этому вопросу, зарубежное законодательство.

Можно сказать, что в научном сообществе предлагается: 1) либо полное снижение возраста административной ответственности с 16 до 14 лет; 2) либо снижение исключительно по отдельному составу правонарушений (как правило, в рамках темы исследования научной статьи, монографии, диссертации лица, предложившего снижение возраста административной ответственности); 3) либо предлагается дифференцированный подход (административная ответственность по общему правилу – с 16 лет, за отдельные административные правонарушения – с 14 лет). Предложения авторов-правоведов по этому вопросу были

<sup>648</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1; СЗ РФ. 2005. № 6. Ст. 404.

<sup>649</sup> Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) // СЗ РФ. 1996. № 25. Ст. 2954; Российская газета. 25.04.2025. № 93.



проанализированными нами с учетом степени общественной опасности в административном праве и историй рассмотрения законопроектов по внесению изменений в ст. 2.3 КоАП РФ. В исследовании проиллюстрировано, что научное сообщество в последнее десятилетие обосновывает необходимость снижения возраста привлечения к административной ответственности, но законодатель придерживается устойчивой позиции отклонения подобных проектов или научных предложений. В данном случае мы придерживаемся позиции законодателя.

5. В главе были проанализированы составы административных правонарушений в сфере информационной безопасности малолетних детей и подростков в сети «Интернет» и рассмотрены их особенности, а также проанализированы наказания за нарушения правонарушений в исследуемой теме. Несомненно, что российское законодательство направлено на административно-правовую защиту морально-нравственных качеств малолетних детей и подростков, выделяя несовершеннолетних как специальный объект противоправных посягательств и ужесточая санкции при совершении правонарушений в отношении несовершеннолетних и с использованием сети «Интернет».

6. В предыдущей главе нами была обозначена правовая проблема, что в Российской Федерации отсутствует правовой механизм контроля (надзора) возрастного критерия при регистрации в социальных сетях несовершеннолетних граждан, в результате чего социальные сети, например, «ВКонтакте», не проверяет и не несет ответственность за достоверность данных, указанных при регистрации, в том числе за сведения о возрасте лица, которое регистрируется, то есть не обеспечивает информационную безопасность несовершеннолетнего лица. В результате нами было предложено дополнить Закон об информации № 149-ФЗ<sup>650</sup> ст. 10.8, в которой кроме обязанности владельца социальной сети по проверке возраста пользователей при регистрации, также предусмотрена административная ответственность. Поэтому, в продолжение реализации этого научного тезиса, нами предлагается дополнить КоАП РФ ст. 6.17.1 в целях выделения нового состава

<sup>650</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448; СЗ РФ. 2024. № 48. Ст. 7218.

административного правонарушения, в котором: объектом правонарушения являются общественные отношения в сфере информационной безопасности несовершеннолетних лиц в сети «Интернет»; объективная сторона представлена регистрацией пользователя социальной сети в информационно-телекоммуникационной сети «Интернет» без идентификации и (или) без аутентификации возраста пользователя; ст. 6.17.1 выделяются специальные субъекты правоотношений, к которым относятся владельцы социальной сети; субъективная сторона представлена умышленной формой вины.

7. В векторе нашего исследования и предложений в части возрастного критерия для ограничения регистрации несовершеннолетних в социальных сетях считаем целесообразным дополнить ст. 5.35 КоАП РФ частью 4 и частью 5 в части установления административной ответственности родителей или иных законных представителей несовершеннолетних за использование недостоверных данных при регистрации малолетних детей в социальной сети.

8. В отношении нормы ч. 4–5 ст. 5.35 КоАП РФ не предусмотрен специальный мониторинг, так как предложенные ч. 4–5 ст. 5.35 КоАП РФ являются коррелирующей мерой со статьей об административной ответственности непосредственно владельцев социальных сетей (ст. 6.17.1 КоАП РФ).

## ЗАКЛЮЧЕНИЕ

Данное диссертационное исследование посвящено административно-правовому обеспечению информационной безопасности несовершеннолетних в сети «Интернет». В результате исследования все поставленные задачи успешно решены, цель исследования достигнута:

– при правовом анализе понятия «несовершеннолетний» с терминами «ребенок» и «подросток» юридической науке и законодательстве, как российском, так и зарубежных государств, в которых отсутствует единообразный подход к понятиям «ребенок (дети)», «подросток», «несовершеннолетний». В результате проведенного правового анализа выявлено, что термин «ребенок (дети)» является, с одной стороны, межотраслевым и декларационным, «рамочным», с другой стороны, имеет значение родственной (кровной, генетической) связи и (или) психологического проявления. Динамичное правовое положение «несовершеннолетних» создает основу для введения понятия «малолетний ребенок» (от 0 до 14 лет) и «подросток» (от 14 до 18 лет). Подростковый возраст, в отличие от детей категории «малолетние», характеризуется быстрыми физическими, когнитивными и социальными изменениями, в том числе половым и репродуктивным созревaniem; постепенным формированием дееспособности, связанной с реализацией прав и обязанностей, требующих новых знаний и навыков, способности нести правовую ответственность. Если правовое положение несовершеннолетних (малолетних) базируется на максимальной защите их прав и интересов ввиду их физиологической и социально-психологической беспомощности (недееспособности), то подростки уже отличаются частичной дееспособностью и деликтоспособностью. Таким образом, в результате исследования понятия «несовершеннолетний» в юридической науке, законодательстве РФ и зарубежных государств, соотношения понятия «несовершеннолетний» с терминами «ребенок» и «подросток» нами предложены авторские понятия «малолетний ребенок» и «подросток».

Согласно результатам проведенного исследования предложена и обоснована градация возрастных групп в рамках общего понятия «несовершеннолетний»; на основе проведенного анализа российского законодательства предложена классификация субъектов ответственности в административном праве:

- лица от 0 до 6,6 лет – не имеют дееспособности и не подлежат ответственности;
- лица с 6,6 до 14 лет – имеют частичную дееспособность и не подлежат ответственности, за исключением случаев, предусмотренных законодательством;
- лица с 14 до 16 лет – имеют ограниченную дееспособность и подлежат юридической ответственности, но осуществляют свои права и обязанности в большем объеме, чем предыдущие группы – российский законодатель эту возрастную категорию наделяет правом получения паспорта гражданина, осуществление различных действий с согласия законного представителя;
- лица с 16 до 18 лет – подлежат административной ответственности.

Следовательно, разграничение в российском праве понятия «несовершеннолетний» на «малолетний ребенок» и «подросток» позволяет унифицировать подход к вышеуказанным понятиям во всех областях права России. Мы группируем в изучаемой сфере лиц с 14 до 18 лет, объединяя их термином «подростки», который предлагается использовать в сфере информационной безопасности несовершеннолетних в сети «Интернет», а именно в правовом механизме подтверждения возраста лиц при регистрации лиц в социальных сетях в сети «Интернет». В качестве обоснования классификации несовершеннолетних в контексте информационной безопасности в сети «Интернет» обозначим возрастнопсихологический подход к оценке вредоносного воздействия на них контента. Так, в классификации несовершеннолетних на малолетних детей и подростков акцент направлен именно на потребление информации (информационной продукции): 1) малолетний ребенок в силу детской психики и еще неспособности к критическому мышлению нуждается либо в максимальной фильтрации информации, либо к ограничению доступа к деструктивному для него контенту в силу возрастных особенностей, то есть в максимальном участии его родителей (законных

представителей), административных органов публичной власти, общественных организаций; иначе самостоятельное потребление информации может нанести вред не только здоровью и развитию малолетнего ребенка, но и его жизни; 2) подросток уже частично сам способен самостоятельно потреблять информацию без ущерба его здоровью, развитию и, тем более, его жизни;

– в результате изучения правовых характеристик информации, причиняющей вред здоровью и развитию несовершеннолетних с помощью сети «Интернет», в российском и зарубежных законодательствах, следует сделать вывод, что в Российской Федерации и зарубежных государствах отсутствует единообразное закрепление в нормативных правовых актах определений «информации, причиняющей вред их здоровью и развитию», «вредоносного онлайн-содержания», «деструктивного контента» и правовое регулирование ограничения их распространения, а основными механизмами защиты детей от вредоносного контента являются фильтрация и возрастная категоризация.

В результате проведенного анализа отечественного законодательства предлагается дополнить текст, в том числе и название Закона № 436-ФЗ, новым объектом правовой охраны – «жизнь», которому может быть причинен вред от информации наравне со здоровьем и развитием несовершеннолетнего лица. Обоснована целесообразность изложения названия Федерального закона от 29.12.2010 № 436-ФЗ в следующем виде: «О защите детей от информации, причиняющей вред их *жизни*, здоровью и развитию».

Согласно результату детального анализа российского и зарубежного законодательства в части определения понятий и видов деструктивного контента разработана авторская классификация контента, наносящего вред жизни, здоровью и развитию несовершеннолетнего (деструктивного контента) в сети «Интернет»:

1) *незаконный (запрещенный) контент международного уровня*, представленный общепринятым противоправным контентом и включающим в себя информацию, содержащую детскую порнографию; информацию, которая склоняет к терроризму несовершеннолетних лиц и т. д.;

2) *незаконный (запрещенный или ограниченный) контент национального, наднационального уровня*, представленный противоправной информацией, распространение которой, в том числе в сети «Интернет», запрещено согласно национальным законодательствам и (или) наднациональным законодательствам. Этот вид контента в значительной мере обусловлен историко-культурными особенностям государств, действующими нормативными актами;

3) *нежелательный контент* – контент, который не указан в законодательно закрепленных перечнях деструктивного контента государств, но из оценки которого выявляется, что этот контент представляет опасность причинения вреда несовершеннолетним;

– *в результате определения концептуальных подходов к пониманию категории «информационная безопасность» в юридической науке и законодательстве* следует отметить, что все изученные легально зафиксированные понятия и авторские понятия «информационной безопасности», «кибербезопасности» как граждан в целом, так и несовершеннолетних в частности, несомненно, представляют научный интерес, отражают важные признаки многогранных вышеуказанных понятий, но в то же время иллюстрируют необходимость выработки единого общепринятого понятийного аппарата, так как проблема информационной безопасности несовершеннолетних в сети «Интернет» имеет трансгосударственный характер. В результате анализа законодательства России и зарубежных государств в сфере информационной безопасности несовершеннолетних в сети «Интернет», различных авторских дефиниций ключевых понятий в этой области правоотношений, предложены авторские определения «информационная безопасность несовершеннолетних» и «информационной безопасности несовершеннолетних в сети «Интернет».

Под информационной безопасностью несовершеннолетних диссертант понимает состояние защищенности физических лиц (граждан и лиц без гражданства), не достигших возраста 18 лет, обеспечиваемое комплексом правовых средств, направленных на защиту несовершеннолетних лиц и их прав от

воздействия на них информации, причиняющей вред их жизни, здоровью или развитию.

Согласно предложенному автором диссертационного исследования определению информационная безопасность несовершеннолетних в сети Интернет «представляет собой состояние защищенности лиц, не достигших возраста 18 лет, от информации, обращение которой в сети «Интернет» правовыми актами признаётся запрещенным». Обеспечение информационной безопасности несовершеннолетних в сети «Интернет» – это деятельность административных органов публичной власти и частных лиц, связанная с применением:

- административными органами публичной власти мер – административно-предупредительных, административно-пресекательных, восстановительных, мер административной ответственности;

- частными лицами (общественными организациями и непосредственно родителями (законными представителями) несовершеннолетних, владельцами социальных сетей, организаторами распространения информации в сети «Интернет») – мер, направленных на мониторинг контента, правовое воспитание несовершеннолетних; повышение родительских компетенций в сфере безопасного поведения детей в сети «Интернет»; проведение мероприятий, направленных на повышение грамотности детей по вопросам информационной безопасности в сети «Интернет»; формирование навыков законопослушного и ответственного поведения в цифровой среде; формирование у детей навыков самостоятельного и ответственного потребления информационной продукции в сети «Интернет»;

- *в результате изучения правового статуса публичных властных субъектов в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в Российской Федерации и зарубежных государствах* установлено, что в РФ отсутствует административный орган публичной власти или его структурное подразделение, основное направление деятельности которых было бы направлено непосредственно на обеспечение информационной безопасности несовершеннолетних в сети «Интернет». Обоснована целесообразность создания в структуре Федеральной службы по надзору в сфере связи, информационных

технологий и массовых коммуникаций (Роскомнадзор) Управления по информационной безопасности несовершеннолетних», полномочия которого предложены в диссертационном исследовании. Органы публичной власти можно разделить на три группы: 1) законодательные органы, принимающие участие в обеспечении информационной безопасности несовершеннолетних в сети «Интернет» посредством принятия законов, содержащих нормы административного права; 2) государственные органы, которые принимают участие в обеспечении информационной безопасности несовершеннолетних в сети «Интернет» путем подзаконного нормотворчества; 3) государственные органы, которые непосредственно обеспечивают защиту информационной безопасности несовершеннолетних в сети «Интернет» и восстановление их нарушенных прав и законных интересов.

На основании проведенного анализа полномочий органов публичной власти зарубежных государств выявлено, что с учетом общественной опасности, правоприменительной практики были введены законодательные ограничения для несовершеннолетних (малолетних) в сети «Интернет», а именно:

- в Австралии законодательно запрещен доступ несовершеннолетних младше 16 лет к социальным сетям, при этом механизм ограничения разрабатывается и обеспечивается исключительно цифровыми платформами;

- законодатели Великобритании обеспечили эффективную проверку возраста: наиболее рискованные сервисы должны использовать высокоэффективную проверку возраста, чтобы определять, кто из пользователей является несовершеннолетним, что может включать в себя запрет несовершеннолетним на доступ ко всему сайту или приложению или только к некоторым частям или видам контента ч. 12 (4) Закона о безопасности в Интернете 2023 года (Online Safety Act 2023)<sup>651</sup>;

---

<sup>651</sup> Online Safety Act 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50/enacted> (дата обращения: 01.05.2025).



– во Франции в ряде электронных ресурсов законодательно зафиксирована необходимость установки системы проверки возраста для предотвращения доступа несовершеннолетних<sup>652</sup>;

– по общему правилу (которое законодательно не закреплено) текущий минимальный возраст доступа во все основные социальные сети составляет 13 лет, что следует из решения Конгресса Соединенных Штатов (USA) от 1998 года по Закону о защите конфиденциальности детей в Интернете<sup>653</sup>, который запрещает веб-сайтам собирать информацию о детях младше 13 лет без их согласия; напомним, что основные мировые цифровые платформы соблюдают законодательство США в этой сфере.

Выявлено, что в России отсутствуют правовые акты, регламентирующие осуществление контроля (надзора), связанные с возрастным критерием при регистрации в социальных сетях несовершеннолетних граждан. Предложен правовой механизм подтверждения возраста лиц при регистрации в социальных сетях несовершеннолетних граждан и меры административной ответственности в этой сфере. Данный правовой механизм и административная ответственность фундируют обязанности владельца социальных сетей в информационно-телекоммуникационной сети «Интернет» при регистрации пользователя провести идентификацию и (или) аутентификацию его возраста и удостовериться, что физическое лицо достигло подросткового возраста, за исключением случаев регистрации в государственных и (или) муниципальных образовательных социальных сетях, регистрация в которых разрешена с 6,6 лет с согласия родителей (законных представителей) регистрируемого лица; также для целей регистрации пользователя в социальной сети владелец социальной сети принимает разумные меры для подтверждения возраста физического лица; а нарушение владельцем социальных сетей в сети «Интернет» требований настоящей статьи влечет за собой административную ответственность;

<sup>652</sup> LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368> (дата обращения: 01.05.2025).

<sup>653</sup> Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (дата обращения: 01.05.2025).

– на основании раскрытия особенностей участия частных лиц в сфере обеспечения информационной безопасности несовершеннолетних в сети «Интернет» в РФ и зарубежных государствах установлено, что к невластным субъектам, осуществляющим общественный контроль в исследуемой сфере правоотношений, относятся в РФ: общественные и добровольческие (волонтерские) объединения (АНО «Цисм», Ассоциация «Лига безопасного интернета», «Альянс по защите детей в цифровой среде», «Киберпатруль» и киберволонтеры, «Кибердружина» Народного фронта, Онлайн-платформа цифровых консультаций и безопасности в сети «Интернет» «РосКибербезопасность» и их аналоги в субъектах РФ, муниципальных образованиях, образовательных учреждениях); провайдеры хостингов, операторы связи и доменных имен, то есть лица, которые осуществляют блокирование запрещенного контента; владельцы социальных сетей, организаторы распространения информации в сети «Интернет», которых государство наделило полномочиями по осуществлению мониторинга за размещением и распространением контента в сети «Интернет» в части установления деструктивного контента и передачи данных об этом властному публичному лицу; также рассмотрены общественные (некоммерческие) объединения Австралии, Великобритании, наднациональные и национальные объединения государств – членов ЕС (Франции и Германии). Проведен сравнительный анализ российской «Лиги безопасного интернета» и зарубежных общественных организаций;

– в результате изучения мер административного принуждения в сфере информационной безопасности несовершеннолетних в сети «Интернет» по законодательству зарубежных государств (Австралия, Великобритания, ЕС) уставлено, что в зарубежных государствах, в отличие от российского законодательства, предусмотрена мера юридической ответственности в виде значительных штрафов цифровых платформ (владельцев социальных сетей), например, за противоправные деяния при идентификации возраста пользователя. Отличительной чертой зарубежного законодательства в исследуемой теме выступает достаточно проработанный подход к обеспечению информационной

безопасности несовершеннолетних в сети «Интернет» – например, выделение таких составов противоправных деяний, как кибербуллинг, киберпреследования (Австралия). Так, российское законодательство не выделяет отдельно такое противоправное деяние, как кибербуллинг (то есть «травля в сети «Интернет»»), привлекая за подобные действия лицо, достигшее 16-летнего возраста либо к административной ответственности за действия, установленные ст. 5.61, 20.1 КоАП РФ, либо к уголовной ответственности в соответствии со ст. 128.1, 213 УК РФ. Несомненно, что выделение этого действия в отдельный административный состав – дискуссионное, но интересное, с учетом его систематического и деструктивного влияния на здоровье и развитие несовершеннолетнего;

– в результате раскрытия общей характеристики административной ответственности за правонарушения в области информационной безопасности несовершеннолетних в российском сегменте сети «Интернет» выявлено, что российское законодательство направлено на административно-правовую защиту здоровья и морально-нравственных качеств малолетних детей и подростков, выделяя несовершеннолетних как специальный объект противоправных посягательств и ужесточая санкции при совершении правонарушений в отношении несовершеннолетних и с использованием сети «Интернет».

После детального анализа существующих составов правонарушений в исследуемой сфере правоотношений, предложен новый состав административного правонарушения, в котором: объектом правонарушения являются общественные отношения в сфере информационной безопасности несовершеннолетних лиц в сети «Интернет»; объективная сторона представлена регистрацией пользователя социальной сети в информационно-телекоммуникационной сети «Интернет» без идентификации и (или) без аутентификации возраста пользователя; предлагаемой новой ст. 6.17.1 КоАП РФ выделяются специальные субъекты правоотношений, к которым относятся владельцы социальной сети; субъективная сторона представлена умышленной формой вины.

Предложено расширить административную ответственность родителей или иных законных представителей несовершеннолетних в части установления

ответственности за использование недостоверных, заведомо ложных или не принадлежащих малолетнему лицу персональных (в том числе биометрических) данных при регистрации малолетних детей в социальной сети, не являющейся государственной (муниципальной) образовательной социальной сетью, путем добавления ч. 4–5 ст. 5.35 КоАП РФ. Отметим, что в отношении предложенных норм не предусмотрен специальный мониторинг, так как предложенные ч. 4–5 ст. 5.35 КоАП РФ являются коррелирующей мерой со статьей об административной ответственности непосредственно владельцев социальных сетей (ст. 6.17.1 КоАП РФ);

*– разработаны следующие предложения по совершенствованию норм российского законодательства, связанного с информационной безопасностью несовершеннолетних в сети «Интернет»:*

1) предложен правовой механизм подтверждения возраста лиц при регистрации в социальных сетях в сети «Интернет» и мер административной ответственности в этой сфере путем дополнения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» статьей «10.8. Обязанности владельца социальных сетей в информационно-телекоммуникационной сети «Интернет» и КоАП РФ статьей «6.17.1. Регистрация пользователя социальной сети в информационно-телекоммуникационной сети «Интернет» без идентификации и (или) без аутентификации возраста пользователя» и дополнением частями 4 и 5 статьи 5.35 «Неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по содержанию и воспитанию несовершеннолетних» КоАП РФ;

2) в целях унификации терминологии в действующем законодательстве и закрепления динамичного правового положения несовершеннолетних и обеспечения их информационной безопасности в сети «Интернет» предложено внести понятия «малолетний ребенок» и «подросток» во второй абзац статьи 1 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

3) дополнить текст, в том числе и название Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» новым объектом правовой охраны – «жизнь», которому может быть причинен вред от информации наравне со здоровьем и развитием несовершеннолетнего лица;

4) дополнить ч. 1 ст. 2 Федерального закона от 11.08.1995 № 135-ФЗ «О благотворительной деятельности и добровольчестве (волонтерстве)» еще одной целью, а именно – «содействие в обеспечении информационной безопасности граждан, в том числе несовершеннолетних, в информационно-телекоммуникационной сети «Интернет»»;

4) внесение изменений в Приказ Роскомнадзора от 25.03.2022 № 53 в части создания в структуре Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) «Управления по информационной безопасности несовершеннолетних», полномочия которого предложены в диссертационном исследовании.

Разумеется, вышеприведенные предложения не претендуют на непогрешимость, но безусловным фактом является то, что необходимо внедрять правовые механизмы, обеспечивающие безопасную и благоприятную для психики и развития несовершеннолетнего лица среду в сети «Интернет». Результаты диссертационного исследования в перспективе могут быть использованы для дальнейшего изучения темы административно-правового обеспечения информационной безопасности несовершеннолетних в сети «Интернет».

## СПИСОК ЛИТЕРАТУРЫ

### I. ДОКУМЕНТЫ

#### **1) Национальные нормативные правовые акты и иные официальные документы Российской Федерации**

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации. – Режим доступа: <http://pravo.gov.ru>, 06.10.2022.
2. Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ (ред. от 01.04.2025) // Собрание законодательства РФ. – 2015. – Ст. 1391; Собрание законодательства РФ. – 2025. – № 14. – Ст. 1587.
3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – Ст. 1; Собрание законодательства РФ. – 2005. – № 6. – Ст. 404.
4. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 22.07.2024) // Российская газета. – 22.12.2006. – № 289; Российская газета. – 29.07.2024. – № 165.
5. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024, с изм. от 31.10.2024) // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301; Собрание законодательства РФ. – 2024. – № 33 (Часть I). – Ст. 4933.
6. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 28.12.2024) // Собрание законодательства РФ. – 2002. – № 46. – Ст. 4532; Собрание законодательства РФ. – 2024. – № 53 (Часть I). – Ст. 8531.

7. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 28.12.2024) // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – Ст. 3; Собрание законодательства РФ. – 2024. – № 53 (Часть I). – Ст. 8551.
8. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 21.04.2025) // Собрание законодательства РФ. – 2001. – № 52 (ч. I). – Ст. 4921; Собрание законодательства РФ. – 2025. – № 17. – Ст. 2130.
9. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954; Собрание законодательства РФ. – 2025. – № 9. – Ст. 860.
10. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954; Российская газета. – 25.04.2025. – № 93.
11. Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. – 2025. – № 14. – Ст. 1574.
12. Федеральный закон от 24.06.1999 № 120-ФЗ (ред. от 01.04.2025) «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» // Собрание законодательства РФ. – 1999. – № 26. – Ст. 3177; Собрание законодательства РФ. – 2025. – № 14. – Ст. 1588.
13. Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 28.02.2025) «Об образовании в Российской Федерации» // Собрание законодательства РФ. – 2012. – № 53 (ч. 1). – Ст. 7598; Собрание законодательства РФ. – 2025. – № 9. – Ст. 859.
14. Федеральный закон от 17.01.1992 № 2202-1 (ред. от 03.02.2025) «О прокуратуре Российской Федерации» // Собрание законодательства РФ. – 1995. – № 47. – Ст. 4472; Собрание законодательства РФ. – 1995. – № 47. – Ст. 4472.
15. Федеральный закон от 11.08.1995 № 135-ФЗ (ред. от 28.12.2024) «О благотворительной деятельности и добровольчестве (волонтерстве)» // Собрание

законодательства РФ. – 1995. – № 33. – Ст. 3340; Собрание законодательства РФ. – 2024. – № 53 (Часть I). – Ст. 8564.

16. Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 28.12.2024) «О полиции» // Собрание законодательства РФ. – 2011. – № 7. – Ст. 900; Собрание законодательства РФ. – 2024. – № 53 (Часть I). – Ст. 8528.

17. Федеральный закон от 13.03.2006 № 38-ФЗ (ред. от 26.12.2024) «О рекламе» // Собрание законодательства РФ. – 2006. – № 12. – Ст. 1232; Собрание законодательства РФ. – 2024. – № 53 (Часть I). – Ст. 8489.

18. Федеральный закон от 29.12.2022 № 572-ФЗ (ред. от 26.12.2024) «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства РФ. – 2023. – № 1 (часть I). – Ст. 19; Собрание законодательства РФ. – 2024. – № 53 (Часть I). – Ст. 8504.

19. Федеральный закон от 24.07.1998 № 124-ФЗ (ред. от 30.11.2024) «Об основных гарантиях прав ребенка в Российской Федерации» // Собрание законодательства РФ. – 1998. – № 31. – Ст. 3802; Собрание законодательства РФ. – 2024. – № 49 (часть IV). – Ст. 7429.

20. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // Собрание законодательства РФ. – 2011. – № 1. – Ст. 48; Собрание законодательства РФ. – 2024. – № 49 (часть IV). – Ст. 7429.

21. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448; Собрание законодательства РФ. – 2024. – № 48. – Ст. 7218.

22. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451; Собрание законодательства РФ. – 2024. – № 33 (Часть I). – Ст. 4929.



23. Федеральный закон от 01.07.2021 № 236-ФЗ (ред. от 22.06.2024) «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» // Собрание законодательства РФ. – 2021. – № 27 (часть I). – Ст. 5064; Официальный интернет-портал правовой информации. – Режим доступа: <http://pravo.gov.ru> (22.06.2024).

24. Федеральный закон от 27.12.2018 № 501-ФЗ (ред. от 10.07.2023) «Об уполномоченных по правам ребенка в Российской Федерации» // Собрание законодательства РФ. – 2018. – № 53 (часть I). – Ст. 8427; Собрание законодательства РФ. – 2023. – № 29. – Ст. 5304.

25. Федеральный закон от 30.12.2020 № 530-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2021. – № 1 (часть I). – Ст. 69.

26. Федеральным законом от 30 декабря 2020 г. № 513-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Собрание законодательства РФ. – 2021. – № 1 (часть I). – Ст. 52.

27. Федеральный закон от 29.12.2020 № 472-ФЗ «Об ограничении оборота закиси азота в Российской Федерации» // Российская газета. – 11.01.2021. – № 1.

28. Федеральный закон от 13.07.2015 № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса РФ» // Собрание законодательства РФ (Начало действия с 01.01.2016). – 2015. – № 29 (часть I). – Ст. 4390.

29. Закон РФ от 15.01.1993 № 4301-1(ред. от 29.05.2024) «О статусе Героев Советского Союза, Героев Российской Федерации и полных кавалеров ордена Славы» // Российская газета. – 10.02.1993. – № 27; Собрание законодательства РФ. – 2024. – № 23 (часть I). – Ст. 3055.

30. Закон РФ от 15.05.1991 № 1244-1 (ред. от 25.12.2023) «О социальной защите граждан, подвергшихся воздействию радиации вследствие катастрофы на

Чернобыльской АЭС» // Ведомости СНД и ВС РСФСР. – 1991. – № 21. – Ст. 699; Собрание законодательства. – 2024. – № 1 (часть I). – Ст. 3.

31. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. – 2021. – № 27 (часть II). – Ст. 5351.

32. Указ Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Собрание законодательства РФ. – 2021. – № 16 (Часть I). – Ст. 2746.

33. Указ Президента РФ от 11.03.2020 № 180 «О дополнительных мерах социальной защиты некоторых категорий граждан Российской Федерации» // Собрание законодательства РФ. – 2020. – № 11. – Ст. 1530.

34. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

35. Указ Президента РФ от 01.06.2012 № 761 «О Национальной стратегии действий в интересах детей на 2012 – 2017 годы» // Собрание законодательства РФ. – 2012. – № 23. – Ст. 2994.

36. Комплексный план противодействия идеологии терроризма в Российской Федерации на 2024 – 2028 годы (утв. Президентом РФ 30.12.2023 № Пр-2610) // СПС «КонсультантПлюс».

37. Постановление Правительства РФ от 28.12.2024 № 1963 «Об отдельных вопросах распространения информации в социальных сетях» // Собрание законодательства РФ. – 2025. – № 1. – Ст. 23.

38. Постановление Правительства РФ от 02.09.2022 № 1547 «О порядке предоставления выплат гражданам Донецкой Народной Республики, Луганской Народной Республики, Украины и лицам без гражданства, вынужденно покинувшим территории Донецкой Народной Республики, Луганской Народной Республики, Украины и прибывшим на территорию Российской Федерации» // Собрание законодательства РФ. – 2022. – № 37. – Ст. 6343.

39. Постановление Правительства РФ от 24.07.2021 № 1259 «Об утверждении перечня одурманивающих веществ» // Собрание законодательства РФ. – 2021. – № 31. – Ст. 5922.

40. Постановление Правительства РФ от 28.07.2018 № 885 (ред. от 07.03.2025) «Об утверждении Положения о Федеральной службе по надзору в сфере образования и науки и признании утратившими силу некоторых актов Правительства Российской Федерации» (с изм. и доп., вступ. в силу с 01.04.2025) // Собрание законодательства РФ. – 2018. – № 32 (Часть II). – Ст. 5344; Собрание законодательства РФ. – 2025. – № 10. – Ст. 1088.

41. Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 25.12.2024) «Об утверждении государственной программы Российской Федерации «Информационное общество»» // Собрание законодательства РФ. – 2014. – № 18 (часть II). – Ст. 2159.

42. Постановление Правительства РФ от 26.10.2012 № 1101 (ред. от 21.02.2025) «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-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // Собрание законодательства РФ. – 2012. – № 44. – Ст. 6044.

43. Постановление Правительства РФ от 20.07.2011 № 590 (ред. от 27.02.2025) «О Министерстве культуры Российской Федерации» (вместе с «Положением о Министерстве культуры Российской Федерации») // Собрание законодательства РФ. – 2011. – № 31. – Ст. 4758; Собрание законодательства РФ. – 2025. – № 9. – Ст. 964.

44. Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 27.03.2025) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых

коммуникаций» // Собрание законодательства РФ. – 2009. – № 12. – Ст. 1431; Собрание законодательства РФ. – 2025. – № 13. – Ст. 1482.

45. Постановление Правительства РФ от 02.06.2008 № 418 (ред. от 27.03.2025) «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» // Собрание законодательства РФ. – 2008. – № 23. – Ст. 2708; Собрание законодательства РФ. – 2025. – № 13. – Ст. 1485.

46. Распоряжение Правительства РФ от 01.07.2024 № 1734-р (ред. от 04.04.2025) «Об утверждении Плана мероприятий по реализации в 2024 – 2026 годах Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // Собрание законодательства РФ. – 2024. – № 28. – Ст. 4058.

47. Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // Собрание законодательства РФ. – 2023. – № 19. – Ст. 3481.

48. Закон г. Москвы от 23.11.2005 № 60 «О социальной поддержке семей с детьми в городе Москве» (ред. от 20.10.2021) // Ведомости Московской городской Думы. – 29.12.2005. – № 12(2). – Ст. 293. – Режим доступа: <https://base.garant.ru/384375/> (дата обращения: 01.05.2025).

49. Закон Приморского края от 29.12.2004 № 217-КЗ «О защите прав ребенка в Приморском крае» (в ред. 1 марта 2023) // Ведомости Законодательного Собрания Приморского края. 29.12.2004. – № 84.

50. Закон Республики Коми от 19 ноября 1996 г. № 36-РЗ «О защите прав детей в Республике Коми». – Режим доступа: <https://base.garant.ru/27300328/> (дата обращения: 01.05.2025).

51. ГОСТ Р 56824-2015. Национальный стандарт Российской Федерации. Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет (утв. и введен в действие Приказом Росстандарта от 03.12.2015 N 2103-ст). – М. : Стандартинформ, 2017.

52. ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения (утв. Приказом Ростехрегулирования от 29.12.2005 № 449-ст). – М. : Стандартинформ, 2006.

53. Пояснительная записка «К проекту Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс».

54. Приказ Генпрокуратуры России от 13.12.2021 № 744 «Об организации прокурорского надзора за исполнением законодательства о несовершеннолетних, соблюдением их прав и законных интересов» // Законность. – 2022. – № 2; СПС «КонсультантПлюс».

55. Приказ Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию» // Российская газета. – 20.08.2014. – № 187.

56. Приказ Минкомсвязи России от 29.08.2012 № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей» (Зарегистрировано в Минюсте России 16.10.2012 N 25682) // Российская газета. – 24.10.2012. – № 245.

57. Приказ Минкомсвязи России от 29.08.2012 № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей» // Российская газета. – 24.10.2012. – № 245.

58. Приказ Минкомсвязи России от 29.08.2012 № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей» (Зарегистрировано в Минюсте России 16.10.2012 № 25682) // Российская газета. – 24.10.2012. – № 245.

59. Приказ Минобрнауки России от 24.01.2024 № 35 «Об утверждении форм аналитических отчетов по результатам осуществления мониторинга реализации молодежной политики в Российской Федерации» // Официальный интернет-портал правовой информации. – Режим доступа: <http://pravo.gov.ru> (29.04.2025).

60. Приказ Минобрнауки России от 24.01.2024 № 35 «Об утверждении форм аналитических отчетов по результатам осуществления мониторинга реализации молодежной политики в Российской Федерации» // Официальный интернет-портал правовой информации. – Режим доступа: <http://pravo.gov.ru> (29.04.2025).

61. Приказ Минцифры России от 01.12.2020 № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021 – 2027 годы» // Вестник образования России. – 2021, январь. – № 1.

62. Приказ Минцифры России от 22.03.2022 № 226 «О перечне федеральных мероприятий, направленных на обеспечение информационной безопасности детей, производство информационной продукции для детей и оборот информационной продукции, на 2022 – 2027 годы» // СПС «КонсультантПлюс».

63. Приказ Роскомнадзора от 05.10.2021 № 208 «Об установлении Требований к экспертам и экспертным организациям, осуществляющим проведение экспертизы информационной продукции» // Официальный интернет-портал правовой информации. – Режим доступа: <http://pravo.gov.ru>, 14.01.2022.

64. Приказ Роскомнадзора от 09.07.2024 № 125 «Об утверждении Порядка аккредитации экспертов и экспертных организаций на право проведения экспертизы информационной продукции» (Зарегистрировано в Минюсте России 06.09.2024 № 79408) // Официальный интернет-портал правовой информации. – Режим доступа: <http://pravo.gov.ru>, 09.09.2024.

65. Приказ Роскомнадзора от 14.10.2016 № 268 «Об утверждении Правил формирования и ведения реестра аттестованных экспертов, привлекаемых Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций к проведению мероприятий по контролю» (Зарегистрировано в Минюсте России 13.01.2017 № 45192) // Официальный интернет-портал правовой информации. – Режим доступа: <http://www.pravo.gov.ru>, 13.01.2017.

66. Приказ Роскомнадзора от 21.06.2016 № 174 «Об утверждении Критериев аттестации экспертов, привлекаемых Федеральной службой по надзору

в сфере связи, информационных технологий и массовых коммуникаций к проведению мероприятий по контролю» (Зарегистрировано в Минюсте России 24.08.2016 № 43381) // Официальный интернет-портал правовой информации. – Режим доступа: <http://www.pravo.gov.ru>, 25.08.2016.

67. Приказ Роскомнадзора от 25.03.2022 № 53 «Об утверждении структуры и штатного расписания Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СПС «КонсультантПлюс».

68. Приказ Роскомнадзора от 25.03.2022 № 53 «Об утверждении структуры и штатного расписания Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СПС «КонсультантПлюс».

69. Приказ Роскомнадзора от 25.03.2022 № 53 «Об утверждении структуры и штатного расписания Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СПС «КонсультантПлюс».

70. Приказ ФАС России от 28.12.2023 № 1079/23 «Об утверждении руководств по соблюдению обязательных требований в сфере рекламы» // СПС «КонсультантПлюс».

71. Письмо Минкомсвязи России от 14.08.2012 № 52-165/ВА «О применении норм Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс».

72. Письмо Роспотребнадзора от 16.05.2007 № 0100/4960-07-32 «О действующих нормативных и методических документах по гигиене детей и подростков» // М. : Федеральный центр гигиены и эпидемиологии Роспотребнадзора, 2007; СПС «КонсультантПлюс».

73. Письмо ФНП от 22.07.2016 № 2668/03-16-3 «О Методических рекомендациях по удостоверению доверенностей» (вместе с «Методическими

рекомендациями по удостоверению доверенностей», утв. решением Правления ФНП от 18.07.2016, протокол N 07/16) // СПС «КонсультантПлюс».

74. Проект Федерального закона «О введении в действие Кодекса Российской Федерации об административных правонарушениях и Процессуального кодекса Российской Федерации об административных правонарушениях» (подготовлен Минюстом России, ID проекта 02/04/01-20/00099058) // СПС «КонсультантПлюс».

75. Проект Федерального закона № 1112019-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с введением понятия уголовного проступка» // СПС «КонсультантПлюс».

76. Закон РФ от 23.09.1992 № 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных» // Ведомости СНД РФ и ВС РФ. – 1992. – № 42. – Ст. 2325; Российская газета. – 08.02.2006. – № 25 (утратил силу).

77. Законопроект № 442510-6 «О внесении изменений в главу 2 Кодекса Российской Федерации об административных правонарушениях (в части уточнения возраста, по достижении которого наступает административная ответственность)» (отклонен 17.06.2014) // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество». . – Режим доступа: <https://sozd.duma.gov.ru/bill/442510-6> (дата обращения: 01.05.2025).

## **2) Международные договоры**

78. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета. – 05.04.1995. – № 67.

79. Декларация о распространении среди молодежи идеалов мира, взаимного уважения и взаимопонимания между народами (принята резолюцией 2037 (XX) Генеральной Ассамблеи от 7 декабря 1965 года). – Режим доступа: [https://www.un.org/ru/documents/decl\\_conv/declarations/youth\\_peace\\_ideals.shtml](https://www.un.org/ru/documents/decl_conv/declarations/youth_peace_ideals.shtml) (дата обращения 30.03.2025).



80. Декларация прав ребенка (Принята 20.11.1959 Резолюцией 1386 (XIV) на 841-м пленарном заседании Генеральной Ассамблеи ООН) // Международная защита прав и свобод человека. Сборник документов. – М. : Юридическая литература, 1990. С. 385–388 (не ратифицирована).

81. Конвенция № 111 Международной организации труда «Относительно дискриминации в области труда и занятий» (принята в г. Женеве 25.06.1958 на 42-й сессии Генеральной конференции МОТ) // Ведомости ВС СССР. – 1 ноября 1961 г. – № 44. – Ст. 448 (ратифицировано СССР).

82. Конвенция № 138 Международной организации труда «О минимальном возрасте для приема на работу» [рус., англ.] (Заключена в г. Женеве 26.06.1973) . – Режим доступа: <https://base.garant.ru/2540542/> (дата обращения: 21.07.2025).

83. Конвенция о защите прав человека и основных свобод (Заключена в г. Риме 04.11.1950, с изм. от 24.06.2013) (вместе с «Протоколом [№ 1]» (Подписан в г. Париже 20.03.1952), «Протоколом № 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (Подписан в г. Страсбурге 16.09.1963), «Протоколом № 7» (Подписан в г. Страсбурге 22.11.1984)) // Собрание законодательства РФ. – 2001. – № 2. – Ст. 163.

84. Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989, вступила в силу для СССР 15.09.1990) // Сборник международных договоров СССР. – 1993. – Вып. XLVI.

85. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г., с изм. от 28.01.2003) // СПС «КонсультантПлюс».

86. Конвенция об обеспечении международной информационной безопасности. – Режим доступа: <https://interkomitet.ru> (дата обращения: 01.05.2025).

87. Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (принята резолюцией 79/243 Генеральной Ассамблеей от

24.12.2024). – Режим доступа: <https://www.un.org/ru/documents/treaty/A-RES-79-243> (дата обращения: 31.08.2025).

88. Международная конвенция о ликвидации всех форм расовой дискриминации (заключена 21.12.1965, с изм. от 15.01.1992) // Ведомости ВС СССР. – 18.06.1969. – № 25. – Ст. 219 (ратифицировано СССР).

89. Международный пакт о гражданских и политических правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-м пленарном заседании Генеральной Ассамблеи ООН) // Ведомости Верховного Совета СССР. – 1976. – № 17. – Ст. 291; Бюллетень Верховного Суда РФ. – 1994. – № 12 (вступил в силу для СССР 23.03.1976).

90. Международный пакт о гражданских и политических правах от 16 декабря 1966 г. // Ведомости ВС СССР. – 1976. – № 17. – Ст. 291.

91. Международный пакт об экономических, социальных и культурных правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-м пленарном заседании Генеральной Ассамблеи ООН) // Ведомости Верховного Совета СССР. – 1976. – № 17. – Ст. 291 (ратифицирован Указом Президиума ВС СССР от 18.09.1973 N 4812-VIII).

92. Минимальные стандартные правила ООН, касающиеся отправления правосудия в отношении несовершеннолетних («Пекинские правила») (приняты 29 ноября 1985 г. Резолюцией 40/33 на 96-м пленарном заседании Генеральной Ассамблеи ООН) // Советская юстиция. – 1991. – №№ 12–14.

93. Постановление № 41-15 Межпарламентской Ассамблеи государств-участников СНГ «О модельном законе «Об информации, информатизации и обеспечении информационной безопасности» (Принято в г. Санкт-Петербурге 28.11.2014) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2015. – № 62 (ч. 2).

94. Резолюция 55/33 Генеральной Ассамблеи ООН «Всеобщее и полное разоружение» (Принята в г. Нью-Йорке 20.11.2000 на 69-м пленарном заседании 55-й сессии Генеральной Ассамблеи ООН) // СПС «Гарант».

95. Решение Коллегии Евразийской экономической комиссии от 13.12.2022 № 195 «О порядке введения в действие изменений в технический регламент Таможенного союза «О безопасности продукции, предназначенной для детей и подростков» (ТР ТС 007/2011)» // Официальный сайт Евразийского экономического союза. – Режим доступа: <https://docs.eaeunion.org/documents/399/7129/> (дата обращения: 03.03.2025).

96. Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. // Бюллетень международных договоров. – 2019. – № 9

97. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. // Бюллетень международных договоров. – 2015. – № 10. – С. 7-13.

98. Хартия Европейского Союза об основных правах (Страсбург, 12 декабря 2007 г.) (2016/С 202/02) // СПС «Гарант». – Режим доступа: <https://base.garant.ru/71672404/> (дата обращения: 21.07.2025).

99. Geneva Declaration of the Rights of the Child of 1924. – Режим доступа: <https://www.humanium.org/en/text-2> (дата обращения: 01.05.2025) (не ратифицирована РФ).

### **3) Национальные нормативные правовые акты зарубежных государств**

100. Age Discrimination Act 2004 No. 68 [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.au/C2004A01302/latest/text> (дата обращения: 01.05.2025).

101. Age of Majority Act 1974 (amendments A2011-3 of 1 March 2011) // The Age of Majority Ordinance 1974 was notified in the Commonwealth Gazette on 24 October 1974 (Cwlth Gaz 1974 No 87A) [Электронный ресурс]. – Режим доступа: <https://www.legislation.act.gov.au/a/1974-46/Default.asp?show=full> (дата обращения: 21.07.2025).

102. Age of Majority by Country 2025 [Электронный ресурс]. – Режим доступа: <https://worldpopulationreview.com/country-rankings/age-of-majority-by-country> (дата обращения 30.03.2025).

103. Age of majority. FRA: the EU's Rights Agency [Электронный ресурс]. – Режим доступа: <https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/age-majority> (дата обращения 30.03.2025)

104. Allgemeines bürgerliches Gesetzbuch or ABGB on 1 June 1811 [Электронный ресурс]. – Режим доступа: <https://www.jusline.at/gesetz/abgb/paragraf/21> (дата обращения: 01.05.2025).

105. Broadcasting Services Amendment (Online Services) Act 1999 No. 90 (утратил силу) [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.au/C2004A00484/asmade/text> (дата обращения: 01.05.2025).

106. Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Bundes-Jugendvertretungsgesetz, Fassung vom 05.05.2025 / Bundesgesetz über die Vertretung der Anliegen der Jugend (Bundes-Jugendvertretungsgesetz) StF: BGBl. I Nr. 127/2000 (NR: GP XXI IA 270/A AB 351 S. 46. BR: 6253 und 6254 AB 6264 S. 670.), BGBl. I Nr. 136/2001 [Электронный ресурс]. – Режим доступа: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001059> (дата обращения: 01.05.2025).

107. Charity commission for England and Wales [Электронный ресурс]. – Режим доступа: [https://register-of-charities.charitycommission.gov.uk/en/charity-search/?p\\_p\\_id=uk\\_gov\\_ccew\\_onereg\\_charitydetails\\_web\\_portlet\\_CharityDetailsPortlet&p\\_p\\_lifecycle=0&p\\_p\\_state=maximized&p\\_p\\_mode=view&\\_uk\\_gov\\_ccew\\_onereg\\_charitydetails\\_web\\_portlet\\_CharityDetailsPortlet\\_regId=1112398&\\_uk\\_gov\\_ccew\\_onereg\\_charitydetails\\_web\\_portlet\\_CharityDetailsPortlet\\_subId=0](https://register-of-charities.charitycommission.gov.uk/en/charity-search/?p_p_id=uk_gov_ccew_onereg_charitydetails_web_portlet_CharityDetailsPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_uk_gov_ccew_onereg_charitydetails_web_portlet_CharityDetailsPortlet_regId=1112398&_uk_gov_ccew_onereg_charitydetails_web_portlet_CharityDetailsPortlet_subId=0) (дата обращения: 01.05.2025).

108. Children (Community Service Orders) Act 1987 No 56 [Электронный ресурс]. – Режим доступа:

<https://legislation.nsw.gov.au/view/whole/html/inforce/2016-01-15/act-1987-056> (дата обращения: 21.07.2025);

109. Children (Criminal Proceedings) Act 1987 No 55 (NSW) [Электронный ресурс]. – Режим доступа: <https://www.legislation.nsw.gov.au/view/pdf/asmade/act-1987-55> (дата обращения: 21.07.2025).

110. Children (Detention Centres) Act 1987 No 57 [Электронный ресурс]. – Режим доступа: <https://legislation.nsw.gov.au/view/html/inforce/2023-07-14/act-1987-057> (дата обращения: 21.07.2025).

111. Children and Young Persons (Care and Protection) Act 1998 No 157 (NSW) [Электронный ресурс]. – Режим доступа: <https://legislation.nsw.gov.au/view/whole/whole/html/inforce/2014-07-04/act-1998-157> (дата обращения: 21.07.2025).

112. Children's Online Privacy Protection Act 2000 (COPPA) [Электронный ресурс]. – Режим доступа: <https://www.congress.gov/> (дата обращения: 01.05.2025).

113. Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 [Электронный ресурс]. – Режим доступа: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (дата обращения: 30.03.2025).

114. Code de l'actionsociale et des familles [Электронный ресурс]. – Режим доступа: [https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006074069/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006074069/) (дата обращения: 01.05.2025).

115. Code of Practise on New Formof Content [Электронный ресурс]. – Режим доступа: <https://www.mobileuk.org/codes-of-practice> (дата обращения: 01.05.2025).

116. Code pénal [Электронный ресурс]. – Режим доступа: [https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006070719/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/) (дата обращения: 01.05.2025).

117. Communications Act 2003 [Электронный ресурс]. – Режим доступа: [www.legislation.gov.uk/ukpga/2003/21/section/3](http://www.legislation.gov.uk/ukpga/2003/21/section/3) (дата обращения: 01.05.2025).

118. Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 [Электронный ресурс]. – Режим доступа:

[https://www.aph.gov.au/Parliamentary\\_Business/Committees/Senate/Environment\\_and\\_Communications/MisandDisinfobill](https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/MisandDisinfobill) (дата обращения: 01.05.2025).

119. Conseil d'Etat le 8 décembre 1994, Paris, La Documentation française, coll. Les études du Conseil d'Etat, 1995. [Электронный ресурс]. – Режим доступа: <https://www.legifrance.gouv.fr/juri/id/CETATEXT000007851037> (дата обращения: 21.07.2025).

120. Crimes (Domestic and Personal Violence) Act 2007 No 80 (current version for 4 April 2025) (NSW) [Электронный ресурс]. – Режим доступа: <https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2007-080> (дата обращения: 21.07.2025).

121. Crimes Act 1900 (NSW) No. 40 [Электронный ресурс]. – Режим доступа: <https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1900-040#sec.31C> (дата обращения: 01.05.2025).

122. Criminal Code Act 1995 No. 12 [Электронный ресурс]. – Режим доступа: <http://www5.austlii.edu.au/au> (дата обращения: 01.05.2025).

123. Cyber Ireland Cluster Strategy 2024- 2027 [Электронный ресурс]. – Режим доступа: <https://cyberireland.ie> (дата обращения: 01.05.2025).

124. Cyberbullying [Электронный ресурс]. – Режим доступа: <https://www.esafety.gov.au> (дата обращения: 01.05.2025).

125. Decision of the Court of Appeal of British Columbia dated June 11, 2015 [Электронный ресурс]. – Режим доступа: <https://www.eff.org/files/2015/12/16/2015bcc265.pdf> (дата обращения: 01.05.2025).

126. Decreto legislativo 8 novembre 2021, n. 208 Attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato. (21G00231) // [Электронный ресурс]. – Режим доступа: <https://www.normattiva.it/uri->

res/N2Ls?urn:nir:stato:DECRETO.LEGISLATIVO:2021-11-08;208!vig= (дата обращения 30.03.2025).

127. Defamation Act 77 of 2005 (at 2 March 2025) Australia, New South Wales [Электронный ресурс]. – Режим доступа: [https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/nsw/consol\\_act/da200599/](https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/nsw/consol_act/da200599/) (дата обращения: 01.05.2025).

128. Digital Markets Act Regulation (EU) 2022/1925 of the European Parliament and of the Council [Электронный ресурс]. – Режим доступа: <http://eur-lex.europa.eu/> (дата обращения 30.03.2025).

129. Directive 2010/13/EU on audiovisual media services (Audiovisual Media Services Directive) [Электронный ресурс]. – Режим доступа: <https://digital-strategy.ec.europa.eu/en/policies/audiovisual-and-media-services> (30.03.2025).

130. Enhancing Online Safety for Children Act 2015 (No. 24 of 2015) [Электронный ресурс]. – Режим доступа: [https://www4.austlii.edu.au/au/legis/cth/num\\_act/eosfca2015321/](https://www4.austlii.edu.au/au/legis/cth/num_act/eosfca2015321/) (дата обращения: 01.05.2025).

131. Equustek Solutions Inc v Google Inc [2015] BCCA 265 [Электронный ресурс]. – Режим доступа: <https://www.eff.org/files/2015/12/16/2015bcc265.pdf> (дата обращения: 01.05.2025).

132. EU cybersecurity strategy: an open, safe and secure cyberspace (European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP))) // Brussels, 7.2.2013. [Электронный ресурс]. – Режим доступа: <https://eur-lex.europa.eu/legal-content/EN/> (дата обращения: 01.05.2025).

133. European Declaration on Digital Rights and Principles for the Digital Decade 28/12/2022 [Электронный ресурс]. – Режим доступа: <https://eur-lex.europa.eu/legal-content/en> (дата обращения: 01.05.2025).

134. European Digital Services Act (DSA) (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC) (the DSA) [Электронный ресурс]. – Режим доступа: <http://eur-lex.europa.eu/> (дата обращения: 30.03.2025).

135. European Strategy for a Better Internet for Children (BIK) 02/05/2012 [Электронный ресурс]. – Режим доступа: <https://eur-lex.europa.eu/legal-content/en> (expired) (дата обращения: 01.05.2025).

136. Evidence Act 1995 No 25 (NSW) [Электронный ресурс]. – Режим доступа: <https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1995-025> (дата обращения: 21.07.2025).

137. Exposure Draft of the Social Media (Anti-Trolling) Bill 2021, December 2021 [Электронный ресурс]. – Режим доступа: [https://www.uts.edu.au/globalassets/sites/default/files/2022-05/cmt-submission-to-attorney-generals-department-on-exposure-draft-of-anti-trolling-bill\\_0.pdf](https://www.uts.edu.au/globalassets/sites/default/files/2022-05/cmt-submission-to-attorney-generals-department-on-exposure-draft-of-anti-trolling-bill_0.pdf) (дата обращения: 01.05.2025).

138. Fairfax Media Publications Pty Ltd v Voller; Nationwide News Pty Limited v Voller; Australian News Channel Pty Ltd v Voller [2021] HCA 27 (8 September 2021) S236/2020, S237/2020 и S238/2020 [Электронный ресурс]. – Режим доступа: [https://www.hcourt.gov.au/cases/case\\_s236-2020](https://www.hcourt.gov.au/cases/case_s236-2020) (дата обращения: 01.05.2025).

139. Family Law Reform Act 1969 [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.uk/ukpga/1969/46/section/1> (дата обращения: 21.07.2025).

140. Federal Government Introduces Bill to Expand Role of the Children's e-Safety Commissioner [Электронный ресурс]. – Режим доступа: <https://www.timebase.com.au/news/2017/AT04136-article.html> (дата обращения: 01.05.2025).

141. Finland's Cyber Security Strategy 2024-2035 [Электронный ресурс]. – Режим доступа: <https://www.itu.int/en/> (дата обращения: 01.05.2025).

142. Gesetz über Ordnungswidrigkeiten (OWiG) [Электронный ресурс]. – Режим доступа: <https://www.buzer.de/gesetz/5827/index.htm> (дата обращения: 01.05.2025).

143. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 29 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149)



geändert worden ist [Электронный ресурс]. – Режим доступа: <https://www.buzer.de/gesetz/12799/index.htm> (дата обращения: 01.05.2025).

144. International Telecommunications Union (ITU) (2008). Overview of Cybersecurity, Recommendation ITU–T X.1205 [Электронный ресурс]. – Режим доступа: <https://www.itu.int/rec/T-REC-X.1205-200804-I> (дата обращения: 01.05.2025).

145. Jugendmedienschutz-Staatsvertrag (JMStV) vom 13. September 2002 (GVBl. 2003 S. 147, BayRS 02-21-S), der zuletzt durch Art. 2 des Vertrages vom 27. Februar 2024 (GVBl. S. 326) geändert worden ist [Электронный ресурс]. – Режим доступа: <https://www.gesetze-bayern.de/Content/Document/JMStV> (дата обращения: 01.05.2025).

146. Jugendschutzgesetz vom 23. Juli 2002 (BGBl. I S. 2730), das zuletzt durch Artikel 12 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist [Электронный ресурс]. – Режим доступа: <https://www.buzer.de/JuSchG.htm> (дата обращения: 01.05.2025).

147. Küberturvalisuse seadus (KüTS) 09.05.2018 [Электронный ресурс]. – Режим доступа: <https://www.riigiteataja.ee/akt/122052018001> (дата обращения: 01.05.2025).

148. Law no. 2007-297 of 5 March 2007 relating to the prevention of delinquency intends to improve the means for preventing delinquency by minors [Электронный ресурс]. – Режим доступа: <https://eurydice.eacea.ec.europa.eu> (дата обращения: 01.05.2025).

149. Legge 17 ottobre 1967, n. 977 Tutela del lavoro dei ((bambini)) e degli adolescent (Ultimo aggiornamento all'atto pubblicato il 14/03/2016) (GU n.276 del 06-11-1967) [Электронный ресурс]. – Режим доступа: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1967-10-17;977> (дата обращения 30.03.2025).

150. Legge n. 71/2017 sul cyberbullismo Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo. (17G00085) (GU n.127 del 3-6-2017) [Электронный ресурс]. – Режим доступа: <https://www.senato.it/> (дата обращения: 30.03.2025).

151. LOI n° 2006-399 du 4 avril 2006 renforçant la prévention et la répression des violences au sein du couple ou commises contre les mineurs (law reinforcing the prevention and repression of violence within couple or against minors) [Электронный ресурс]. – Режим доступа: <https://www.legifrance.gouv.fr> (дата обращения: 01.05.2025).

152. LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles [Электронный ресурс]. – Режим доступа: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952> (дата обращения: 01.05.2025).

153. LOI n° 2020-766 du mercredi 24 juin 2020 visant à lutter contre les contenus haineux sur internet (Publiée au Journal Officiel du jeudi 25 juin 2020) [Электронный ресурс]. – Режим доступа: <https://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSX1913052L> (дата обращения: 01.05.2025).

154. LOI n° 2022-140 du 7 février 2022 relative à la protection des enfants [Электронный ресурс]. – Режим доступа: <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000043668561/> (дата обращения: 01.05.2025).

155. LOI n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet [Электронный ресурс]. – Режим доступа: <https://www.legifrance.gouv.fr> (дата обращения: 01.05.2025).

156. LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique [Электронный ресурс]. – Режим доступа: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368> (дата обращения: 01.05.2025).

157. LOI n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs [Электронный ресурс]. – Режим доступа: <https://www.legifrance.gouv.fr> (дата обращения: 01.05.2025).

158. LOI № 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Электронный ресурс]. – Режим доступа:

[https://www.legifrance.gouv.fr/loda/article\\_lc/LEGIARTI000037822807/](https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037822807/) (дата обращения: 10.08.2025).

159. National Cyber Strategy 2022 [Электронный ресурс]. – Режим доступа: <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022> (дата обращения: 21.07.2025).

160. National Cybersecurity Strategy 2021-2025 [Электронный ресурс]. – Режим доступа: <https://digital-skills-jobs.europa.eu/en/> (дата обращения: 01.05.2025).

161. Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 29 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist [Электронный ресурс]. – Режим доступа: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> (дата обращения: 01.05.2025).

162. Office of Communications Act 2002 [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.uk/ukpga/2002/11> (дата обращения: 01.05.2025).

163. Official website eSafety Commissioner. eSafety Research. 2024. Parenting in the Digital Age, p. 4 [Электронный ресурс]. – Режим доступа: <https://www.esafety.gov.au/> (дата обращения: 01.05.2025).

164. Online Safety Act 2021 No. 76 [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.au> (дата обращения: 01.05.2025).

165. Online Safety Act 2023 [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.uk/ukpga/2023/50> (дата обращения: 21.07.2025).

166. Online Safety Amendment (Social Media Minimum Age) Act 2024 [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.au/C2024A00127/asmade/text> (дата обращения: 01.05.2025).

167. Online Safety and Media Regulation Act Number 41 of 2022 [Электронный ресурс]. – Режим доступа: <https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/html> (дата обращения: 01.05.2025)

168. Online Safety Code 2024 (Coimisiún na Meán) [Электронный ресурс]. – Режим доступа: <https://www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf> (дата обращения: 01.05.2025).

169. Österreichische Jugendziele 30. September 2020 wurden 28 (aller Bundesministerien beschlossen) [Электронный ресурс]. – Режим доступа: <https://www.bundeskanzleramt.gv.at/agenda/jugend/oesterreichische-jugendstrategie/jugendziele.html> (дата обращения: 01.05.2025).

170. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [Электронный ресурс]. – Режим доступа: <https://ogdpr.eu/> (дата обращения 30.03.2025).

171. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [Электронный ресурс]. – Режим доступа: <https://ogdpr.eu/> (дата обращения: 30.03.2025).

172. Regulation EU 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Электронный ресурс]. – Режим доступа: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (дата обращения: 01.05.2025).

173. S.1409 Kids Online Safety Act 2023 [Электронный ресурс]. – Режим доступа: <https://www.congress.gov/bill/118th-congress/senate-bill/1409> (дата обращения: 01.05.2025).

174. Sexual Offences Act 2003/ UK Public General Acts 2003 [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.uk/ukpga/2003/42/contents/enacted> (дата обращения: 01.05.2025).

175. Sozialgesetzbuch (SGB VIII) [Электронный ресурс]. – Режим доступа: <https://www.sozialgesetzbuch-sgb.de/sgbviii/7.html> (дата обращения: 28.03.2025).

176. Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nr. 351) geändert worden ist [Электронный ресурс]. – Режим доступа: <https://www.gesetze-im-internet.de/stgb/BJNR001270871.html> (дата обращения: 01.05.2025).

177. Stratégie nationale française de sécurité de l'information [Электронный ресурс]. – Режим доступа: [https://cyber.gouv.fr/sites/default/files/IMG/pdf/2011-02-15\\_Defense\\_et\\_securite\\_des\\_systemes\\_d\\_information\\_strategie\\_de\\_la\\_France.pdf](https://cyber.gouv.fr/sites/default/files/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf) (дата обращения: 01.05.2025).

178. Sweden Unveils Ambitious Cybersecurity Strategy for 2025-2029 [Электронный ресурс]. – Режим доступа: <https://www.government.se/> (дата обращения: 01.05.2025).

179. The Bail Act 2013 No 26 (NSW) [Электронный ресурс]. – Режим доступа: <https://legislation.nsw.gov.au/view/pdf/asmade/act-2013-26> (дата обращения: 21.07.2025).

180. The Computer Fraud and Abuse Act 1986 (CFAA) [Электронный ресурс]. – Режим доступа: <https://www.congress.gov/bill/99th-congress/house-bill/4718> (дата обращения: 01.05.2025).

181. Young Offenders Act 1997 No 54 (NSW) [Электронный ресурс]. – Режим доступа: <https://legislation.nsw.gov.au/view/pdf/asmade/act-1997-54> (дата обращения: 21.07.2025).

182. Директива № 2016/1148 Европейского парламента и Совета Европейского Союза «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» [рус., англ.] (Принята в г. Страсбурге 06.07.2016) [Электронный ресурс] // Официальный сайт законодательства Европейского Союза. – Режим доступа: <http://eur-lex.europa.eu> (дата обращения: 30.03.2025).

183. Директива № 2022/2555 Европейского парламента и Совета Европейского Союза «О мерах по обеспечению высокого общего уровня кибербезопасности на территории Союза, о внесении изменений в Регламент (ЕС) 910/2014 и Директиву (ЕС) 2018/172, а также об отмене Директивы (ЕС) 2016/1148 (Директива NIS 2)» [рус., англ.] [Электронный ресурс] // Официальный сайт законодательства Европейского Союза. – Режим доступа: <http://eur-lex.europa.eu/> (дата обращения: 30.03.2025). [Россия не участвует].

184. Договор о функционировании Европейского Союза [рус., англ.] (Вместе со «Списком, предусмотренным в статье 38...», «Заморскими странами и территориями, к которым применяются положения части четвертой Договора...») (Подписан в г. Риме 25.03.1957) (с изм. и доп. от 13.12.2007) [Электронный ресурс]. – Режим доступа: <http://eur-lex.europa.eu/> дата обращения: 01.05.2025).

185. Европейская стратегия «Лучший Интернет для детей+» (European strategy for a better Internet for kids (BIK+)) 11/05/2022 [Электронный ресурс]. – Режим доступа: <https://eur-lex.europa.eu> (дата обращения: 01.05.2025).

186. Закон об административных решениях (судебном пересмотре) Австралии от 16 июня 1977 г. (Administrative decisions (judicial review) Act 1977) [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.au/Details/C2013C00365> (дата обращения: 01.05.2025).

187. Замечание общего порядка № 20 (2016) об осуществлении прав ребенка в подростковом возрасте [Электронный ресурс]. – Режим доступа: [https://fgbu-ac.ru/international\\_obligations/2/1/2\\_52.G1640448.pdf](https://fgbu-ac.ru/international_obligations/2/1/2_52.G1640448.pdf) (дата обращения: 30.03.2025).

188. Замечание общего порядка № 4 (2003) «Здоровье и развитие подростков в контексте Конвенции о правах ребенка» CRC/GC/2003/4 от 1 июля 2003 года [Электронный ресурс]. – Режим доступа: <https://european-court-help.ru/zamechanie-obshhego-porjadka-4-2003-god-zdorove-i-razvitie-podrostkov-v-kontekste-konvencii-o-pravah-rebenka/> (дата обращения: 01.05.2025).

189. Замечание общего порядка №20 об осуществлении прав ребенка в подростковом возрасте. Конвенция о правах ребенка ООН [Электронный ресурс]. – Режим доступа: <https://docs.un.org/ru/CRC/C/GC/20> (дата обращения 30.03.2025).

190. Кодекс Республики Беларусь об административных правонарушениях от 6 января 2021 г. № 91-З (с изм. и доп. по сост. на 20.02.2025 г.) [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: <https://pravo.by/document/?guid=11031&p0=НК2100091> (дата обращения: 01.05.2025).

191. Кодекс Республики Казахстан от 5 июля 2014 года № 235-V ЗРК (с изм. и доп. по сост. на 09.04.2025 г.) [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/K1400000235> (дата обращения: 01.05.2025).

192. Кодекс Республики Узбекистан об административной ответственности (утв. Законом Республики Узбекистан от 22 сентября 1994 г. N 2015-XII (с изм. и доп. по сост. на 28.04.2025 г.) [Электронный ресурс]. – Режим доступа: <https://lex.uz/ru/docs/97661> (дата обращения: 01.05.2025).

193. Лиссабонский договор, изменяющий Договор о Европейском Союзе и Договор об учреждении Европейского Сообщества (Лиссабон, 13 декабря 2007 г.) (2007/С 306/01) [Электронный ресурс]. – Режим доступа: <https://eulaw.ru/treaties/lisbon/> (дата обращения: 01.05.2025).

194. Регламент (EU) 2019/881 Европейского парламента и Совета от 17 апреля 2019 года «О Европейском агентстве по кибербезопасности ENISA и сертификации информационных и коммуникационных технологий, а также об отмене Регламента (EU) № 526/2013».

195. Регламент (ЕС) 2021/784 Европейского парламента и Совета от 29 апреля 2021 года о борьбе с распространением террористического контента в интернете (текст с учётом ЕЭЗ) [Электронный ресурс]. – Режим доступа: <https://eur-lex.europa.eu/eli/reg/2021/784/oj> (дата обращения: 01.05.2025).

196. Регламент № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» // Official Journal of the European Union N L 119. 04.05.2016. P. 1. (пер. на русск. яз.).

197. Регламент Европейского Парламента и Совета Европейского Союза 2022/2065 от 19 октября 2022 г. о едином рынке цифровых услуг и о внесении изменений в Директиву 2000/31/ЕС (Акт о цифровых услугах) // СПС Гарант.

198. Рекомендация № 2006/952/ЕС Европейского парламента и Совета Европейского Союза «О защите несовершеннолетних и человеческого достоинства, а также о праве на ответ в отношении конкурентоспособности европейской аудиовизуальной и онлайн-индустрии информационных услуг» [Электронный ресурс]. – Режим доступа: <http://eur-lex.europa.eu/> (дата обращения: 01.05.2025).

199. Рекомендация № CM/Rec (2018)7 Комитета министров Совета Европы «О соблюдении, защите и осуществлении прав детей в цифровой среде» (Вместе с «Руководящими принципами...») (Принята 04.07.2018 на 1321-м заседании представителей министров) // Бюллетень Европейского суда по правам человека. Российское издание. – 2018. – № 12.

#### **4) Судебные решения и материалы**

200. Постановление Пленума Верховного Суда РФ от 01.02.2011 № 1 (ред. от 28.10.2021) «О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних» // Российская газета. – 11.02.2011. – № 29; Российская газета. – 12.11.2021. – № 257.

201. Постановление Пленума Верховного Суда РФ от 29.06.2010 № 17 (ред. от 16.05.2017) «О практике применения судами норм, регламентирующих участие потерпевшего в уголовном судопроизводстве» // Российская газета. 07.07.2010. – № 147; Российская газета. – 24.05.2017. – № 110.

202. Постановление Пленума Верховного Суда Российской Федерации от 24 февраля 2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» // СПС «КонсультантПлюс».



203. Обзор судебной практики рассмотрения гражданских дел, связанных с нарушением авторских и смежных прав в информационно-телекоммуникационной сети «Интернет» (утв. Президиумом Верховного Суда РФ 29.05.2024) // СПС «КонсультантПлюс».

204. Обзор судебной практики Верховного Суда Российской Федерации № 4 (2021) применения судами общей юрисдикции ч. 1.1 ст. 6.13 КоАП РФ, утвержденного Президиумом Верховного Суда Российской Федерации 16.02.2022 // СПС «КонсультантПлюс».

205. Обзор судебной практики Верховного Суда Российской Федерации № 2 (2021) (утв. Президиумом ВС РФ 30.06.2021) // СПС «КонсультантПлюс».

206. Кассационное определение Второго кассационного суда общей юрисдикции от 19.12.2024 № 77-3490/2024 (приговор: По п. «д» ч. 2 ст. 110 УК РФ (доведение до самоубийства)) // СПС «КонсультантПлюс».

207. Постановление Второго кассационного суда общей юрисдикции от 29 апреля 2022 г. № 16-2483/2022 «О привлечении к ответственности по ч. 1.1 ст. 6.13 КоАП РФ за пропаганду наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства» // СПС «КонсультантПлюс».

208. Постановление Арбитражного суда Дальневосточного округа от 26.02.2024 № Ф03-6598/2023 по делу № А51-3988/2023 // СПС «КонсультантПлюс».

209. Постановление Арбитражного суда Московского округа от 03.02.2022 N Ф05-34646/2021 по делу № А40-1845/2021 // СПС «КонсультантПлюс».

210. Постановление Арбитражного суда Центрального округа от 25.04.2025 № Ф10-77/2025 по делу N А09-8618/2023 // СПС «КонсультантПлюс».

211. Постановление Чусовского городского суда Пермского края от 13 июля 2022 г. по делу N 5-194/2022 «О привлечении к административной ответственности по статье 6.13 КоАП РФ» // СПС «КонсультантПлюс».

212. Постановления Советского районного суда города Липецка от 19 января 2022 г. по делу N 5-22/2022 и от 26 июля 2022 г. по делу № 5-321/2022 «О

привлечении к административной ответственности по статье 6.13.1 КоАП РФ (пропаганда закиси азота)» // СПС «КонсультантПлюс».

213. Решение № 12-115/2017 от 26 апреля 2017 г. по делу № 12-115/2017 Ленинского районного суда г. Саратова. – Режим доступа: <https://actofact.ru/case-64RS0046-12-115-2017-2017-04-03-1-1/> (дата обращения: 01.05.2025).

214. Решение Верховного суда Республики Алтай от 30.11.2017 № 21-81/2017 (Жалоба на определение об отказе в возбуждении дела об административном правонарушении по ст. 5.61 КоАП РФ (оскорбление) оставлена без изменения) // СПС «КонсультантПлюс».

215. Решение Московского городского суда от 15.11.2021 по делу № 7-17345/2021 «О привлечении к ответственности по ч. 1 ст. 6.17 КоАП РФ за нарушение законодательства о защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс».

216. Решение Череповецкого городского суда Вологодской области от 22 декабря 2021 г. по делу № 12-1016/2021 «Об отмене актов о привлечении к административной ответственности по ст. 5.61 КоАП РФ (оскорбление)» // СПС «КонсультантПлюс».

217. CJEU. Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia de Datos (AEPD) and. ECLI: EU:C:2014:317. – Режим доступа: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131> (дата обращения: 01.05.2025).

218. X v Twitter Inc [2017] NSWSC 1300 (28 September 2017). – Режим доступа: <https://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html> (дата обращения: 01.05.2025).

## II. ЛИТЕРАТУРА

### 1) Монографии, учебники и учебные пособия

*На русском языке*

219. Абрамов В. И. Права ребенка в России (теоретический аспект) / Под ред. Н. И. Матузова. – Саратов : СГАП, 2005. – 324 с.
220. Алексеев С. С. Теория права. – М. : Издательство БЕК, 1995. – 320 с.
221. Астемиров З. А. Уголовная ответственность и наказание несовершеннолетних. – М. : Изд-во ВШ МВД СССР, 1970. – 125 с.
222. Бачило И. Л. Информационное право. Основы практической информатики : учеб. пособие. – М. : Юринформцентр, 2001. – 352 с.
223. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право / Под ред. Топорнина Б. Н. – СПб. : Юридический центр Пресс, 2001. – 789 с.
224. Ветошкин С. А. Ювенальное право: уч. пос. – Екатеринбург : ГОУ ВПО, 2009. – 230 с.
225. Глобализация и развитие законодательства. Очерки / Отв. ред. А. С. Пиголкин, Ю.А. Тихомиров. – М. : Городец, 2004. – 464 с.
226. Голенко Д. В. Преступления против жизни и здоровья: учеб. пособие. – Самара : Изд-во Самарского ун-та, 2019. – 137 с.
227. Головненков П. В. Уголовное уложение Федеративной Республики Германия – Strafgesetzbuch (StGB) : Научно-практический комментарий и перевод текста закона. – Universitätsverlag Potsdam, М. : Проспект, 2021. – 312 с.
228. Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере : монография / Н. С. Волкова, А. А. Ефремов, С. М. Зырянов и др.; отв. ред. Л. К. Терещенко. – М. : Инфотропик Медиа, 2024. – 352 с.
229. Гражданский процесс : учебник для студентов высших юридических учебных заведений / Отв. ред. В. В. Ярков. – 10-е изд., перераб. и доп. – М. : Статут, 2017. – 721 с.
230. Моисеев Н. Н. Человек, наука и общество. – М. : Наука, 1982. – 240 с.
231. Молодежная политика: европейский опыт. Доклады ИЕ РАН № 163 / Отв. ред. А. Ю. Борка. – М. : ИЕ РАН, 2005. – 65 с.
232. Постатейный комментарий к Кодексу РФ об административных правонарушениях. Часть первая / Р. В. Амелин, А. В. Колоколов, М. Д. Колоколова и др.; под общ. ред. Л. В. Чистяковой. – М. : ГроссМедиа, 2019. – Т. 1. – 1343 с.

233. Правовое регулирование защиты несовершеннолетних от деструктивной информационной среды : монография / Под общ. ред. С. Е. Титор. М. : РУСАИНС, 2025. – 350 с.

234. Словарь по этике / Под ред. И. С. Кона. – М. : Политиздат, 1984. – 447 с.

235. Смирнов А. И. Информационная глобализация и Россия: вызовы и возможности. – М. : Парад, 2005. – 392 с.

236. Стернин И. А., Антонова Л. Г., Карпов Д. Л., Шаманова М. В. Выявление признаков унижения чести, достоинства, умаления деловой репутации и оскорбления в лингвистической экспертизе текста. – Ярославль, 2013. – 35 с.

237. Цимбал В. Н., Толстых М. Ю. Противодействие деструктивному контенту в сети Интернет. – М. : Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя (Москва), 2023. – 52 с.

*На иностранных языках*

238. Crofts P., Rijswijk Honni van. Bringing Cyber Hate Under Control Through a Pro-active Legal Approach: An Australian Case Study // In book: Handbook on Cyber Hate. Volume 13 of Law and Visual Jurisprudence Book Series. – Cham : Springer, 2024 – P. 261-274.

239. Freeman M. A Commentary on the United Nations Convention on the Rights of the Child, Article 3: The Best Interests of the Child. Martinus Nijhoff; First Edition. – Boston, 2007. – 79 p.

240. Greene S., Asmolov G., Fagan A., Fridman O., Gjuzelov B. Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them. Study requested by the AFET Committee. European Parliament: Policy Department for External Relations, Directorate General for External Policies of the Union. PE 653.621. – 2021. – 104 p.

241. Hanson K. Schools of Thought in Children's Rights // M. Liebel, K. Hanson, I. Saadi and W. Vandenhoe (eds.), *Children's Rights from Below: Cross-Cultural Perspectives*, Palgrave Macmillan, 2012. – 282 p.

242. Hanson K. Children's Participation and Agency When They Don't "Do the Right Thing". – *Childhood*, 2016. – 471 p.

243. Hollingsworth K. Theorising Children's Rights in Youth Justice: The Significance of Autonomy and Foundational Rights // *The Modern Law Review* 1046 (76), at 1060. – 2013.

244. Kshetri N. *Global Cybersecurity: Key Issues and Concepts. The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies* / N. Kshetri (ed.). – Springer International Publishing, 2016. – 264 p.

245. Kuner C. and others. *The EU General Data Protection Regulation (GDPR): A Commentary / Update of Selected Articles*. – Oxford University Press, 2020. – 1486 p.

246. Liefaard, T. *Juvenile Justice from an International Children's Rights Perspective* // W. Vandenhoe, E. Desmet, D. Reynaert and S. Lembrechts (eds.), *Routledge International Handbook of Children's Rights Studies*, 2015. – 234 p.

247. *Les pouvoirs de l'administration dans le domaine des sanctions. Etude adoptée par l'Assemblée Générale du Conseil d'Etat le 8 décembre 1994*. – Paris: Les pouvoirs de l'administration dans le domaine des sanctions 1995. – 197 p.

248. Stalford H. *Introduction: The EU as a Children's Rights Actor: Law, Policy and Structural*. *The EU as a Children's Rights Actor*. – Publisher: Barbara Budrich publisher, 2015. – 11 p.

249. *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation* (ed. by R. Greifeneder, M. E. Jaffé, E. J. Newman, N. Schwarz). – N.Y. : Routledge, 2020. – 240 p.

250. Tisdall, E.K.M. *Children and Young People's Participation: A Critical Consideration of Article 12* // W. Vandenhoe, E. Desmet, D. Reynaert and S. Lembrechts (eds.). *Routledge International Handbook of Children's Rights Studies*. – London: Routledge, 2015. – 185 p.

## 2) Научные статьи

### *На русском языке*

251. Абраменко Е. В. Кибермоббинг как глобальная интернет-проблема в молодежной среде // *Primo Aspectu*. – 2024. – № 2 (58). – С. 31-39.
252. Авакьян С. А. Задачи конституционного права в аспекте защиты (от) информации // *Конституционное и муниципальное право*. – 2022. – № 8. – С. 3-11.
253. Акимова А. Н., Афанасьева Л. И. Особенности интернет-зависимости подростков // *Проблемы современного педагогического образования*. – 2024. – № 84-1. – С. 390-392.
254. Амировой Д. К. Понятие «ребёнок» в категориальном аппарате уголовно-правового регулирования: проблемы законодательной регламентации и совершенствования // *Вестник Казанского юридического института МВД России*. – 2022. – № 4 (50). – С. 40–46.
255. Аникина Н. А., Чувашова Я. А. Некоторые аспекты информационной безопасности и кибербезопасности. Проблемная зона // *Научный альманах*. – 2024. – № 1-3 (111). – С. 24.
256. Аратова А. А. Квалификация оскорбления // *Административное право и процесс*. – 2012. – № 11. – С. 60.
257. Астафичев П. А. Законодательство о защите детей от приносящей им вред информации в механизме ограничений конституционных прав граждан на информацию и доступ к культурным ценностям // *Конституционное и муниципальное право*. – 2020. – № 2. – С. 17-22.
258. Ащепкова М. М., Маглинова Т. Г. Что такое цифровая безопасность: обзор, типы и применение / *Актуальные проблемы международных отношений в условиях формирования мультиполярного мира : сборник научных статей*, Курск, 15 декабря 2023. – Курск : Университетская книга, 2023.
259. Баландин А. Ю. Кибербезопасность и информационная безопасность. Демаркация правовых категорий // *Правовая политика и правовая жизнь*. – 2023. – № 3. – С. 261.

260. Балашова Т. Н. Соотношение понятий «ребенок» и «несовершеннолетний» в законодательстве Российской Федерации / Закон и право. – 2019. – № 11. – С. 32-36.

261. Бандурка И. Понятие ребенка в национальном законодательстве и международно-правовых документах // Закон и жизнь. – 2015. – № 8. – С. 36.

262. Банщикова С. Л., Гольяпина И. Ю. Обязанности родителей по обеспечению информационной безопасности несовершеннолетних детей и административная ответственность за неисполнение обязанности // Вестник Сибирского института бизнеса и информационных технологий. – 2018. – № 1 (25). – С. 95-100.

263. Бахман А.Р. Об актуальности создания детского кодекса в России // Вестник Томского государственного университета. – 2011. – № 352. – С. 120-122.

264. Бахрах Д.Н. Дисциплинарно-правовое принуждение в Российской Федерации // Государство и право. – 2006. – № 6. – С. 46.

265. Бегларян С. Д. К вопросу о правовом регулировании обеспечения безопасности детей в информационной среде // Актуальные проблемы права, экономики и управления: сборник материалов студенческой научной конференции, посвященной памяти заслуженного деятеля науки Российской Федерации, учёного-правоведа, доктора юридических наук, профессора М. Н. Марченко. – М., 2022. – С. 357-361.

266. Беликова К. М. Некоторые направления и риски использования нейросетей для борьбы с деструктивным контентом: мнение юриста // Юрист. – 2025. – № 2. – С. 8-13.

267. Беликова С. Б., Туаева С. О. К вопросу о снижении возраста привлечения к административной ответственности // Инновации. Наука. Образование. – 2021. – № 29. – С. 508-514.

268. Белозерцева В. В. Доступ несовершеннолетнего к правосудию как неотъемлемое право человека // Вестник Восточно-Сибирского института МВД России. – 2024. – № 3 (110). – С. 9-18.

269. Белякова Е. Г., Загвязинская Э. В., Березенцева А. И. Информационная культура и информационная безопасность школьников // Образование и наука. – 2017. – Т. 19. – № 8. – С. 147-162.

270. Борисенко А. В. Понятие кибербезопасности. Кибербезопасность государственных органов // Актуальные проблемы развития экономических, финансовых и кредитных систем : сб. материалов X Междунар. научно-практич. конф. – Белгород, 2022. – С. 297-299.

271. Бородин К. В. Правовая защита несовершеннолетних от информации, приносящей вред их здоровью и развитию, распространяющейся в сети Интернет // Актуальные проблемы российского права. – 2016. – № 7(68). – С. 68-74.

272. Бошаева Л. Л. Интернет-технологии как способ вовлечения несовершеннолетнего лица в преступную деятельность // Право и государство: теория и практика. – 2022. – № 4 (208). – С. 153-155.

273. Бриллиантов А. В. Новые особенности уголовной ответственности и наказания несовершеннолетних // Российский судья. – 2004. – № 2. – С. 13.

274. Буданов С. А., Гаврилов С. Т. Информационная безопасность несовершеннолетних: правовой аспект // Территория науки. – 2015. – № 2. – С. 165-169.

275. Букалерева Л. А. Защита прав и интересов детей в информационной сфере требует внимания // Вестник Московского университета им. С. Ю. Витте. Серия 2: Юридические науки. – 2019. – № 4 (22). – С. 58.

276. Булаков О. Н. Взаимодействие уполномоченного при президенте Российской Федерации по правам ребенка с институтами гражданского общества по вопросам защиты прав и законных интересов несовершеннолетних // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2021. – № 1 (57). – С. 47-53.

277. Бурдин К. К. Понятийный аппарат как точка роста юридической науки и практики // Теория и практика общественного развития. – 2024. – № 7 (195). – С. 175-180.



278. Венцель С. В. Особенности мониторинга противоправного контента в интернете в рамках киберволонтерской деятельности // Обзор. НЦПТИ. – 2021. – № 1 (24). – С. 30-37.

279. Власенко М. С. Обеспечение информационной безопасности несовершеннолетних в сети Интернет: современное состояние и совершенствование правового регулирования // Вестник Волжского университета им. В. Н. Татищева. – 2019. – Т. 1, № 3. – С. 98-105.

280. Гаврилова Л. В. Разграничение преступления и административного правонарушения как научная и нормотворческая проблема в ФРГ // Академический юридический журнал. – 2003. – № 3.

281. Гезгиев М. А. Ответственность несовершеннолетних за административные правонарушения // Право и управление. – 2023. – № 7. – С. 298-302.

282. Геляхов К. Э. Информационная безопасность несовершеннолетних: конституционно-правовой аспект // Научные исследования студентов и учащихся : сборник статей X Международной научно-практической конференции. – Пенза, 2023. – С. 63.

283. Голикова А. В. Обоснование формирования перечня уголовных проступков посредством перераспределения деяний в КоАП РФ и УК РФ // Право и практика. – 2020. – № 3. – С. 77-83.

284. Гольяпина И. Ю., Мухаметова Д. Ф. Нормативно-правовое обеспечение информационной безопасности детей // Инновационная экономика и общество. – 2017. – № 3 (17). – С. 71-79.

285. Гришина Т. М. Обеспечение безопасности российского бизнеса в сетевом обществе: некоторые правовые вопросы // Безопасность бизнеса. – 2017. – № 4. – С. 3-8.

286. Грищенко Г. А., Никишин В. Д. Проблемы правового регулирования деструктивной информации // В сб.: Организация работы по предупреждению деструктивной идеологии в подростковой среде. Материалы научно-практической конференции. – Москва, 2025. – С. 24-27.

287. Дадаева М. С. Государственная система кибербезопасности и предупреждение экстремизма среди несовершеннолетних // Современные научные исследования и разработки. – 2018. – Т. 1. – № 5 (22). – С. 183.

288. Дедов Д. И., Гаджиев Х. И. Сфера применения права на забвение: комментарий к Постановлению Большой палаты Европейского суда по правам человека по делу «Хурбейн против Бельгии» // Журнал зарубежного законодательства и сравнительного правоведения. – 2024. – № 2. – С. 84-94.

289. Демидова И.А. Понятие информации: теоретико-прикладной аспект // Актуальные вопросы развития правовой информатизации в условиях формирования информационного общества. Сборник научных статей // Под общей ред. Е. И. Коваленко. – Минск, 2017. – С. 342-349.

290. Динисламова А. З. Административно-правовой статус субъектов обеспечения информационно-психологической безопасности несовершеннолетних // Полиция и общество: проблемы и перспективы взаимодействия. – 2023. – № 5. – С. 58-67.

291. Дугенец А. С., Павлова Л. В. Государственное регулирование обеспечения информационной безопасности несовершеннолетних как составляющая национальной безопасности России // Административное право и процесс. – 2023. – № 5. – С. 22-25.

292. Емельянов В. М. Правовое положение несовершеннолетнего в административно-юрисдикционном производстве // Правопорядок: история, теория, практика. – 2019. – № 3 (22). – С. 6-11.

293. Емельянов Д.С. Ограничение права на свободу слова в эпоху социальных сетей // Образование и право. – 2021. – № 3. – С. 46-53.

294. Жукова Т. А., Сайфуллина Н. А. Соотношение понятий «ребёнок», «несовершеннолетний», «малолетний», «подросток», «дети» в юридической науке // В сб.: Наука и инновации в современном мире. Сборник научных статей. – Москва, 2018. – С. 249-254.

295. Зайцев И. А. Административная ответственность за оскорбление, совершенное публично с использованием информационно-телекоммуникационных

сетей, включая сеть Интернет // Административное право и процесс. – 2023. – № 8. – С. 54-60.

296. Занина Т. М., Лукина Е. И. Формирование государственной системы защиты несовершеннолетних от вредоносной информации в Российской Федерации // Научный вестник Омской академии МВД России. – 2016. – № 3 (62). – С. 40-44.

297. Захаров Г. Н. Некоторые вопросы обеспечения безопасности детей в сети Интернет // В сб.: Социально-правовые аспекты трансформации института современной семьи в контексте реализации государственной семейной политики. Сборник статей по материалам международной научно-практической конференции, посв. 25-летию принятия Семейного кодекса Российской Федерации // Под общ. ред. О. Ю. Ильиной. – 2020. – С. 76-79.

298. Зеленцов А. Б. Концептуальные подходы к определению административного права: опыт сравнительно-правового исследования // Административное право и процесс. – 2019. – № 7. – С. 5-21.

299. Зеленцов А. Б. Частное лицо как субъект административного права // Административное право и процесс. – 2025. – № 2. – С. 3-20.

300. Зеленцов А. Б., Гацолати В. Э. Административно-правовые аспекты взаимодействия правоохранительных органов и организаций гражданского общества // Вестник Сургутского государственного университета. – 2020. – № 3(29). – С.78-87.

301. Зоз В. А., Лагуточкина А. С. Об отдельных направлениях правового регулирования сетевой безопасности цифровой среды в условиях противодействия подростковой преступности // Вестник Саратовской государственной юридической академии. – 2022. – № 6 (149). – С. 289-297.

302. Иванов С. В. Информационная безопасность детей (теоретико-правовой аспект) // Вестник Екатерининского института. – 2011. – № 2(14). – С. 62-66.

303. Иванский В. П. Правовая сущность информации в условиях использования цифровых технологий // RUDN Journal of Law. – 2025. – Т. 29. – № 1. – С. 221–234.

304. Ильгова Е. В., Сметанникова А. И. К вопросу о снижении возраста административной ответственности // Вестник Саратовской государственной юридической академии. – 2018. – № 5 (124). – С. 58-61.

305. Ищейнов В. Я. Информационная безопасность и защита информации : учеб. пособие. – М. : Директ-Медиа, 2020. – 271 с.

306. Как подтвердить учётную запись ребёнку с 14 лет. – Режим доступа: [https://www.gosuslugi.ru/help/faq/login\\_child/252144](https://www.gosuslugi.ru/help/faq/login_child/252144) (дата обращения: 01.05.2025).

307. Карауш И. С., Куприянова И. Е., Кузнецова А. А. Кибербуллинг и суицидальное поведение подростков // Суицидология. – 2020. – Т. 11. – № 1(38). – С. 117-129.

308. Каримова Г. Ю. Некоторые проблемные аспекты административной ответственности несовершеннолетних // Евразийский юридический журнал. – 2021. – № 4 (155). – С. 119-120.

309. Картавенко У. А. Квалификация мелкого хищения как административного правонарушения // Международный журнал гуманитарных и естественных наук. – 2024. – № 12-1 (99). – С. 128-130.

310. Кириллова Н. М. Негативный контент в информационно-телекоммуникационной сети Интернет: проблемы определения и классификации // Вестник Московского университета. Серия 11: Право. – 2018. – № 4. – С. 116-127.

311. Кириченко Ю. Н., Меняйло Д. В., Крупенникова К. К. Социально-правовые аспекты профилактики преступлений несовершеннолетних, совершаемых под влиянием деструктивного контента в сети Интернет // Научный портал МВД России. – 2024. – № 2 (66). – С. 75-81.

312. Козлова Н. Ш., Довгаль В. А. Кибербезопасность: сходства и отличия // Вестник АГУ. – 2021. – Вып. 3 (286). – С. 90.

313. Комбаров Н. В. Институт прав и свобод ребенка: понятие, содержание, признаки. – Ленинградский юридический журнал. – СПб., 2009. – С. 87.

314. Корнев А. В., Танимов О. В. Информационное право в условиях цифровой трансформации российского права : монография. – М. : Проспект, 2024. – С. 8.
315. Краснова Н. Е. Перспективы реформирования законодательства привлечения несовершеннолетних к административной ответственности // E-Scio. – 2020. – № 2 (41). – С. 60-68.
316. Крейген Д., Диакун-Тибо Н., Пёрс Р. Определение кибербезопасности // Обзор управления технологическими инновациями. – 2014. – № 4 (10). – С. 13-21.
317. Кузина Л. С. «Сетевой наркомаркетинг» как один из факторов вовлечения несовершеннолетних в незаконный оборот наркотиков // Вестник Воронежского института МВД России. – 2020. – № 4. – С. 285-290.
318. Кузнецов А. А., Ланчева Ю. А., Малец Д. С. Защита прав и свобод несовершеннолетних в цифровом пространстве // Юридический факт. – 2021. – № 148. – С. 13-15.
319. Куц Д. В., Виноградова Н. С., Третьяк Н. В. Понятие информационной безопасности государства и основные направления ее обеспечения // Вестник УрФО. – 2016. – № 3(21). – С. 56-61.
320. Лаврухин В. А. Информационная безопасность и кибербезопасность в условиях вызовов современности: актуальность, сходства, различие // Человек и образование. – 2024. – № 1 (78). – С. 126.
321. Лаптев А.С. Роль негосударственных субъектов в осуществлении регионального криминологического планирования // Бизнес и общество. – 2023. – № 2 (38).
322. Лещина Э. Л. Дисциплинарное принуждение по административному праву: понятие, признаки, структура // Вестник Нижегородского университета им. Н. И. Лобачевского. – 2018. – № 1. – С. 87-95.
323. Любченко, М. И. Правовые основы защиты несовершеннолетних от информации, причиняющей вред их здоровью и духовному развитию // Тенденции развития современной юриспруденции: материалы VII Всероссийской

студенческой научно-практической конференции Юридического института Балтийского федерального университета имени Иммануила Канта, Калининград, 19–21 апреля 2019 года / Под общ. ред. О. А. Заячковского. – Калининград : Издательство Балтийского федерального университета имени Иммануила Канта, 2019. – С. 63.

324. Мазова В. Д. Административно-правовой статус кибердружин // Правопорядок в России: проблемы совершенствования : сб. научных трудов XVIII Всероссийской научно-практической конференции». – Москва, 2024. – С. 135-137.

325. Маскальцова О. В. Формирование добровольных кибердружин как проявление гражданской инициативы противодействия распространения негативной и противоправной информации в сети «Интернет» // В сб.: Культура открытого города: волонтерство как ресурс городских проектов. Материалы Международной научно-практической конференции студентов, аспирантов и молодых ученых. Управление культуры Администрации города Екатеринбурга, МБОУ ВО «Екатеринбургская академия современного искусства» (институт). – 2020. – С. 23-27.

326. Матвеев С. П. Актуальные проблемы реализации информационных прав граждан // Административное право и процесс. – 2024. – № 12. – С. 29-33.

327. Матюшенков Д. М. Деятельность кибердружин в сфере охраны общественного порядка // Современный юрист. – 2021. – № 1 (34). – С. 34-42.

328. Медведева И. В. Проблема защиты несовершеннолетних от деструктивного контента // Государство, общество и личность в современных условиях: актуальные вопросы правового регулирования. Сборник научных статей II Всероссийской научно-практической конференции с международным участием. – Саратов, 2024. – С. 64-68.

329. Мензелинцева А. А. Защита прав ребенка в цифровом пространстве в рамках Европейского Союза // Международное право прав человека: состояние и перспективы : материалы круглого стола XVIII Международного конгресса «Блищенковские чтения». Москва, 10 декабря 2022 г. = International Law of Human Rights: Current Status and Perspectives: Proceedings of the Roundtables Discussion of

the XVIII Blischenko Congress. Moscow, 10 December 2022 / Отв. ред. А. Х. Абашидзе. – М. : РУДН, 2023. – С. 74-79.

330. Миняева Т. Ф., Серебренникова А. В. Уголовная ответственность юридических лиц в России и Германии: к постановке проблемы // *Lex russica*. – 2017. – № 2 (123). – С. 147-154.

331. Михалева Г. Г. Вопросы совершенствования административно-юрисдикционной деятельности полиции по привлечению несовершеннолетних к административной ответственности // *Аграрное и земельное право*. – 2023. – № 6 (222). – С. 72-74.

332. Недоступенко Т. А. Предупреждение противоправных действий со стороны несовершеннолетних и в отношении них: новые подходы и перспективы внедрения // *Пробелы в российском законодательстве*. – 2021. – Т. 14. – № 4. – С. 218-222.

333. Нечай А. А. Кибербезопасность и информационная безопасность: сущность, содержание и отличие понятий // В сб.: XXIV Царскосельские чтения. 75-летие Победы в Великой Отечественной войне. Материалы международной научной конференции // Под общ. ред. С. Г. Еремеева. – 2020. – С. 230.

334. Никишин В. Д., Осипов С. А. Меры противодействия деструктивному контенту: опыт и перспективы // *Обзор.НЦПТИ*. – 2024. – № 4 (39). – С. 14-25.

335. Новгородов Д. А. Административные наказания за правонарушения, совершаемые посредством сети Интернет, и практика их применения // *Научный портал МВД России*. – 2017. – № 4. – С. 11.

336. Новикова Н. В., Брылева Е. А. О некоторых аспектах информационной безопасности несовершеннолетних на примере Пермского края // *Вопросы ювенальной юстиции*. – 2013. – № 6. – С. 7-9.

337. Номоконов В. А. «Криминализация» административного права или административный произвол криминализации? // *Библиотека криминалиста*. – 2013. – № 2. – С. 208-213.

338. Обыденнова Т. В. Правовое регулирование административной ответственности несовершеннолетних // Административное и муниципальное право. – 2012. – № 6. – С. 67-69.

339. Оловенцова С. Ю. Информационная безопасность несовершеннолетних: условия возникновения и средства предупреждения // Уголовная ответственность и наказание : сб. материалов Международной научно-практической конференции, посв. памяти профессоров кафедры уголовного права Рязанской высшей школы МВД СССР В. А. Елеонского и Н. А. Огурцова / Под ред. В. Ф. Лапшина. – Рязань, 2018. – С. 139-144.

340. Омельченко А. В., Седова А. А. К вопросу о снижении возраста привлечения к административной ответственности // Еромен. Global. – 2023. – № 37. – С. 103-107.

341. Петрова О. Н. Роль наказания в превенции преступности несовершеннолетних в свете изменений Уголовного кодекса Российской Федерации // Преступность как она есть и направления антикриминальной политики. – М., 2004. – С. 155-160.

342. Полякова Т. А., Смирнов А. А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Российский юридический журнал. – 2022. – № 3. – С. 7-15.

343. Полянина А. К., Чистяков В. А. Государственное управление и институт детского омбудсмена в сфере обеспечения информационной безопасности личности // Общество: политика, экономика, право. – 2024. – № 6 (131). – С. 47-54.

344. Правиков Д. И., Петухов А. В. Кибербезопасность как новое фундаментальное направление в области информационной безопасности / Вестник современных цифровых технологий. – 2019. – № 1. – С. 17-23.

345. Пресняков М. В. Ментальные права: конституционное содержание и допустимость ограничений // Конституционное и муниципальное право. – 2024. – № 9. – С. 45-53.

346. Прохорова Д. А. Международная информационная безопасность как современная проблема // Информационное общество. – 2022. – № 5. – С. 80-90.



347. Пучков О. А. Разграничение понятий «информационная безопасность» и «кибербезопасность» в законодательстве Российской Федерации, доктрине и юридической практике // Право и государство: теория и практика. – 2019. – № 5 (173). – С. 66-69.

348. Ренжигло Р. Е. Влияние деструктивного интернет-контента на формирование экстремистских взглядов у молодежи // Вестник Донецкого национального университета. Серия Е: Юридические науки. – 2023. – № 2. – С. 43-50.

349. Романовский В. Г. Правовые основы противодействия терроризму в цифровом пространстве // Ex Jure. – 2022. – № 4. – С. 163-177.

350. Рыдченко К. Д. Запрещенная для детей информация: легальная трактовка и толкование правоприменителя // Информационное право. – 2014. – № 5. – С. 16-21.

351. Савва Ю. Б., Савва Т. Ю. Использование искусственного интеллекта при модерации деструктивного контента социальных сетей // В сб.: Интеллектуальные информационные системы. Труды Международной научно-практической конференции, посв. 40-летию кафедры САПРИС. – Воронеж, 2024. – С. 133-136.

352. Садина О. В. Правовой статус несовершеннолетнего в российском законодательстве: теоретико-правовой анализ. – Мытищи, 2010. – С. 20.

353. Сарабеков А. А. Регулирование цифровых платформ и интернет-услуг: правовые аспекты и перспективы // Universum: экономика и юриспруденция. – 2024. – № 11-1 (121). – С. 40-43.

354. Ситкова О. Ю. Механизмы регулирования информационного потребления в странах Европейского союза в целях обеспечения кибербезопасности детей // Правовая политика и правовая жизнь. – 2021. – № 4. – С. 58-68.

355. Смирнов А. А. Обеспечение информационно-психологической безопасности детей в Европейском союзе // Информационное право. – 2010. – № 4. – С. 30-34.

356. Соколова О. С. Защита персональных данных посредством права на забвение // Современное право. – 2016. – № 9. – С. 69-72.
357. Солдатов А. П. Гарантии и обеспечение прав в границах местного самоуправления. – Славянск-на-Кубани : СГПИ, 2015. – 387 с.
358. Соловьева С. В. Механизм реализации административной ответственности за возбуждение ненависти или вражды // Право и практика. – 2020. – № 3. – С. 72-77.
359. Статьев В. Ю., Тиньков В. А. Информационная безопасность распределенных информационных систем // Информационное общество. – 1997. – № 1. – С. 68.
360. Стрельникова В. Н. Системный подход к обеспечению информационной безопасности детства // Вестник Самарского университета. История, педагогика, филология. – 2021. – Т. 27. – № 4. – С. 92-98.
361. Стуканов А. П., Соловьева А. К. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства: проблемы привлечения к административной ответственности // Законность. – 2019. – № 8. – С. 29-33.
362. Сургуладзе В. Ш. Новые категории информационной борьбы: mis-, dis-, malinformation и правовые последствия использования модели информационного беспорядка mdm // Власть. – 2024. – Т. 32. – № 1. – С. 23-30.
363. Талапина Э. В. Административное право Франции сегодня // В сб.: «Ежегодник сравнительного правоведения» 2004 год // Общество сравнительного правоведения. – М., 2005. – С. 136-151.
364. Талапина Э. В. Право на забвение: французский опыт // Конституционное и муниципальное право. – 2023. – № 11. – С. 42-45.
365. Талапина Э. В. Цифровая трансформация во Франции: правовые новеллы // Право. Журнал Высшей школы экономики. – 2019. – № 4. – С. 164–184.
366. Ткачев И. О. Использование информационно-телекоммуникационных сетей как квалифицирующий признак состава преступления // Уголовное право. – 2024. – № 10. – С. 72-83.

367. Тогузаева Е. Н. Опыт закрепления запрета пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду, в конституциях стран – членов Содружества Независимых Государств // Современное право. – 2013. – № 8. – С. 131-134.

368. Токарева А. В. Подходы к трактовке понятий «несовершеннолетний» и «ребенок» в конституционном праве Российской Федерации // Наука и мир. – 2015. – № 9. – С. 171-173.

369. Трофимова Г. А. Совершеннолетний ребенок: пробелы в правовом статусе // Адвокат. – 2014. – № 8. – С. 67-72.

370. Усачева Е. А. Понятие «ребенок» в категориальном аппарате семейно-правового регулирования // Законы России: опыт, анализ, практика. – 2016. – № 8. – С. 40-43.

371. Фетисов П. И. Преступления против личности, совершаемые с использованием информационно-телекоммуникационных технологий (включая сеть Интернет) // Известия Юго-Западного государственного университета. Серия: История и право. – 2024. – Т. 14. – № 2. – С. 119-130.

372. Фролова Н. А., Фархутдинов И. З., Панченко В. Ю. Фролова Н. А. Диалектическое единство развития и безопасности – платформа будущего // Евразийский юридический журнал. – 2018. – № 5 (120). – С. 13.

373. Хромова Н. М. Правовой статус несовершеннолетних: частный и публичный аспекты // Российская юстиция. – 2024. – № 8. – С. 23-34.

374. Хромова Н. М. Трансформация правового статуса несовершеннолетних с древнейших времен до наших дней // Черные дыры в российском законодательстве. – 2020. – № 2. – С. 36-39.

375. Черненко И. В. Особенности лишения свободы на определенный срок для несовершеннолетних // Вестник Кемеровского государственного университета. – 2006. – № 1. – С. 17.

376. Чубукова С. Г. Проблемы правового статуса информационного посредника // Вестник Академии права и управления. – 2017. – № 2 (47). – С. 39-44.

377. Чудинов С. И. Классификация девиантно-деструктивного контента в социальной сети ВКонтакте // Российская наука и образование сегодня: проблемы и перспективы. – 2024. – № 4 (59). – С. 64-68.

378. Шарипов, А. М. Информационная безопасность в современных условиях: понятие, сущность // Обеспечение безопасности личности, общества и государства в условиях глобализации: правовые и организационные проблемы и перспективы: сб. статей Всероссийской научно-практической конференции студентов, магистров и молодых ученых, посв. 50-летию юридического образования в Удмуртской Республике. – Ижевск, 2022. – С. 129-134.

379. Шарофзода Р. Ш., Шокиров Г. А. Информация как объект юридического научного познания и правового воздействия // Правовая жизнь. – 2021. – № 3 (35). – С. 5-22.

380. Шварц Л. В. Проблемы нормативно-правового регулирования распределения полномочий Российской Федерации и ее субъектов в сфере обеспечения информационной безопасности детей // Вестник Санкт-Петербургской юридической академии. – 2021. – № 4 (53). – С. 70-76.

381. Шитов А. М. Анализ информационных систем родительского контроля web-ресурсов // Актуальные вопросы современной науки : сб. научных статей по материалам II Международной научно-практической конференции. – Уфа, 2023. – С. 200-205.

382. Шкатулов К. О. К вопросу о снижении возрастного порога для привлечения к административной ответственности // Молодой ученый. – 2020. – № 21(311). – С. 418-421.

383. Шуликов К. А. Деструктивный контент: понятие, административно-правовая характеристика, виды // Вестник Нижегородского университета им. Н. И. Лобачевского. – 2023. – № 2. – С. 176-182.

384. Шуликов К. А. Субъекты противодействия распространению деструктивного контента в сети Интернет и административно-правовая характеристика их деятельности // Административное право и процесс. – 2024. – № 8. – С. 69-73.

385. Яхина Н. Д., Тулупова Е. О. Понятие «несовершеннолетний» в законодательстве Российской Федерации. Соотношение с понятием «ребенок» // E-Scio. – 2022. – № 10 (73). – С. 635-641.

*На иностранных языках*

386. Aitken S. C. Global Crises of Childhood: rights, justice and the unchildlike child // Area. – 2001. – № 33(2). – P. 119-127.

387. Bateman W., McDonald L. The Normative Structure of Australian Administrative Law // Federal Law Review. – 2017. – № 45(2). – P. 153-179.

388. Büttne C. The Protection of Minors Against Harmful Media Content in Europe // Nordicom Review. – 2005. – № 26(1). – P. 121-129.

389. Bygrave, L. A. Information Concepts in Law: Generic Dreams and Definitional Daylight // Oxford Journal of Legal Studies. – 2014. – № 35(1). – P. 91–120. – (quote from p. 112).

390. Cabral, L., Haucap J., Parker G., Petropoulos G., et al. The EU Digital Markets Act // Publications Office of the European Union, Luxembourg. – 2021. – 1-36 p.

391. Corcoran B.. A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace. Harvard National Security Journal 11 // 2020. – № 1. – P. 1–9.

392. Daly A. No Weight for “Due Weight”? A Children’s Autonomy Principle in Best Interest Proceedings’, 26 // The International Journal of Children’s Rights 61. – 2018.

393. Desmet E. Implementing the Convention on the Rights of the Child for ‘youth’: who and how? // International Journal of Children’s Rights. – 2012. – № 20. – P. 3–23.

394. Dong H., Yang F., Lu X., Hao W. Internet Addiction and Related Psychological Factors Among Children and Adolescents in China During the Coronavirus Disease 2019 (COVID-19) Epidemic // Frontiers in Psychiatry. – 2020. – Vol. 275. – P. 112-118.

395. Eekelaar J. The Emergence of Children's Rights // Oxford Journal of Legal Studies. – 1986. – Vol. 6(161). – P. 170-171.
396. Freeman M. Taking Children's Rights More Seriously // International Journal of Law and the Family. – 1992. – Vol. 6 (52). – P. 59.
397. Freeman M. Why It Remains Important to Take Children's Rights Seriously // The International Journal of Children's Rights. – 2007. – Vol. 15(1). – P. 5-23.
398. Fuster G. G. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights // The Ethics of Cybersecurity. – 2020. – Pp. 97-115.
399. Gengler B. FTC rules for children on the Internet // Computer Fraud & Security. – 1999. – Vol. (6). – P. 8-9.
400. Guggenberger N. Das Netzwerkdurchsetzungsgesetz in der Anwendung // Neue Juristische Wochenschrift. – 2017. – № 36. – P. 2577-2582.
401. Hallinan D., Gellert R. The Concept of «Information»: An Invisible Problem in the GDPR // SCRIPT-ed. – 2020. – Vol. 17(2). – P. 269-319.
402. Hanson K., Peleg N. Waiting for Children's Rights Theory // International Journal of Children's Rights. – 2020. – Vol. 28 (15). – P. 1-28.
403. Hanson K., Peleg N. Waiting for Children's Rights Theory // International Journal of Children's Rights. – 2020. – Vol. 28 (1). – P. 15-35.
404. Hartzog W., Solove D. J. The scope and potential of FTC data protection. November 2015 // The George Washington law review. – 2015. – Vol. 83(6). – P. 2230-2300.
405. Hu T. The Role of Age Verification Systems in Protecting Minors from Harmful Online Content in Australia // International Journal of Social Sciences and Public Administration. – 2025. – Vol. 6(2). – P. 134-141.
406. Jarvie C., Renaud K. Online Age Verification: Government Legislation, Supplier Responsibilization, and Public Perceptions // Children. – 2024. – Vol. 11(9). – P. 1068.
407. Kabelka, L. German Youth Protection Body Endorses AI as Biometric Age-Verification Tool [Электронный ресурс]. – 2022. – Режим доступа:

<https://www.euractiv.com/section/digital/news/german-youth-protection-body-endorses-ai-as-biometric-age-verification-tool/> (дата обращения: 01.05.2025).

408. Kladzinski M. Jugendmedienschutz in Polen // tv-diskurs. – 2003. – Vol. 23. – P. 4-1.

409. Likhota O. Legislative support of the US information policy // Economics Finances Law. – 2025. – Vol. 3/2024(-). – P. 65-68.

410. Lindskoug P. Global content orders: A legal analysis of eSafety Commissioner 14 Legal Theories of Private International Law: Overview and Practical Implications for Internet Regulation // Essays in Honour of Michael Bogdan. – 2013. – P. 539-555.

411. Ludvigsen K. R. Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law [Электронный ресурс]. – 2025. – Режим доступа: <https://www.researchgate.net/> (дата обращения: 30.03.2025).

412. Moreno F. R. Generative AI and deepfakes: a human rights approach to tackling harmful content // International review of law, computers & technology. – 2024. – Vol. 38 (№ 3). – P. 297–326.

413. Nolan S. A., Kimball M. The Intent behind a Lie: Mis-, Dis-, and Malinformation. Can you differentiate among the varieties of untruths you encounter online? [Электронный ресурс] // Psychology Today. – 2021. – Режим доступа: <https://www.psychologytoday.com/> (30.03.2025).

414. Pardhey N., Dias R. T., Irfan M., Galvão R. M., et al. 3.3 Children and youth rights in the digital era and environmental development through binding legal instruments / Insight Into Child and Youth Safety Online Via International Laws Edges. Revista de Gestão Social e Ambiental. – 2024. – Vol. 18(9). – P. 1-20.

415. Peukert A. The Regulation of Disinformation in the EU – Overview and Open Questions (June 30, 2023) [Электронный ресурс] // Research Paper of the Faculty of Law of Goethe University Frankfurt/M. – 2023. – № 2/2023. – Режим доступа: SSRN: <https://ssrn.com/abstract=4496691> (30.03.2025).

416. Phippen A. Online Safety Policy–Moving On? // Policy and Rights Challenges in Children’s Online Behaviour and Safety. – 2025. – 2017–2023. – Pp. 1-18.

417. Rap S. Safeguarding the Dynamic Legal Position of Children: A Matter of Age Limits? // *Erasmus Law Review*. – 2020. – Vol. 1. – P. 4-12.

418. Ritleng D. Chronique Jurisprudence administrative française intéressant le droit de l'UE - Le Conseil d'État rappelle comment faire le filtre des QPC portant sur des lois de transposition d'une directive européenne // *Revue générale de droit international public*. – 2019. – Vol. 1. – P. 1-12.

419. Sani A. I., Vara M., Dinis M. A. P. Online Sexual Grooming of Children: Psychological and Legal Perspectives for Prevention and Risk Management // *Modern Insights and Strategies in Victimology*. – 2024. – Pp. 25-55. – Chapter: 2 Publisher: IGI Global.

420. Santos-D'Amorim, K., de Miranda, M. K. F. d. O.. Misinformation, disinformation, and malinformation: Clarifying the definitions and examples in disinfodemic times // *Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação*. – 2021. – Vol. 26. – P. 1-23.

421. Scheffle S. Age Verification Systems Will Be a Personal Identifiable Information Nightmare // *Communications of the ACM*. – 2024. – Vol. 67(7). – P. 31-33.

422. Smith M., Nolan M., Gaffey J. Online safety and social media regulation in Australia: eSafety Commissioner v X Corp. // *Griffith Law Review*. – 2024. – Vol. 33(1). – P. 1-17.

423. Staksrud E., Livingstone S. Children and online risk: Powerless victims or resourceful participants? // *Information, Communication & Society*. – 2009. – Vol. 12(3). – P. 364-387.

424. Svantesson D. «Scope of Jurisdiction» – A Key Battleground for Private International Law Applied to the Internet, *Yearbook of Private International Law*. These ten principles were first. – 2020. – Vol. 22. – P. 245–274.

425. Svantesson D., Jerker B., Symeonides S. C. Cross-border internet defamation conflicts and what to do about them: Two proposals // *Journal of Private International Law*. – 2023. – № 19(2). – P. 137-185.

426. Svantesson, D. Global content orders: A legal analysis of eSafety Commissioner v X Corp. (May 7, 2024) [Электронный ресурс]. – 2024. – Режим



доступа: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4819178](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4819178) (дата обращения: 01.05.2025).

427. Svantesson, D. J. B. Internationalisation of Law in the Digital Information Society // Nordic yearbook of Law and Informatics 2010-2012. – 2013. – Vol. 21. – P. 195-215.

428. Szpor G. The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland // Review of European and Comparative Law. – 2021. – № 46(3). – P. 219-235.

429. Talley, V. A. M. Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR // Indiana Int'l & Comp. Law Review. – 2019. – Vol. 30(1). – P. 127-162.

430. Tobin J. Seeking to Persuade: A Constructive Approach to Human Rights Treaty Interpretation // Harvard Human Rights Journal. – 2010. – Vol. 23. – P. 1-50.

431. Tobin J. Understanding a Human Rights Based Approach to Matters Involving Children: Conceptual Foundations and Strategic Considerations // A. Invernizzi, J. Williams (eds.). The Human Rights of Children: From Visions to Implementation. – 2011. – Vol. 61. – P. 78.

432. Trotter S. The Child in European Human Rights Law // Modern Law Review. – 2018. – Vol. 81(3). – P. 452-479.

433. Watney M. Regulation of social media intermediary liability for illegal and harmful content // European Conference on Social Media. – 2022. – Vol. 9(1). – P. 194-201.

434. Yeung K., Bygrave L. A. Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship // Regulation & Governance. – 2021. – Vol. 16(2). – P. 1-9.

### **3) Диссертации и авторефераты диссертаций**

435. Банщикова С. Л. Административная ответственность за неисполнение родителями или иными законными представителями несовершеннолетних

обязанностей по их содержанию и воспитанию : автореф. дис. ... канд. юрид. наук : 12.00.14 / Банщикова Светлана Леонидовна; [Место защиты: Ом. гос. ун-т им. Ф. М. Достоевского]. – Омск, 2017. – 35 с.

436. Буданов С. А. Правовое обеспечение информационной безопасности несовершеннолетних : дис. ... канд. юрид. наук : 05.13.19 / Буданов С. А.; Воронеж. ин-т МВД России. – Воронеж, 2006. – 220 с.

437. Гирис В. А. Правовое регулирование деятельности Европейского Союза в области обеспечения кибербезопасности : автореф. дис. ... канд. юрид. наук : 5.1.5 / Гирис Валерия Алексеевна; [Место защиты: ФГАОУ ВО «Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)» ; Диссовет Д 212.123.XX (24.2.336.04)]. – Москва, 2024. – 29 с.

438. Горбачева Е. В. Административное правовое обеспечение информационной безопасности несовершеннолетних: диссертация на соискание ученой степени кандидата юридических наук: 12.00.14 / Горбачева Елена Владимировна; [Место защиты: Рост. юрид. ин-т МВД РФ]. Ростов-на-Дону, 2011. 206 с.

439. Дегтярева Л. Н. Конституционно-правовая защита несовершеннолетних в современной России (на примере Центрального федерального округа) : дис. ... канд. юрид. наук : 12.00.02 <Конституционное право; муниципальное право> / Дегтярева Леся Николаевна; [Елец. гос. ун-т им. И. А. Бунина]. – Белгород 2010. – 242 с.

440. Капитонова Е. А. Конституционные обязанности ребенка в Российской Федерации : автореф. дис. ... канд. юрид. наук : 12.00.02 / Капитонова Елена Анатольевна; [Место защиты: Сарат. гос. ун-т им. Н. Г. Чернышевского]. – Пенза, 2010. – 25 с.

441. Кубышкин А. В. Международно-правовые проблемы обеспечения информационной безопасности государства : дис. ... канд. юрид. наук : 12.00.10 / Кубышкин Алексей Викторович [Место защиты: Московская государственная юридическая Академия]. – Москва, 2002. – 193 с.

442. Кузнецова Е. В. Предупреждение делинквентного поведения несовершеннолетних, продуцируемого контентом сети Интернет : автореф. дис. ... канд. юрид. наук : 12.00.08 / Кузнецова Елена Владимировна. – Курск, 2019. – 25 с.

443. Леонов Р. А. Общественно опасные деяния (проступки), совершаемые лицами, не достигшими возраста уголовной ответственности (уголовно-правовой и криминологический аспекты) : дис. ... канд. юрид. наук : 12.00.08 / Леонов Роман Анатольевич; [Сарат. юрид. ин-т МВД России], [Место защиты: Моск. гос. лингвист. ун-т]. – Саратов, 2011. – 194 с.

444. Маурин В. С. Правовой анализ вредной информации в условиях информационного общества : дис. ... канд. юрид. наук : 12.00.14 / Маурин Владимир Сергеевич. – Москва, 2004. – 190 с.

445. Муратова Е. В. Административная юстиция в Австралии : автореф. дис. ... канд. юрид. наук : 12.00.14 / Муратова Елена Владимировна; [Место защиты: Рос. ун-т дружбы народов]. – Москва, 2013. – 21 с.

446. Рыдченко К. Д. Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации : дис. ... канд. юрид. наук : 12.00.14 / Рыдченко Кирилл Дмитриевич; [Место защиты: Воронеж. гос. ун-т]. – Воронеж, 2011. – 308 с.

447. Федотова О. А. Административная ответственность за правонарушения в сфере обеспечения информационной безопасности : дис. ... канд. юрид. наук : 12.00.14 / Федотова, Ольга Анатольевна. – Москва, 2003. – 195 с.

448. Шуликов К. А. Административно-правовые основы противодействия распространению деструктивного контента в сети «Интернет» : дис. ... канд. юрид. наук : 5.1.2. / Шуликов Кирилл Андреевич; [Место защиты: ФГАОУ ВО «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» ; Диссовет 99.2.091.02 (99.2.091.02)]. – Санкт-Петербург, 2024. – 238 с.

#### 4) Электронные ресурсы

449. 95 % of UK internet is censored? 23 February 2009. Aaisp.net.uk [Электронный ресурс]. – Режим доступа: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.76a79339-676433cc-d5666dd6-74722d776562/https/web.archive.org/web/20111101215616/http://aaisp.net.uk/news-censorship.html](https://translated.turbopages.org/proxy_u/en-ru.ru.76a79339-676433cc-d5666dd6-74722d776562/https/web.archive.org/web/20111101215616/http://aaisp.net.uk/news-censorship.html) (дата обращения: 01.05.2025).

450. «Лига безопасного интернета» готовит документ, призванный законодательно ограничить в России доступ к ресурсам, содержащим детское порно, пропаганду наркотиков и экстремистские материалы [Электронный ресурс] / Минцифры РФ. – Режим доступа: <https://digital.gov.ru/ru/events/28870/> (дата обращения: 01.05.2025).

451. Administrative Review Tribunal Act 2024 [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.au/C2024A00040/latest/text> (дата обращения: 01.05.2025).

452. Advice on child internet safety 1.0 [Электронный ресурс]. – Режим доступа: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/251455/advice\\_on\\_child\\_internet\\_safety.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251455/advice_on_child_internet_safety.pdf) (дата обращения: 21.07.2025).

453. Advisory Committee on Disinformation and Misinformation Terms of Reference 29 November 2024 [Электронный ресурс]. – Режим доступа: <https://www.ofcom.org.uk/siteassets/resources/documents/about-ofcom/how-ofcom-is-run/mis-and-dis-information-committee/advisory-committee-on-disinformation-and-misinformation-terms-of-reference.pdf?v=386330> (дата обращения: 01.05.2025).

454. Australian Cyber Security Strategy [Электронный ресурс]. – Режим доступа: <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy> (дата обращения: 21.07.2025).

455. Beschwerdeverfahrenjugendschutz.net [Электронный ресурс]. – Режим доступа: <https://www.jugendschutz.net/ueber-uns/beschwerdeverfahren> (дата обращения: 01.05.2025).

456. Children and youth. EU youth dashboard [Электронный ресурс]. – Режим доступа: <https://ec.europa.eu/eurostat/web/children-youth/database/eu-youth-dashboard> (дата обращения: 30.03.2025).

457. Commonwealth law uses the term ‘child abuse material’ to capture material that depicts or represents the sexual or physical abuse of a person who is or appears to be under 18 years of age [Электронный ресурс]. – Режим доступа: <https://www.criminalsolicitorsmelbourne.com.au/blog/child-abuse-material> (дата обращения: 01.05.2025).

458. Department of Communications and the Arts, Online Safety Legislative Reform: Discussion Paper, (Canberra: Department of Communications and the Arts, December 2019), p. 36 [Электронный ресурс]. – Режим доступа: <https://www.communications.gov.au> (дата обращения: 01.05.2025).

459. Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001 [Электронный ресурс]. – Режим доступа: <https://rm.coe.int/16800cse5b> (дата обращения: 01.05.2025).

460. FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Childrens Online Privacy Protection Rule [Электронный ресурс]. – Режим доступа: <https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over-their-information-amending-childrens> (дата обращения: 01.05.2025).

461. German youth protection body endorses AI as biometric age-verification tool [Электронный ресурс]. – Режим доступа: <https://www.euractiv.com/section/digital/news/german-youth-protection-body-endorses-ai-as-biometric-age-verification-tool/> (дата обращения: 01.05.2025).

462. Guidelines on the implementation of the Court of Justice of the European Union judgment in the case of Google Spain SL and Google Inc. v. Agencia Espanola de Protection de Datos (AEPD) and Mario Costeja Gonzalez (C-131/12).

463. International Youth Service of the Federal Republic of Germany [Электронный ресурс]. – Режим доступа: <https://www.kinder->

jugendhilfe.info/ru/obshchie-ramochnye-uslovija/obshchestvo/deti-podrostki-i-molodye-vzroslye (дата обращения: 28.03.2025).

464. IWF [Электронный ресурс]. – Режим доступа: <https://www.iwf.org.uk/contact-us/> (дата обращения: 01.05.2025).

465. Module 8. (2022) «False News», Misinformation and Propaganda. Summary Modules on litigating Digital Rights and Freedom of Expression Online. London: Media Defense. November. 2022 11 p. [Электронный ресурс]. – Режим доступа: <https://www.mediadefence.org> (дата обращения: 01.05.2025).

466. Online age verification: balancing privacy and the protection of minors [Электронный ресурс]. – Режим доступа: <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors> (дата обращения: 01.05.2025).

467. Press release. Strategy to protect and empower children in the online world. European Commission. – 11.05.2022. – [Электронный ресурс]. – Режим доступа: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_2825](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2825) (дата обращения: 01.05.2025).

468. Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy [Электронный ресурс]. – Режим доступа: <https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy> (дата обращения: 01.05.2025).

469. Safer Internet Day [Электронный ресурс]. – Режим доступа: <https://www.webwise.ie/saferinternetday/> (дата обращения: 01.05.2025).

470. Statement on removal of extreme violent content 23/4/24 [Электронный ресурс]. – Режим доступа: <https://www.esafety.gov.au/newsroom/media-releases/statement-on-removal-of-extreme-violent-content> (дата обращения: 01.05.2025).

471. The Children's Online Privacy Protection Rule (COPPA Rule) [Электронный ресурс]. – Режим доступа: <https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule> (дата обращения: 01.05.2025).

472. The IWF: Charity disparity? The Register [Электронный ресурс]. – Режим доступа: [https://www.theregister.com/2009/02/20/iwf\\_charity/](https://www.theregister.com/2009/02/20/iwf_charity/) (дата обращения: 01.05.2025).

473. Réseaux sociaux : l'accord parental obligatoire pour les mineurs de moins de 15 ans définitivement adopté par le Parlement [Электронный ресурс]. – Режим доступа: [https://www.lemonde.fr/pixels/article/2023/06/29/reseaux-sociaux-vote-final-au-parlement-pour-instaurer-un-accord-parental-obligatoire-pour-les-mineurs-de-moins-de-15-ans\\_6179745\\_4408996.html](https://www.lemonde.fr/pixels/article/2023/06/29/reseaux-sociaux-vote-final-au-parlement-pour-instaurer-un-accord-parental-obligatoire-pour-les-mineurs-de-moins-de-15-ans_6179745_4408996.html) (дата обращения: 01.05.2025).

474. The State of the World's Children 2011. United Nations Children's Fund (UNICEF) [Электронный ресурс]. – Режим доступа: <https://www.unicef.org/media/84876/file/SOWC-2011.pdf> (дата обращения: 01.05.2025).

475. Sydney to be become the Internet content blocking capital of the world? [Электронный ресурс]. – Режим доступа: <https://www.linkedin.com/pulse/sydney-become-internet-content-blocking-capital-world-svantesson/?trackingId=yA8980A1Q0GE23P4zsRsjw%3D%3D> (дата обращения: 01.05.2025).

476. World Health Organization. Toxicological and Health Aspects of Bisphenol A [Электронный ресурс]. – Режим доступа: [http://apps.who.int/iris/bitstream/handle/10665/44624/97892141564274\\_eng.pdf?sequence=1](http://apps.who.int/iris/bitstream/handle/10665/44624/97892141564274_eng.pdf?sequence=1) (дата обращения: 31.03.2023).

477. Yoti. Yoti Age Scan. 2021 [Электронный ресурс]. – Режим доступа: <https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-May-2022.pdf> (дата обращения: 01.05.2025).

478. В Госдуме разработали законопроект о «кибердружинах» [Электронный ресурс]. – Режим доступа: <https://otr-online.ru/news/v-gosdume-razrabotali-zakonoproekt-o-kiberdruzhinah-114027.html> (дата обращения: 01.05.2025).

479. В российской полиции остро не хватает сотрудников (22 января 2025) [Электронный ресурс]. – Режим доступа: <https://lenta.ru/articles/2025/01/22/police/> (дата обращения: 01.05.2025).

480. Дети в интернете / ИСИЭЗ. 2023. 1 июня [Электронный ресурс]. – Режим доступа: <https://issek.hse.ru/news/837320649.html?ysclid=m4schi9m1400480739> (дата обращения: 01.05.2025).

481. Дорожная карта по проверке возраста Комиссара по электронной безопасности [Электронный ресурс]. – Режим доступа: <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification> (дата обращения: 01.05.2025).

482. Информационное агентство ТАСС [Электронный ресурс]. – Режим доступа: <https://tass.ru/obschestvo/24919635> (дата обращения: 21.08.2025).

483. Кибердружина. Народный Фронт [Электронный ресурс]. – Режим доступа: <https://onf.ru/cyberguard> (дата обращения: 01.05.2025).

484. Кибердружина. Центр информационной безопасности и психологической помощи молодежи Ханты-Мансийского автономного округа – Югры [Электронный ресурс]. – Режим доступа: <https://cybersquad.ru/> (дата обращения: 01.05.2025).

485. Киберпатруль [Электронный ресурс]. – Режим доступа: <http://киберпатруль.рф/> (дата обращения: 01.05.2025).

486. Концепция Стратегии кибербезопасности Российской Федерации (проект). [Электронный ресурс]. – Режим доступа: <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf> (дата обращения 30.03.2025).

487. Куликов В. Почему предлагают снизить возраст наказания подростков в новом КоАП // Российская газета. Столичный выпуск. № 110 (7868) [Электронный ресурс]. – Режим доступа: <http://rg.ru/2019/05/22/pochemu-predlagaiut-snizit-voznrast-nakazaniia-podrostkov-v-novom-koap.html> (дата обращения: 01.05.2025).

488. Лаборатория Касперского. Исследование «Лаборатории Касперского»: дети онлайн [Электронный ресурс]. – Режим доступа: <https://securelist.ru/issledovanie-laboratorii-kasperskogo-deti-onlajn/25212/> (дата обращения: 01.05.2025)



489. Мизулина попросит Генпрокуратуру проверить детские книги // РИА Новости. 2024. 14 ноября. [Электронный ресурс]. – Режим доступа: <https://ria.ru/20241114/kultura-1983783129.html> (дата обращения: 01.05.2025).

490. На страже интересов онлайн-пользователей: борьба с кибербуллингом в Германии // Сайт Федерального министерства иностранных дел Германии [Электронный ресурс]. – Режим доступа: <https://germania-online.diplo.de/ru-dz-ru/gesellschaft/neuerordner/2419918-2419918> (дата обращения: 01.05.2025).

491. Национална стратегия за киберсигурност «Киберустойчива България 2020 [Электронный ресурс]. – Режим доступа: <https://cyberbg.eu/> (дата обращения: 01.05.2025).

492. Общий регламент защиты персональных данных ЕС [Электронный ресурс] / Общ. ред. С. Воронкевич. – Режим доступа: <https://gdpr-text.com/ru/> (дата обращения: 01.08.2025).

493. Онлайн-платформа цифровых консультаций и безопасности в сети «Интернет» «РосКибербезопасность» [Электронный ресурс]. – Режим доступа: <https://roskiber.ru/> (дата обращения: 01.05.2025).

494. Отчет «Лаборатория Касперского» от 23.05.2024 «Взрослые и дети в интернете: аналитический отчет 2023» [Электронный ресурс]. – Режим доступа: <https://kids.kaspersky.ru> (дата обращения: 01.05.2025).

495. Официальный портал судов общей юрисдикции города Москвы [Электронный ресурс]. – Режим доступа: <https://mos-gorsud.ru/rs/tverskoj/services/cases/civil/details/de7ea6a0-a3ab-11ec-8a7e-51b31fb55b35> (дата обращения: 01.12.2024).

496. Официальный сайт. Ассоциация по сертификации возрастных проверок (Age Check Certification Scheme, ACCS) [Электронный ресурс]. – Режим доступа: <https://avpassociation.com/> ) дата обращения: 01.05.2025).

497. Официальный сайт «Headspace» [Электронный ресурс]. – Режим доступа: <https://www.healthdirect.gov.au/> (дата обращения: 01.07.2025).

498. Официальный сайт «The Australian Child Rights Taskforce» [Электронный ресурс]. – Режим доступа: <https://childrightstaskforce.org.au/> (дата обращения: 01.07.2025).

499. Официальный сайт «Альянс по защите детей в цифровой среде» [Электронный ресурс]. – Режим доступа: <https://internetforkids.ru/> (дата обращения: 01.05.2025).

500. Официальный сайт «Государственная образовательная платформа «Российская электронная школа»» [Электронный ресурс]. – Режим доступа: <https://resh.edu.ru/> (дата обращения: 01.05.2025).

501. Официальный сайт Internet Watch Foundation [Электронный ресурс]. – Режим доступа: <https://www.iwf.org.uk/> (дата обращения: 01.05.2025).

502. Официальный сайт Kids Helpline [Электронный ресурс]. – Режим доступа: <https://kidshelpline.com.au/> (дата обращения: 01.07.2025).

503. Официальный сайт OFCOM [Электронный ресурс]. – Режим доступа: <https://www.ofcom.org.uk/about-ofcom/structure-and-leadership/advisory-committee-on-disinformation-and-misinformation> (дата обращения: 01.05.2025).

504. Официальный сайт UKCIS [Электронный ресурс]. – Режим доступа: <https://www.gov.uk/government/organisations/uk-council-for-internet-safety> (дата обращения: 01.05.2025).

505. Официальный сайт АНО «ЦИСМ» [Электронный ресурс]. – Режим доступа: <https://cism-ms.ru/poleznye-materialy> (дата обращения: 01.05.2025).

506. Официальный сайт АО «Газета.Ру» [Электронный ресурс]. – Режим доступа: <https://www.gazeta.ru/social/news/2025/08/26/26580014.shtml?updated> (дата обращения: 31.08.2025).

507. Официальный сайт Ассоциация «Лига безопасного интернета» [Электронный ресурс]. – Режим доступа: <https://ligainternet.ru/o-nas/> (дата обращения: 01.05.2025).

508. Официальный сайт Европейского союза [Электронный ресурс]. – Режим доступа: <https://better-internet-for-kids.europa.eu/en/about/unsafe-inhope> (дата обращения: 01.05.2025).

509. Официальный сайт Европейской комиссии ЕС [Электронный ресурс]. – Режим доступа: [https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online\\_en](https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en) (дата обращения: 01.12.2024)

510. Официальный сайт ООН. Безопасность детей и молодежи в Интернете [Электронный ресурс]. – Режим доступа: <https://www.un.org/ru/global-issues/child-and-youth-safety-online> (дата обращения: 01.05.2025).

511. Официальный сайт Уполномоченного по правам ребенка в ЯНАО [Электронный ресурс]. – Режим доступа: <https://yamalchild.ru/?p=1683> (дата обращения: 01.05.2025).

512. Официальный сайт ФНС [Электронный ресурс]. – Режим доступа: <https://egrul.nalog.ru/index.html> (дата обращения: 01.05.2025).

513. Официальный сайтg GmbH «jugendschutz.net» [Электронный ресурс]. – Режим доступа: <https://www.jugendschutz.net/> (дата обращения: 01.05.2025).

514. Положение об использовании сети «Интернет» в МБОУ «Столбовская СОШ» [Электронный ресурс]. – Режим доступа: [https://shkolastolbovskaya-r22.gosweb.gosuslugi.ru/netcat\\_files/30/69/polozhenie\\_ob\\_ispol\\_zovanii\\_seti\\_Internet\\_podpisano.pdf](https://shkolastolbovskaya-r22.gosweb.gosuslugi.ru/netcat_files/30/69/polozhenie_ob_ispol_zovanii_seti_Internet_podpisano.pdf) (дата обращения: 01.05.2025).

515. Положение об использовании сети Интернет в образовательном учреждении» Отдела образования Администрации Белокалитвинского района [Электронный ресурс]. – Режим доступа: <https://sosh12.bkobr.ru/deyatelnost/informatsionnaya-bezopasnost/dokumenty-shkoly/2333-polozhenie-ob-ispolzovanii-seti-internet-v-obrazovatelnom-uchrezhdenii> (дата обращения: 01.05.2025).

516. Положение Об Управлении контроля и надзора в сфере электронных коммуникаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс]. – Режим доступа: <https://rkn.gov.ru/about/structure/> (дата обращения: 01.05.2025).

517. Положение об Управлении по защите прав субъектов персональных данных Федеральной службы по надзору в сфере связи, информационных

технологий и массовых коммуникаций [Электронный ресурс]. – Режим доступа: <https://rkn.gov.ru/about/structure/> (дата обращения: 01.05.2025).

518. Пользовательское соглашение Экосистемы VK [Электронный ресурс]. – Режим доступа: <https://id.vk.com/terms> (дата обращения: 01.05.2025).

519. Почему предлагают снизить возраст наказания подростков в новом КоАП (22.05.2019) [Электронный ресурс]. – Режим доступа: <https://rg.ru/2019/05/22/pochemu-predlagaiut-snizit-voznrast-nakazaniia-podrostkov-v-novom-koap.html> (дата обращения: 01.05.2025).

520. Правила пользования сайтом ВКонтакте [Электронный ресурс]. – Режим доступа: <https://vk.com/terms> (дата обращения: 01.05.2025).

521. Пресс-релиз Еврокомиссии "Agreement on Commission's EU data protection reform will boost Digital Single Market"[Электронный ресурс]. – Режим доступа: [http://europa.eu/rapid/press-release\\_IP-12-46\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en) (дата обращения: 01.05.2025).

522. Преступления, совершаемые в сети «Интернет» [Электронный ресурс]. – Режим доступа: <https://prokuratura-zo-krd.ru/pravovoe-prosveshchenie/prestupleniya-sovershaemye-v-seti-internet-0> (дата обращения: 01.05.2025).

523. Прокуратура Саратовской области [Электронный ресурс]. – Режим доступа: [https://epp.genproc.gov.ru/web/proc\\_64/mass-media/news?item=85499501](https://epp.genproc.gov.ru/web/proc_64/mass-media/news?item=85499501) (дата обращения: 01.05.2025)

524. Роскомнадзор подтвердил блокировку порталов с аниме-контентом / РИА Новости. 2024. 5 декабря [Электронный ресурс]. – Режим доступа: <https://ria.ru/20241205/roskomnadzor-1987599452.html> (дата обращения: 01.05.2025).

525. Роскомнадзор РФ ведёт Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. РКН РФ [Электронный ресурс]. – Режим доступа: <https://eais.rkn.gov.ru/> (дата обращения: 01.05.2025).

526. Россияне рассказали, в каком возрасте пора покупать ребенку телефон [Электронный ресурс]. – Режим доступа: <https://www.kp.ru/daily/27581/4851382/> (дата обращения: 01.05.2025).

527. Сайт Государственной Думы РФ. Авторы проекта о кибердружинах выслушали мнение общественников и экспертов в рамках «нулевых чтений» [Электронный ресурс]. – Режим доступа: <http://duma.gov.ru/news/29944/> (дата обращения: 01.05.2025).

528. Сайт ООН. [Электронный ресурс]. – Режим доступа: [https://www.un.org/ru/documents/decl\\_conv/conventions/beijing\\_rules.shtml](https://www.un.org/ru/documents/decl_conv/conventions/beijing_rules.shtml) (дата обращения: 27.03.2025).

529. Сайт ООН. Новые данные об использовании интернета в мире: прогресс есть, но различия сохраняются [Электронный ресурс]. – Режим доступа: <https://www.ungeneva.org/ru/news-media/news/2023/11/87882/novye-dannye-ob-ispolzovanii-interneta-v-mire-progress-est-no> (дата обращения: 01.05.2025).

530. Селфи в одежде с «конопляным» принтом: осторожно штраф! // Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – Режим доступа: <https://238.56.мвд.рф/document/21128094> (дата обращения: 01.05.2025),

531. Семейное соглашение об использовании гаджетов [Электронный ресурс]. – Режим доступа: <https://ligainternet.ru/wp-content/uploads/2022/09/semejnoe-soglashenie-ob-ispolzovanii-gadzheto-v-web.pdf> (дата обращения: 01.05.2025).

532. Сетевое издание «Интерфакс-Россия» [Электронный ресурс]. – Режим доступа: <https://www.interfax-russia.ru/northwest/main/kazhdoe-pyatoe-kiberprestuplenie-v-rf-soversheno-podrostkami-statistika-skr> (дата обращения: 21.08.2025).

533. Слово директора. Лига безопасного интернета [Электронный ресурс]. – Режим доступа: <https://ligainternet.ru/direktor/> (дата обращения: 01.05.2025).

534. Смартфон и ребенок. Почему думающие родители составляют семейное соглашение об использовании цифровых устройств [Электронный

ресурс]. – Режим доступа: <https://ligainternet.ru/semejnoe-soglashenie-ob-ispolzovanii-gadzhetrov/> (дата обращения: 01.05.2025).

535. Советы родителям по проблемам безопасности в Интернете [Электронный ресурс]. – Режим доступа: <https://ligainternet.ru/10-sovetov-roditelyam-po-bezopasnosti-v-seti/?ysclid=m500syuezp674323284> (дата обращения: 01.05.2025).

536. Ответственность за травлю (буллинг) : статья [Электронный ресурс]. – Режим доступа: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=СЛ&n=146734#ZqujryUWcAPCI9gq> (дата обращения: 01.05.2025).

537. Судебная статистика. Официальный сайт Агентства правовой информации [Электронный ресурс]. – Режим доступа: <https://stat.апи-пресс.рф/stats/adm/t/31/s/65> (дата обращения: 01.05.2025).

538. Учебный профиль Сферум в VK Мессенджере [Электронный ресурс]. – Режим доступа: <https://sferum.ru> (дата обращения: 01.05.2025).

539. Форма для приёма обращений о наличии на сайтах в сети «Интернет» запрещённой информации [Электронный ресурс]. – Режим доступа: <https://eais.rkn.gov.ru/feedback/> (дата обращения: 01.05.2025).

540. Хартия «Цифровая этика детства» [Электронный ресурс]. – Режим доступа: <https://internetforkids.ru/upload/docs/charter.pdf> (дата обращения: 01.05.2025).

541. Юридические вопросы на слушании 10 мая 2024 г. [Электронный ресурс]. – Режим доступа: <https://www.capitalbrief.com/briefing/x-says-stabbing-video-does-not-encourage-or-provoke-violence-f7fadc50-21a9-4eb2-a5f9-01f20a4788b2/> (дата обращения: 01.05.2025).

## Приложение А

### Виды деструктивного контента в сети «Интернет» для несовершеннолетних лиц

Государство	РФ	Австралия	Великобритания	ЕС	Франция	Италия	Германия
Вид контента							
<b>Незаконный (противоправный) контент</b>	Согласно ст. 5 закона № 436-ФЗ: <b>запрещенная информация</b> , предусмотренной ч. 2 ст. 5 Закона № 436-ФЗ – информации, которая влечет вред жизни и здоровью детей и подростков, склоняет к терроризму, насилию, наркотическим средствам, проституции и т. д.  Перечень запрещенной информации и ограниченный.	Согласно ст. 6 (1) Online Safety Act 2021, информация считается <b>деструктивной</b> , если обычный здравомыслящий человек пришел бы к выводу, что вполне вероятно, что материал был предназначен для воздействия на конкретного австралийского ребенка; и материал, вероятно, будет представлять для австралийского ребенка серьезную угрозу, запугивать, беспокоить или унижать его достоинство.  Обозначим, в самом законе Online Safety Act 2021 указаны классы контента (первый и второй класс), а на официальном сайте Комиссара по электронной безопасности <sup>654</sup> представлена классификация на «незаконный и оскорбительный контент» ( <b>«незаконный контент и с ограниченным доступом контент»</b> ).  В соответствии с Законом о безопасности в Интернете от 2021 года (Online Safety Act 2021), который ссылается на Национальную классификационную схему для определения материалов «класса 1» (незаконных) и «класса 2» (с ограниченным доступом), включая материалы о жестоком обращении с детьми, террористические акты, отвратительное насильственное поведение и материалы, непригодные для детей. Кроме того, положения УК Содружества (например, раздел 474) касаются	Ст. 59 закона Online Safety Act содержит описание понятия <b>«незаконный контент»</b> – «illegal content», под которым понимают контент, который является правонарушением, а именно наличие слов (текстов), аудиофайлов, видеофайлов, которые считаются правонарушением при условии: использование; хранение, просмотр, доступ, распространение подобного контента. Кроме того, в незаконном контенте выделяют «приоритетный незаконный контент», то есть «приоритетное правонарушение» (преступления связанные с террористической направленности, сексуальной эксплуатацией и насилием над детьми и другие тяжкие преступления);	Ч. (12) Преамбулы 11-20 закона о цифровых услугах (DSA) дает концептуальное понятие <b>«незаконный контент»</b> как относящееся к информации, независимо от ее формы, которая в соответствии с применимым правом сама по себе является незаконной: незаконное разжигание ненависти, террористический контент и незаконный дискриминационный контент, или которая становится незаконной в соответствии с применимыми нормами ввиду того, что она относится к противоправной деятельности. Также в качестве примеров в ч. 12 приведено: распространение изображений, демонстрирующих сексуальное насилие над детьми, незаконное распространение личных изображений без согласия владельца, онлайн-преследование. Примечание (26) Стратегии BIK+, содержит отсылку к «запрещенной» информации («незаконный контент» или «вредный контент»): «запрещено для всех пользователей: ксенофобский, террористический контент или материалы о сексуальном насилии над детьми». Но согласно ч. (34) закона о цифровых услугах (DSA) соответствующие национальные органы должны	Во Франции действуют законы, направленные на защиту детей от <b>незаконного контента</b> в сети «Интернет». Закон LOPPSI 2 от 2009 г., предусматривал, чтобы МВД создало и вело реестр сайтов, содержащих детскую порнографию, который интернет-провайдеры должны блокировать. Законы «Борьба с ненавистью в Интернете» 2020 (определенный незаконный контент, связанный с детской порнографией и терроризмом, должен быть удален в течение 1 часа после пометки – но данное положение отменено по решению Конституционного суда Франции) и Закон о защите и регулировании цифровой среды 2024 г. (SREN) направлены на защиту несовершеннолетних от порнографического контента в интернете.	Законодательный декрет № 208 от 8 ноября 2021 года определяет виды контента, которые могут нанести ущерб физическому, умственному или нравственному развитию несовершеннолетних, а именно в статьях 37 и 38 (ст. 6a(1) AVMSD) о программах, которые могут нанести серьезный вред несовершеннолетним, включая те, которые содержат: необоснованно е, настойчивое или экстремальное насилие; порнографические сцены; фильмы, которые были запрещены компетентными органами для публичного показа детям младше 18 лет.	Закон о правоприменении в сети 2017 года - (NetzDG) в абз. (3) § 4a употребляется термин <b>«незаконный контент»</b> без легальной трактовки и или характеристик данного понятия.

<sup>654</sup> Официальный сайт Комиссара по электронной безопасности // URL: <https://www.esafety.gov.au/key-topics/Illegal-restricted-content> (дата обращения: 28.08.2025)

		таких преступных деяний, как изготовление, распространение или хранение материалов, связанных с эксплуатацией детей.		иметь возможность издавать распоряжения в отношении контента, который считается незаконным			
ограниченный (вредоносный) контент	<b>ограниченная информация</b> (распространение которой среди детей определенных возрастных категорий ограничено и которая предусмотрена ч. 3 ст. 5 Закона № 436-ФЗ с учетом положений ст. 7-10 Закона № 436-ФЗ). К ограниченной информации относится контент с изображением или описанием насилия, жестокости и т. д.	статья 107 Online Safety Act 2021 содержит перечень контента, (по терминологии Комиссариата – «с <b>ограниченным доступом контент</b> ») который относится по оценкам Квалификационной комиссии (а также такой контент, который не классифицированный комиссией, но который в случае оценки, вероятно, получил бы ограничение 18+) к возрастной группе старше восемнадцати лет и который может быть опубликован только с учетом технических мер, которые пресекут доступ несовершеннолетних к данному контенту: порнографический материал; публикации, фильмы и компьютерные игры, содержащие порнографические элементы, сцены жестокости, насилия.	<b>«контент, вредный для детей»</b> – «content that is harmful to children» (ст. 60 Online Safety Act); – контент с высоким приоритетом, вредный для детей (контент, представляющий опасность для детей) – «primary priority content that is harmful to children» (ст. 61); – «приоритетный контент, вредный для детей» – «priority content that is harmful to children» (ст. 62). Согласно ст. 60 «контент, вредный для детей» включает в себя: (а) <i>контент с высоким приоритетом</i> или <i>главный приоритетный контент</i> («primary priority content that is harmful to children»), который может нанести вред детям (согласно содержанию ст. 61 данный контент содержит порнографию; информацию, которая поощряет, пропагандирует или содержит инструкции по совершению самовредительства и (или) самоубийства; расстройство пищевого поведения); (б) <i>приоритетный контент, причиняющий вред детям</i> («priority content that is harmful to children»). Так, согласно ст. 62 Online Safety Act «приоритетный контент, вредный для детей» означает контент, направленный на дискриминацию (оскорбление) или разжигание ненависти к людям какой-либо расы, сексуальной ориентации, религии, инвалидности, смены пола – которая, уточним, законодательно запрещена в России; контент, поощряющий или пропагандирующий жестокость (насилие) в отношении человека (в том числе учитывается согласно (5) ст. 62 элементы буллинга), а также	согласно возрастного рейтинга и классификации контента Стратегии BIK+  В BIK+ установлены: <b>незаконный</b> контент; <b>вредоносный</b> (вредоносный ил и несоответствующий возрасту) (illegal and <b>harmful content</b> (age -inappropriate or harmful content online)).  Вредоносный контент может прославлять и пропагандировать членовредительство, суицид, насилие, разжигание ненависти, сексуальные домогательства, употребление наркотиков, рискованные онлайн-челленджи, расстройства пищевого поведения и опасные диеты.  Стратегия Европейского союза BIK+ (Лучший Интернет для детей) использует сочетание общих принципов и конкретных, неисчерпывающих перечней для борьбы с вредным и незаконным контентом для детей в Интернете. Он направлен на защиту детей, но не содержит окончательного закрытого списка «незаконного и вредного контента», вместо этого фокусируясь на создании более безопасной онлайн-среды и обучении детей навыкам цифровой грамотности.	согласно Стратегии BIK+	согласно Стратегии BIK+	согласно Стратегии BIK+



			жестокость (насилие) в отношении животных; контент, поощряющий или пропагандирующий действия, которые травмоопасные или связанные с приемом внутрь (в том числе внутривенно или вдыханием) каких-либо веществ, способных нанести вред здоровью человека;				
<b>Иной нежелатель- ный<sup>655</sup> контент</b>		согласно системному анализу ст. Согласно ст. 6 (1) и ст. 107 Online Safety Act 2021, в том числе полномочий комиссаром по электронной безопасности	<p>(c) ст. 62 Online Safety Act устанавливает <b>«или иной контент»</b>, не относящийся к пунктам (a) или (b), <i>который представляет существенную опасность причинения значительного вреда большому количеству детей</i> в Соединённом Королевстве.</p> <p>С одной стороны, данный контент законодатель относит как разновидность «контента, вредного для детей», с другой стороны – представляет собой открытую категорию, включение в которую контента возможно на основании анализа признаков информации для несовершеннолетних.</p> <p>Таким образом, перечень контента, причиняющий для несовершеннолетних, согласно Online Safety Act является детальным и открытым.</p>				

<sup>655</sup> Понятие «*нежелательная информация (контент), размещенная в сети Интернет*» обозначено:

Письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет» (вместе с «Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования», «Рекомендациями по организации системы ограничения в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования») // Интернет-источник. URL: <https://www.consultant.ru> (дата обращения: 21.08.2025).

**Полномочия «Управления по информационной безопасности несовершеннолетних» в составе структуры Роскомнадзора**

– обеспечивать формирование и ведение информационной системы взаимодействия между Роскомнадзором, правообладателями, провайдерами хостинга, операторами связи и иными лицами при принятии мер по ограничению доступа к информации, информационным ресурсам и программным приложениям в сети «Интернет» в соответствии со статьями 10.6, 15.1 Федерального закона № 149-ФЗ;

– организовывать мониторинг сайтов и страниц сайтов в сети «Интернет» в целях реализации полномочий Управления в установленной сфере ведения;

– осуществлять проверку ограничения доступа к информации, распространение которой запрещено статьями 10.6, 15.1 Федерального закона № 149-ФЗ, со стороны провайдера хостинга или иного лица, обеспечивающего размещение в сети «Интернет» информационного ресурса;

– осуществлять проверку удаления владельцем сайта в сети «Интернет» информации, распространение которой запрещено статьями 10.6, 15.1 Федерального закона № 149-ФЗ;

– осуществлять контроль и надзор за соблюдением требований законодательства в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию на предмет соответствия требованиям российского законодательства знака информационной продукции на сайтах в информационно-телекоммуникационной сети «Интернет», не зарегистрированных в качестве средств массовой информации, если такие интернет-ресурсы содержат знак информационной продукции;

– организовывать и контролировать исполнение территориальными органами полномочий Службы в установленной сфере деятельности Управления;

- взаимодействовать с другими структурными подразделениями, территориальными органами и подведомственными предприятиями в своей сфере деятельности.

- организовывать работу горячих линий и информационных ресурсов, созданных в рамках реализации статей 10.6, 15.1 Федерального закона № 149-ФЗ.

- разработка рекомендаций, которые должны приниматься платформами социальных сетей с возрастными ограничениями;

- управление системой подачи жалоб на информацию, деструктивно влияющей на несовершеннолетних;

- требовать от операторов цифровых (электронных) платформ получения подданных проверке согласий родителей несовершеннолетних перед сбором, использованием или раскрытием информации о них (за некоторыми ограниченными исключениями, например, порталов государственных органов власти или публичных услуг);

- устанавливать и поддерживать процедуры для защиты конфиденциальности, безопасности и целостности личной информации несовершеннолетних;

- оказание образовательной, психологической поддержки несовершеннолетним и их семьям, которые столкнулись с трудностями, которые могут поставить под угрозу здоровье, безопасность, нравственность этих несовершеннолетних или серьезно поставить под угрозу их физическое, эмоциональное, интеллектуальное и психологическое развитие;

- профилактика правонарушений с участием несовершеннолетних в сети «Интернет».

***Законопроект статьи 10.8. Обязанности владельца социальных сетей в информационно-телекоммуникационной сети «Интернет»***

***«Статья 10.8. Обязанности владельца социальных сетей в информационно-телекоммуникационной сети «Интернет»***

1. Владелец социальной сети обязан при регистрации пользователя провести идентификацию и (или) аутентификацию его возраста и удостовериться, что физическое лицо достигло подросткового возраста, за исключением случаев регистрации в государственных и (или) муниципальных образовательных социальных сетях, регистрация в которых разрешена с 6,6 лет с согласия родителей (законных представителей) регистрируемого несовершеннолетнего лица.

2. Для целей регистрации пользователя в социальной сети владелец социальной сети принимает разумные меры для подтверждения возраста физического лица.

Предоставление реквизитов документов, удостоверяющих личность гражданина; страховой номер индивидуального лицевого счёта; доступ через учетную запись Единой системы идентификации и аутентификации на портале Госуслуг не могут быть единственными способами для пользователей подтвердить свой возраст на платформах социальных сетей, но все же могут быть одним из доступных вариантов.

3. Нарушение владельцем социальных сетей в сети «Интернет» требований настоящей статьи влечет за собой административную и иную ответственность в соответствии с законодательством Российской Федерации.».

## Приложение Г

**Составы административных правонарушений по КоАП РФ в сфере информационной безопасности несовершеннолетних  
в сети «Интернет»**

Статья КоАП РФ	Состав административного правонарушения			
	Объект	Объективная сторона	Субъект	Субъективная сторона
ст. 6.17	общественные отношения, связанные с защитой детей и подростков от деструктивного контента, в том числе размещенного непосредственно на информационной продукции	а) нарушении установленных требований распространения среди несовершеннолетних информационной продукции, содержащей деструктивную информацию, если это действие не содержит уголовно наказуемого деяния (ч. 1 ст. 6.17 КоАП РФ); б) неприменении лицом, организующим доступ к распространяемой посредством сети Интернет информации (за исключением операторов связи) необходимых средств защиты несовершеннолетних от деструктивной информации (ч. 2 ст. 6.17 КоАП РФ); в) размещении (в том числе в сети Интернет) в информационной продукции для детей, объявления о привлечении несовершеннолетних к участию в создании деструктивной информационной продукции	– граждане; – должностные лиц; – индивидуальные предприниматели; – юридические лица	– умысел; – неосторожность
ст. 5.61	общественные отношения в области морали и нравственности несовершеннолетних	действия, которые унижают честь и достоинство определенного лица в неприличной форме (циничной, противоречащей установленным правилам поведения, требованиям общечеловеческой морали).	– граждане; – должностные лица; – юридические лица	– умысел;
ст. 5.62	общественные отношения, связанные с защитой прав и свобод человека и гражданина, в том числе несовершеннолетнего, которые нарушаются в результате дискриминации	действия, нарушающие права, свободы и законные интересы человека и гражданина, в том числе несовершеннолетнего, в зависимости от его пола, расы, цвета кожи, национальности, языка, происхождения и т. д.	– граждане; – юридические лица	– умысел; – неосторожность
ст. 6.13	общественные отношения в сфере пропаганды оборота наркотических средств, психотропных	деяния, выражающиеся в пропаганде или незаконной рекламе наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей,	– граждане – должностные лица – индивидуальные предприниматели;	– умысел; – неосторожность

	веществ, а также в области противодействия их незаконному обороту в целях охраны здоровья граждан, в том числе несовершеннолетних	содержащих наркотические средства или психотропные вещества либо их прекурсоры, а также новых потенциально опасных психоактивных веществ.	– юридические лица; – иностранные граждане; – лица без гражданства	
ст. 6.13.1	общественные отношения в сфере охраны здоровья граждан, в том числе несовершеннолетних	пропаганда закиси азота, выраженная в распространении сведений о местах приобретения, хранения, производства, поставок, методах изготовления закиси азота не в целях производства пищевой продукции, продовольственных товаров или продуктов питания либо не для медицинского, промышленного или технического применения, в том числе в сети «Интернет»	– граждане; – должностные лица; – индивидуальные предприниматели; – юридические лица	– умышленная форма вины
ст. 6.20	общественные отношения в области соблюдения гарантий прав и законных интересов несовершеннолетнего	в изготовлении, приобретении, хранении, перевозке, распространении, публичной демонстрации либо рекламировании юридическим лицом материалов или предметов с порнографическими изображениями несовершеннолетних.	– юридические лица	– умышленная форма вины
ст. 6.21	общественные отношения в области морали и нравственности несовершеннолетнего	действия, выражающиеся в пропаганде нетрадиционных сексуальных отношений и (или) предпочтений, смены пола среди несовершеннолетних, в том числе в сети «Интернет»	– граждане; – должностные лица; – юридические лица; – иностранные граждане; – лица без гражданства	– умышленная форма вины
ст. 6.21.1	общественные отношения в области морали и нравственности несовершеннолетнего	объективная сторона выражается в совершении действий, нацеленных на распространение информации, направленной на обоснование и (или) оправдание педофилии или формирование привлекательности педофилии, либо навязывание информации о педофилии, вызывающей интерес к педофилии;	– граждане; – должностные лица; – юридические лица; – иностранные граждане; – лица без гражданства	– умышленная форма вины
ст. 6.21.2	общественные отношения в области морали и нравственности несовершеннолетнего	объективная сторона тождественна наименованию состава Распространение среди несовершеннолетних информации, демонстрирующей нетрадиционные сексуальные отношения и (или) предпочтения либо способной вызвать у несовершеннолетних желание сменить пол	– граждане; – должностные лица; – юридические лица; – иностранные граждане;	– умысел; – неосторожность

			– лица без гражданства	
ст. 5.35	общественные отношения в области защиты прав и законных интересов ребенка, в том числе в сфере информационной безопасности в сети «Интернет»	Объективную сторону правонарушения по ст. 5.35 КоАП РФ составляет неисполнение или ненадлежащее исполнение родителями или иными законными представителями несовершеннолетних обязанностей по содержанию, воспитанию, обучению, защите прав и интересов несовершеннолетних	– специальные субъекты, к которым относятся родители и иные законные представители несовершеннолетнего	– умысел; – неосторожность
ст. 19.7.10-4	общественные отношения в сфере информационной безопасности граждан, в том числе несовершеннолетних в сети «Интернет»	Неисполнение владельцем социальной сети предписания Роскомнадзора об осуществлении мониторинга социальной сети в целях выявления информации, схожей до степени смешения с информацией, меры по удалению которой владелец данной или иной социальной сети обязан принимать на основании ранее направленного требования или уведомления указанного федерального органа	– специальные субъекты, к которым относятся владельцы социальной сети	– умысел; – неосторожность

***Законопроект статьи 6.17.1. Регистрация пользователя социальной сети в информационно-телекоммуникационной сети «Интернет» без идентификации и (или) без аутентификации возраста пользователя***

*«Статья 6.17.1. Регистрация пользователя социальной сети в информационно-телекоммуникационной сети «Интернет» без идентификации и (или) без аутентификации возраста пользователя*

1. Неисполнение владельцем социальной сети обязанности по идентификации и (или) аутентификации достижения пользователем подросткового возраста при регистрации (за исключением случаев регистрации в государственных и (или) муниципальных образовательных социальных сетях, регистрация в которых разрешена с 6,6 лет с согласия родителей (законных представителей) регистрируемого несовершеннолетнего лица)), –

влечет наложение административного штрафа на граждан в размере от пятидесяти тысяч до ста тысяч рублей; на должностных лиц - от двухсот тысяч до четырехсот тысяч рублей; на юридических лиц - от шестисот тысяч до одного миллиона рублей.

2. Повторное совершение административного правонарушения, предусмотренного частью 1 настоящей статьи, –

влечет наложение административного штрафа на граждан в размере ста тысяч рублей до двухсот тысяч рублей; на должностных лиц – от четырехсот тысяч рублей до восьмисот тысяч рублей; на юридических лиц – от одного миллиона рублей до двух миллионов рублей».



## Приложение Е

### Статистика размеров административных штрафов, налагаемых на граждан в сфере информационной безопасности несовершеннолетних в сети «Интернет»

Статья КоАП РФ	Название статьи КоАП РФ	Размер административного штрафа, руб.		Год введения нормы или год последней редакции
		Минимальный размер	Максимальный размер (за повторное совершение)	
ч. 2 ст. 5.61	Оскорбление	от 5000 до 10 000	—	2020
ст. 5.62	Дискриминация	от 1000 до 3000	—	2011
ч. 1.1 ст. 6.13	Пропаганда наркотических средств, психотропных веществ или их прекурсоров <...>	от 5000 до 30 000	—	2020
ст. 6.13.1	Пропаганда закиси азота	от 1000 до 2000	—	2021
ст. 6.17	Нарушение законодательства РФ о защите детей от информации, причиняющей вред их здоровью и (или) развитию	от 2000 до 3000	—	2013
ч. 4 ст. 6.21	Пропаганда нетрадиционных сексуальных отношений и (или) предпочтений, смены пола, отказа от деторождения	от 200 000 до 400 000	—	2022
ч. 2 ст. 6.21.1	Пропаганда педофилии	от 400 000 до 800 000	—	2022
ч. 2 ст. 6.21.2	Распространение среди несовершеннолетних информации, демонстрирующей нетрадиционные сексуальные отношения и (или) предпочтения либо способной вызвать у несовершеннолетних желание сменить пол	от 100 000 до 200 000	—	2022
ч. 2, ч. 3 ст. 13.50	Неисполнение обязанностей владельцем социальной сети	от 50 000 до 100 000	от 100 000 до 200 000	2023
ст. 19.7.10-4	Неисполнение владельцем социальной сети предписания <...>	от 100 000 до 200 000	—	
ст. 5.35	Неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по содержанию и воспитанию несовершеннолетних	от 500 до 2000	—	2025