

Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации
Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя

В. Н. Цимбал, М. Ю. Толстых

ПРОТИВОДЕЙСТВИЕ ДЕСТРУКТИВНОМУ КОНТЕНТУ В СЕТИ ИНТЕРНЕТ

Учебное пособие

Москва
Московский университет
МВД России имени В.Я. Кикотя
2023

УДК 004
ББК 626.3+67
Ц61

Рецензенты:

начальник кафедры информационной безопасности Краснодарского университета МВД России доктор технических наук, профессор **А. В. Еськов**; начальник кафедры огневой и тактико-специальной подготовки Уфимского юридического института МВД России кандидат юридических наук **А. А. Романов**

Цимбал, В. Н.

Ц61 **Противодействие деструктивному контенту в сети Интернет** : учебное пособие / В. Н. Цимбал, М. Ю. Толстых. – М. : Московский университет МВД России имени В.Я. Кикотя, 2023. – 52 с.
ISBN 978-5-9694-1378-8

В пособии анализируется влияние информации деструктивного содержания или воздействия на пользователей сети Интернет. Приведен обзор некоторых особенностей интернет-контента, имеющих принципиальное значение с точки зрения психологии восприятия.

Учебное пособие предназначено для курсантов и слушателей образовательных организаций системы МВД России, обучающихся по направлению подготовки 2.3.6 «Методы и системы защиты информации, информационная безопасность», а также для слушателей групп повышения квалификации сотрудников органов внутренних дел, деятельность которых связана с мониторингом информационно-телекоммуникационных сетей на предмет наличия в них информации, распространение которой на территории Российской Федерации запрещено, ограничено или может причинять вред здоровью или развитию детей.

УДК 004
ББК 626.3+67

ISBN 978-5-9694-1378-8

© Московский университет
МВД России имени В.Я. Кикотя, 2023
© Цимбал В. Н., Толстых М. Ю., 2023

ОГЛАВЛЕНИЕ

СПИСОК ИСПОЛЪЗУЕМЫХ СОКРАЩЕНИЙ.....	4
ВВЕДЕНИЕ.....	5
ГЛАВА 1 АНАЛИЗ ДЕСТРУКТИВНОГО МАТЕРИАЛА В СЕТИ ИНТЕРНЕТ	
§ 1.1. Законодательные аспекты в области контроля проявления деструктивных материалов в сети Интернет.....	6
§ 1.2. Виды, формы и классификация деструктивных материалов в сети Интернет.....	15
<i>Вопросы для повторения и самостоятельного контроля.....</i>	<i>24</i>
ГЛАВА 2 ОБЗОР СОЦИАЛЬНЫХ СЕТЕЙ И МЕССЕНДЖЕРОВ КАК ИСТОЧНИКОВ ДЕСТРУКТИВНОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ	
§ 2.1. Социальные сети в Интернете: понятие, анализ возможностей, виды деструктивного материала.....	25
§ 2.2. Мессенджеры: понятие, анализ возможностей, виды деструктивного материала.....	31
<i>Вопросы для повторения и самостоятельного контроля.....</i>	<i>37</i>
ГЛАВА 3 ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОИСКУ И ПРОТИВОДЕЙСТВИЮ РАСПРОСТРАНЕНИЮ ДЕСТРУКТИВНОГО КОНТЕНТА	
§ 3.1. Правовые методы противодействия.....	38
§ 3.2. Технические методы противодействия.....	41
<i>Вопросы для повторения и самостоятельного контроля.....</i>	<i>44</i>
ЗАКЛЮЧЕНИЕ.....	45
БИБЛИОГРАФИЧЕСКИЙ СПИСОК.....	46

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

ВЦИОМ – Всероссийский центр изучения общественного мнения

ИБ – информационная безопасность

ИТ – информационные технологии

ИТКС – информационно-телекоммуникационная сеть

МВД России – Министерство внутренних дел Российской Федерации

НПА – нормативный правовой акт

НСД – несанкционированный доступ

ОВД – органы внутренних дел

ОГВ – органы государственной власти

ОМС – органы местного самоуправления

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

постановление Правительства Российской Федерации № 1101 – постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе „Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено”»

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

СМИ – средства массовой информации

ФНС России – Федеральная налоговая служба

ФОИВ – федеральный орган исполнительной власти

149-ФЗ – Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

272-ФЗ – Федеральный закон от 28 декабря 2012 г. № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации»

436-ФЗ – Федеральный закон от 29 декабря 2010 г. № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию»

ВВЕДЕНИЕ

Социальные и экономические преимущества Интернета нельзя отрицать, однако некоторые из возможностей глобальной сети могут серьезно повлиять на такие императивы, как уважение прав и свобод человека, гуманность и демократия, духовные и культурные ценности общества. Ущерб, связанный с использованием Интернета в целях разрушения основ государственности и безопасности, нравственности и этики, здоровья и благополучия людей, а также влияние на социальные структуры и институты с каждым годом лишь возрастает.

Наличие в сети Интернет большого объема деструктивной информации, которая может побуждать к совершению противоправных действий, оправдывать противоправное поведение, содержать сведения экстремистского и террористического характера, разжигать межнациональную рознь и т. п., обосновывает актуальность исследований в данной области, результатом которых могут быть практические рекомендации по поиску и противодействию распространению информации деструктивного содержания или воздействия на пользователей в сети Интернет.

Обнаружение и предотвращение распространения информации – актуальные задачи в деятельности правоохранительных органов, представляющие несомненную сложность. Востребованы системный анализ информации деструктивного характера, выявление ее источников, конкретизация практических подходов к мониторингу сети Интернет, прикладным методам и способам выявления и противодействия распространению деструктивного контента.

Учебное пособие посвящено указанной проблематике, в частности, в нем рассматриваются такие ключевые вопросы, которым посвящены отдельные главы, как анализ деструктивного материала в сети Интернет, обзор социальных сетей и мессенджеров как источников деструктивного контента в сети Интернет, практические рекомендации по поиску и противодействию распространению деструктивного контента.

Цели пособия: повышение цифровой компетентности и медиаграмотности в области ИБ; формирование компетенций, необходимых для противодействия и профилактики деструктивного поведения в Интернете; развитие позитивной цифровой культуры в глобальной сети.

ГЛАВА 1

АНАЛИЗ ДЕСТРУКТИВНОГО МАТЕРИАЛА В СЕТИ ИНТЕРНЕТ

§ 1.1. Законодательные аспекты в области контроля проявления деструктивных материалов в сети Интернет

Проблематика измерения глубины и направлений распространения разнообразных информационных материалов в интернет-пространстве приобретает все большую популярность, о чем свидетельствует научный интерес представителей профессионального сообщества в области права, экономики, техники, психологии, педагогики, социологии, филологии, культуры и др.

С одной стороны, подобные векторы строго обеспечены отраслевыми нормативно-правовыми источниками, с другой – законодатель не может оперативно рефлексировать насчет динамично трансформирующейся и обогащающейся новыми видами и типами деструктивного материала обстановки информационной эволюции в виртуализированном поле. По указанным причинам в глобальной сети регулярно возникают и бесконтрольно распространяются огромные потоки деструктивного информационного материала. Действительность свидетельствует о том, что в процессе увеличивающегося значения для пользования, коммуникаций, жизнедеятельности мессенджеров, социальных сетей, сервисов и приложений, иных информационных ресурсов сети Интернет кардинально возросли угрозы их применения в криминальных и преступных целях.

Наиболее активными пользователями большинства ресурсов Интернета являются представители молодого поколения. Они первыми подхватывают тренды и начинают использовать их в своей повседневной жизни, что совершенно логично, ведь пользователи в возрасте 10–25 лет – это первое цифровое поколение, которое сформировалось как личности неотрывно от технологий (поколение Z, или зумеры¹). В своих предпочтениях, ценностях и ориентирах, а также в поведении онлайн они сильно отличаются от миллениалов² (поколения Y) и предыдущих поколений, проводя в сети значительно больше времени.

В большинстве случаев потребителем деструктивного материала в сети Интернет выступает детская, подростковая и молодежная аудитория. Масштабное распространение противоправного материала

¹ Зумеры – люди, родившиеся в период с 1997 по 2012 г.

² Миллениалы – люди, родившиеся в период с первой половины 1980-х до конца 1990-х гг.

опасно именно тем, что его зрителями может стать наиболее уязвимая группа пользователей – несовершеннолетние.

Под деструктивным материалом (контентом) обобщенно можно понимать информацию в современном виртуальном пространстве в любой «...форме (текстовой, аудиовизуальной, графической, электронной)», которая своим содержанием может причинять вред «...физическому, психическому, духовному, нравственному развитию»¹. Текстовые и визуальные материалы, размещаемые в глобальной сети, определяют и задают представления и ориентиры, аксиологические векторы и интересы, предопределяют действия общества, формируют социальную позицию. При этом подобное восприятие, понимание и оценка информации непосредственно связаны с поведением людей в обществе.

Строгой дефиниции рассматриваемого понятия в правовом поле на данный момент нет. В российском законодательстве выделяются определения разного рода запрещенных материалов, которые охватывают небольшую часть информационного пространства. Словосочетание «деструктивный контент» (англ. destructive – разрушительный) нечасто фигурирует в зарубежных источниках по отношению к правовой регламентации безопасности в глобальной сети. В документах Европейской комиссии употребляется форма «защита от абьюзивного поведения» (англ. protection against abusive behavior), законодательство США оперирует термином «неприемлемый контент» (англ. inappropriate content), Великобритании – «незаконный и вредоносный контент» (англ. illegal and harmful content). Так или иначе, правительства развитых государств внедряют соответствующую регуляторную базу в целях обеспечения ИБ, национальных экономических интересов, защиты прав своих граждан в глобальной сети. Принимаются нормы по введению механизмов и мер регулирования информации в Интернете, которые предполагают противодействие распространению в цифровой среде противоправных (запрещенных, ограниченных к распространению) материалов, считающихся таковыми согласно критериям национального законодательства.

В российских источниках права деструктивный контент/материалы зачастую описываются с помощью терминов «деструктивное поведение», «деструктивные действия», обозначающих умышленное разрушение общественных отношений, включая экстремизм, вред жизни и здоровью, духовно-нравственное унижение, жестокость, в том числе к представителям фауны, вандализм и др. В нормативных актах Роскомнадзора, основного регулятора в области государственного контроля и надзора СМИ и коммуникации, связи, ИТ и т. п., определение деструктивного контента отсутствует. Термин употребляется в большинстве случаев в контексте защиты несовершеннолетних в интернет-пространстве. В действи-

¹ Тазин И. И. Правовое обеспечение информационно-психологической безопасности несовершеннолетних // Вестник Томского государственного педагогического университета. 2012. № 6 (121). С. 222.

тельности, под деструктивными материалами подразумеваются разновидности данных, приводимые в 436-ФЗ. Вместе с тем иные государственные органы (Государственная Дума Федерального Собрания Российской Федерации) дискутируют о востребованности увеличения списка сведений, которые относятся к деструктивным.

Базовым НПА в изучаемой области также выступает 149-ФЗ. Часть 3 ст. 5 149-ФЗ дифференцирует сведения, которые в том числе могут находиться в сети Интернет, в зависимости от порядка их предоставления или распространения: на свободно распространяемую информацию; предоставляемую по соглашению лиц, участвующих в соответствующих отношениях; подлежащую предоставлению или распространению в соответствии с действующим законодательством государства; информацию, распространение которой в стране ограничивается или запрещается.

Как указано в ч. 6 ст. 10 149-ФЗ, запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

В силу ст. 15.3 149-ФЗ незамедлительное ограничение доступа на территории государства производит-ся в отношении интернет-ресурсов, распространяющих:

- информацию с призывами к массовым беспорядкам;
- информацию с призывами к осуществлению экстремистской деятельности;
- информацию с призывами к участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка;
- ложных сообщений об актах терроризма и иной недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, создающих угрозу национальной безопасности;
- информационные материалы иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации, и др.

В качестве примера классификации информации в зависимости от ее содержания можно привести упомянутый ранее 436-ФЗ, в ч. 1 ст. 5 которого установлены следующие виды информации, причиняющей вред здоровью и (или) развитию детей:

- информация, запрещенная для распространения среди детей;
- информация, распространение которой среди детей определенных возрастных категорий ограничено (отсылочные нормы к положениям ст.ст. 7–10 436-ФЗ, в которых регламентируются перечни информационной продукции, допускаемой к обороту в зависимости от возрастных цензов: для детей, не достигших

возраста 6 лет; детей, достигших возраста 6 лет; детей, достигших возраста 12 лет; детей, достигших возраста 16 лет).

В соответствии с ч. 2 ст. 5 436-ФЗ к информации, запрещенной для распространения среди детей, относится информация¹:

1. Побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству. К таковой можно отнести информационные материалы, способные побудить детей к действиям, угрожающим их жизни, здоровью, в том числе психическому (самоубийство, членовредительство, искусственное прерывание беременности, манипуляции с взрывчатыми, ядовитыми, сильнодействующими, радиоактивными веществами, оружием или боеприпасами, занятие азартными играми), либо провоцирующие несовершеннолетних на потребление веществ, товаров и услуг, опасных для жизни и здоровья. Под побуждением в данном контексте понимается психическое воздействие на лицо с целью заставить его трансформировать поведение в необходимом направлении. Обязательным (конструктивным) признаком побуждения выступает цель: заставить выполнить деяния, угрожающие жизни и (или) здоровью.

2. Способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заняться проституцией, бродяжничеством или попрошайничеством. Здесь подразумеваются сведения, способные побудить детей к употреблению перечисленных веществ и продукции, а также к занятию проституцией, бродяжничеством или попрошайничеством, к совершению актов вандализма, кощунства или надругательства над традиционными национальными и (или) религиозными ценностями, а также к совершению иных деяний, грубо нарушающих права и законные интересы других лиц. Сюда относятся различные формы убеждения, внушения, давления. Вызвать решимость совершить указанные выше действия могут следующие мотивы различного характера: престижного (стремление продемонстрировать отвагу и смелость, самостоятельность, ощутить опасность); подражательного (мнимые солидарность, товарищество, следование авторитету); альтруистического (демонстрация глубины эмоций).

3. Обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным. Информация подоб-

¹ Бирюкова Т. А., Егоров Ю. В., Захарова Н. А. [и др.]. Комментарий к Федеральному закону от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (постатейный) / под ред. Н. Н. Ковалевой // НПП «Гарант-сервис». 2013. URL: <https://base.garant.ru/57622377> (дата обращения: 18.04.2023). Режим доступа: заказ через систему «Гарант».

ного характера способствует существенным изменениям в духовно-нравственном поле, уничтожает основы нормативного и культурного воспитания, пропагандирует зло. В настоящее время наблюдается невысокий уровень морального воспитания в учебных заведениях и, как следствие, потеря идеалов и смыслообразующих целей. В эмоционально-психологическом настрое молодежи распространена ориентация на допустимость насилия в кризисной ситуации. Эмоциональное напряжение приводит детей к желанию его ослабить, вследствие чего провоцирует их на уход из реальной среды и поиск суррогатных выходов.

4. Отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи. Таковыми являются материалы, умаляющие значимость социальных институтов семьи, брака, материнства и отцовства, способствующие формированию искаженных ориентаций и установок в брачно-семейной сфере. Подобная информация зачастую воспринимается неосознанно и регулярно.

4.1. Пропагандирующая либо демонстрирующая нетрадиционные сексуальные отношения и (или) предпочтения. Такие материалы преследуют цель сформировать нетрадиционные сексуальные установки, придать привлекательность нетрадиционным сексуальным отношениям, сформировать у детей искаженное представление о социальной равноценности традиционных и нетрадиционных сексуальных отношений, навязать ценности нетрадиционных сексуальных отношений, вызвать к ним стойкий интерес. Сексуальная ориентация – личный выбор каждого взрослого человека, но у ребенка перед глазами в первую очередь должен быть вариант нормы. Публичное одобрение и формирование привлекательности нетрадиционных сексуальных отношений опасно не только для детей и молодежи, но и для общества в целом, поскольку несет угрозу демографическому росту и экономическому развитию страны.

4.2. Пропагандирующая педофилию. Материалы направлены на обоснование или оправдание сексуального интереса взрослых, вызванного психическим расстройством, к детям и подросткам; формирование его привлекательности; распространение девиантного интереса, представляющего собой ключевой фактор риска сексуального рецидива. В общемировом информационном пространстве экстремистские или запрещенные социальные сети и зарубежные СМИ распространяют подобный контент, который детьми может быть воспринят в качестве варианта нормы. В подобном случае, если ребенок станет жертвой педофила, он может не понять, что в отношении его совершено преступление. У детей-жертв страдает психика, при этом они часто оправдывают насильника, не обращаются в правоохранительные органы и не сообщают о насилии родителям.

4.3. Способная вызвать у детей желание сменить пол. Преследуется цель навязать существование проблем половой идентичности, связанных с эмоциональными и поведенческими трудностями, а так-

же с высоким уровнем сопутствующих психических заболеваний детей и подростков. В результате воздействия данного вида информации жертвы выражают желание принадлежать к противоположному полу или настаивают на том, что они действительно принадлежат к нему. Они исследуют гендерную идентичность и стремятся экспериментировать с гендерным выражением, демонстрируют характерное поведение противоположного пола.

5. **Оправдывающая противоправное поведение.** Признаки противоправного поведения определяются законом или другими нормативными актами в любой отрасли права (гражданского, трудового, административного, семейного и т. д.). Противоправные действия могут выражаться в произволе, беззаконии, быть по своему характеру исключительно грубыми и циничными. Они могут непосредственно угрожать жизненно важным интересам как самого несовершеннолетнего, так и его близких, иных лиц. Противоправное поведение может быть аморальным, если оно нарушает общечеловеческие нормы поведения и коммуникации в обществе. Противоправное поведение обуславливает возникновение преступного умысла.

6. **Содержащая нецензурную брань.** Материалы, содержащие бранные, вульгарные, нецензурные или иные ненормативные слова, речевые обороты и выражения, а равно слова, речевые обороты и выражения, сходные до степени смешения с нецензурными. К нецензурной брани следует относить табуированную (ненормативную) лексику и матерную брань. Главным признаком оскорбительности высказывания выступает прежде всего неприличная форма выражения отрицательной оценки человека, которая может стать причиной подрыва его престижа в глазах окружающих, также способная нанести ущерб уважению к самому себе.

7. **Содержащая информацию порнографического характера.** Порнография – вульгарно-натуралистическая, омерзительно-циничная, непристойная фиксация половых сношений, самоцельная, умышленная демонстрация большей частью обнаженных гениталий, антиэстетичных сцен полового акта, сексуальных извращений, зарисовок с натуры, которые не соответствуют нравственным критериям, оскорбляют честь и достоинство личности, ставя ее на уровень проявлений животных инстинктов. Под информацией порнографического характера понимается не имеющее научного, медицинского или учебного предназначения описание или фото-, видеоизображение или иное изображение (в том числе созданное средствами компьютерной графики, анимационными или иными изобразительными средствами) реально совершаемого человеком или имитируемого им полового сношения или иных действий сексуального характера, в том числе совершаемых в отношении животного, а также натуралистическое описание или изображение половых органов человека в сексуаль-

ных целях или иных интимных сторон жизни человека, связанных с удовлетворением сексуальных потребностей.

8. О несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения несовершеннолетнего, аудиозапись его голоса, место жительства или место временного пребывания, место учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

9. Содержащаяся в информационной продукции, произведенной иностранным агентом. Критерием опасности выступает автор – любое российское или иностранное юридическое лицо независимо от его организационно-правовой формы, иное объединение лиц или физическое лицо независимо от его гражданства, если они получают иностранную поддержку или находятся под зарубежным влиянием. Иностранные агенты не могут получать государственное финансирование при осуществлении творческой деятельности, а результаты их деятельности, воплощенные в информационных активах, требуют маркировки печатной продукции, на сайтах и в социальных сетях.

В Российской Федерации долгое время отсутствовали нормы, защищающие права несовершеннолетних потерпевших, устанавливающие запрет на разглашение в СМИ такого рода информации. Сегодня незаконное распространение информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), или нарушение предусмотренных федеральными законами требований к распространению такой информации, если эти действия (бездействие) не содержат уголовно наказуемого деяния, влекут наложение административного штрафа с конфискацией предмета административного правонарушения.

Согласно ч. 3 ст. 5 436-ФЗ к информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:

- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия;
- вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
- представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С 1 февраля 2021 г. в силу вступили изменения в положениях 149-ФЗ¹, которые призваны решить задачу устранения из общедоступного информационного пространства материалов, распространение которых запрещено законодательством, на ранних этапах без увеличения числа контролирующих органов и полной блокировки информационных ресурсов.

Новые нормы², регулирующие аспекты распространения информации в социальных сетях, регламентируют следующие направления:

- признаки социальных сетей;
- обязанности их владельцев и права пользователей;
- порядок блокировки нелегальных информационных материалов;
- регламент включения социальной сети в соответствующий реестр.

В блоке обязанностей владельцев социальных сетей отмечается требование осуществления мониторинга своего ресурса для выявления запрещенного контента, к которому относятся материалы:

- содержащие публичные призывы к осуществлению террористической деятельности или публично оправдывающие терроризм;
- пропагандирующие порнографию, культ насилия и жестокости;
- содержащие нецензурную брань;
- распространение которых может опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями;
- о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;
- о способах совершения самоубийства, а также призывов к суициду;
- нарушающие требования законодательства о запрете деятельности по организации и проведению азартных игр и лотерей с использованием Интернета и иных средств связи;

¹ Ключевская Н. Стоп, контент: новые обязанности владельцев соцсетей и права пользователей // НПП «Гарант-сервис». URL: <https://www.garant.ru/article/1444081> (дата обращения: 17.06.2022).

² Федеральный закон от 30 декабря 2020 г. № 530-ФЗ «О внесении изменений в Федеральный закон „Об информации, информационных технологиях и о защите информации“» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_372700 (дата обращения: 18.04.2023).

- содержащие предложения о розничной продаже дистанционным способом алкогольной продукции, спиртосодержащей пищевой и непищевой продукции, этилового спирта, розничная продажа которых ограничена или запрещена законодательством;
- выражающие в неприличной форме, оскорбляющей человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или ОГВ;
- содержащие призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в несанкционированных массовых мероприятиях;
- содержащие недостоверную общественно значимую информацию, распространяемую под видом достоверных сообщений, создающую угрозу причинения вреда жизни или здоровью граждан, имуществу, угрозу массового нарушения общественного порядка или общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, информационных материалов иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории России, сведения, позволяющие получить доступ к указанной информации или материалам;
- направленные на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и здоровья либо для жизни или здоровья иных лиц;
- с порнографическими изображениями несовершеннолетних или объявлениями о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера.

В феврале 2022 г. депутатами Государственной Думы Федерального Собрания Российской Федерации было предложено расширить перечень противоправных информационных материалов в сети Интернет¹. Актуальность изменений подтверждается тем, что сегодня в глобальной сети появляется множество материалов, прямо не подпадающих под категорию запрещенных, но представляющих собой реальную угрозу безопасности пользователей, а также национальной безопасности. Тематика материалов касается абортов, радикального феминизма, концепции чайлдфри², пропаганды нездоровых половых отношений, тренингов по нормализации девиантных форм поведения и психических отклонений и др.

¹ Мустафа С. В Совфеде предложили внести чайлдфри и радфем в перечень противоправного контента // Газета.ру. URL: <https://www.gazeta.ru/tech/news/2022/02/17/17302537.shtml> (дата обращения: 20.06.2022).

² Чайлдфри (англ. childfree – свободный от детей) – движение, которое придерживается концепции жизни без детей.

Зимой 2023 г. законопроект был повторно внесен в Государственную Думу Федерального Собрания Российской Федерации. По состоянию на данный момент законопроект рассмотрен в первом чтении.

Завершить обзор нормативных источников в изучаемой области целесообразно положениями Стратегии национальной безопасности, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400. Она относит к национальным интересам Российской Федерации сбережение народа России, развитие безопасного информационного пространства, защиту российского общества от деструктивного информационно-психологического воздействия, укрепление традиционных российских духовно-нравственных ценностей.

§ 1.2. Виды, формы и классификация деструктивных материалов в сети Интернет

Подходы к типологизации деструктивных материалов в сети Интернет опираются прежде всего на научно-исследовательский базис ввиду текущей востребованности нахождения эффективных мероприятий для решения задач обеспечения безопасности в сети Интернет и отсутствия строгого нормативного закрепления термина. Также в рамках определения видов и форм данной категории цифровой информации актуальны предложения, выдвигаемые государственными и общественными организациями и сообществами, профилизирующимися на обеспечении интернет-безопасности (например, «Лига безопасного интернета», «Альянс по защите детей в цифровой среде», «Лаборатория Касперского» и др.).

Пользователи могут обнаружить незаконные цифровые материалы в Интернете в различных местах, включая веб-сайты, платформы социальных сетей или службы обмена файлами. В основном подобные деструктивные материалы детектируются непреднамеренно, например когда пользователь нажимает на ссылки в спам-сообщениях. Такие сведения также могут распространяться по электронной почте или через службы обмена сообщениями.

Пользователи могут получить доступ к деструктивному материалу посредством иных действий или событий, таких как:

- неожиданные результаты от поисковых систем;
- переход по неизвестным ссылкам;
- неправильный ввод веб-адреса;
- «щелчок» («клик», «нажатие») по всплывающей рекламе, в приложениях или онлайн-играх.

Иногда пользователи намеренно получают доступ к нелегальным цифровым материалам, особенно в подростковом возрасте, что может происходить ввиду любопытства. Деструктивные материалы могут от-

крыть концепции, с которыми общество не готово справиться и которые могут нарушить социальные и культурные убеждения. Некоторая информация может вызывать беспокойство: дети, увидевшие такой контент, могут не сообщить о нем учителям или родителям, потому что им может быть стыдно за то, что они увидели.

В последние годы Интернет получает все более негативное освещение в СМИ. Многочисленные статьи сообщают о крупных скандалах с конфиденциальностью и нарушением безопасности, распространении фейковых (англ. fake – подделка, фальшивка) новостей, возрастающей интернет-зависимости, о таких преступных проявлениях, как киберзапугивание, киберворовство, порноместь, а также о негативных последствиях, которые Интернет может оказать на социальные отношения. Выделяют следующие негативные психофизиологические последствия использования Интернета:

1. Интернет-зависимость и проблемное использование. Отсутствие контроля над количеством и существом потребления материалов в глобальной сети может привести к снижению физического и психологического благополучия людей с сопутствующими симптомами (депрессия, гнев, потеря контроля, социальная изоляция, семейные конфликты и другие факторы, подталкивающие людей к изоляции). Лица с сопутствующими психическими симптомами подвержены большему риску интернет-зависимости, в то время как культурные проблемы или использование цифровых ресурсов для медиациелей могут способствовать развитию глобальности интернет-зависимости.

2. Отрицательное влияние на когнитивное развитие. Имеются данные, свидетельствующие о том, что когнитивное развитие детей может быть нарушено ввиду их длительного пребывания в Интернете. Страдают развитие навыков памяти, концентрации внимания, способности к критическому мышлению, овладению языком, чтению и обучению.

3. Информационная перегрузка. Наличие слишком большого количества информации может затруднить адекватное понимание проблемы или нахождение эффективного решения. Информационная перегрузка связана с потерей контроля, чувством подавленности, снижением интеллектуальной работоспособности и удовлетворенности работой. Перегрузка большим объемом информации, возникающая в результате общения, может быть последствием постоянного притока сообщений, электронных писем или иной информации.

4. Нарушение общественных/частных границ. Интернет и мобильные устройства стирают границы между работой и домом, общественной и частной жизнью людей. Отрицательные эффекты, которые могут возникнуть в результате такого перемерения, включают более низкое качество жизни, отсутствие конфиденциальности, снижение безопасности (личной и общественной) и негативное воздействие на социальные отношения.

5. Разрушение социальных связей и отношений. Частое использование Интернета коррелирует с одиночеством и социальной изоляцией. Под угрозой могут быть интимные отношения, особенно ввиду просмотра онлайн-порнографии. Злонамеренное поведение в сети (киберзапугивание, киберпреследование) затрагивает значительную долю пользователей Интернета. Многие офлайн-сообщества страдают от частичной миграции человеческой деятельности, например товаропотребления (шопинга), коммерции, досуга или профессионального общения.

Владельцы (администраторы) интернет-площадок (провайдеры) играют важную роль в обеспечении бесперебойной работы сервисов в сети Интернет. Они должны функционировать без опасений быть привлеченными к ответственности за незаконность материалов, который проходит через их системы. Как правило, провайдеры не осуществляют глобальный редакционный контроль (модерацию) над всеми онлайн-материалами, проходящими через их сервисы.

Сегодня интернет-провайдеры несут юридические риски за первичные и вторичные обязательства функциональности их сервисов, таких как хостинг, кеширование, маршрутизация и т. д. В перечень незаконных/запрещенных и потенциально опасных материалов, которые могут быть размещены провайдерами через своих абонентов, могут быть включены:

- порнография, к примеру детская, изображения сексуального характера, в том числе сцены сексуального насилия над детьми, зоофилия и т. п.;
- инструкции о том, как совершить преступление, насильственные действия, изготовить оружие и взрывные устройства, произвести и употребить наркотики, пропаганда нетрадиционных отношений, небезопасного поведения, экстремизма (терроризма);
- кадры реального или смоделированного насилия, несчастных случаев или преступной деятельности из фильмов, видеоклипов или игр;
- онлайн-груминг¹, сексуальная эксплуатация;
- буллинг²;
- разжигание ненависти, пропаганда крайних политических взглядов, потенциально используемая для радикализации;
- расизм, материалы, пропагандирующие ненависть к группам или отдельным лицам на основе религии, расы или сексуальных предпочтений;

¹ Онлайн-груминг – формирование доверительных отношений с несовершеннолетними в целях сексуальной эксплуатации / сексуального насилия, онлайн-обмена контентом сексуального (эротического, порнографического) содержания.

² Буллинг – преследование (запугивание) человека другим человеком или группой людей, имеющее агрессивный характер.

- угрожающие и оскорбительные материалы, клевета;
- нарушение авторских прав;
- получение НДС к стриминговым сервисам (потокковому вещанию)¹;
- кража IP-адресов, совершение компьютерных (кибер-) преступлений и злоупотребление доверием.

Таким образом, список незаконных и опасных материалов весьма разнообразен. Интернет-провайдеры не имеют соответствующих правовых компетенций для определения незаконности онлайн-контента, а порой не всегда заинтересованы в этом в связи с необходимостью дополнительного вложения денежных средств в модерацию.

Рассмотрим некоторые из перечисленных угроз в проекции их воздействия на подростковую аудиторию.

В Интернете буллинг принимает различные формы. Он включает в себя отправку ненавистнических сообщений или угроз смерти детям, распространение лжи о них в Интернете, оскорбительные комментарии в их профилях в социальных сетях или создание веб-сайта для оскорбления их внешности или репутации.

Кибербуллинг отличается от травли в реальном мире. Киберхулиганы не наблюдают за реакцией своих жертв, как если бы они оскорбляли других в лицо. Некоторые нарушители изображают из себя своих жертв и рассылают другим сообщения оскорбительного характера. В последнее время они также начали публиковать унижительные видео других детей. Часто подростки не говорят родителям, что они подвергаются буллингу: они боятся, что их семья отреагирует остро или лишит их возможности использовать интернет-ресурсы.

Киберпространство подталкивает молодых людей к доверию в ходе общения с виртуальными незнакомцами. Ребенок не защищен от сексуальных домогательств в Интернете: сексуальные маньяки преследуют детей в чатах, социальных сетях, на иных площадках. Профиль пользователя обычно включает фотографии, сведения о личных интересах и блоги, что для преступника является удобным ресурсом, с помощью которого они могут добраться до жертв. Злоумышленники могут выдавать себя за другую личность, симулировать интерес к любимым музыкальным группам, телешоу, видеоиграм или хобби жертвы. Они кажутся детям новыми лучшими друзьями с совпадающими симпатиями и антипатиями.

Для родителей одной из самых страшных опасностей Интернета является возможность просмотра порнографических материалов их детьми. Программные фильтры не являются идеальным решением для блокировки: некоторые сайты с подобным содержанием могут остаться неотфильтрованными, а ресурсы образовательного или развлекательного характера (не содержащие негативных материалов), наоборот, могут быть заблокированы.

¹ Стрим (англ. stream, букв. поток) – потоковая передача информации, онлайн-вещание через разнообразные интернет-платформы (YouTube, Twitch).

Сегодня повсеместно распространены мобильные устройства с камерами, цифровые камеры и веб-камеры, и дети могут стать жертвами собственной неопытности в новых технологиях. Многие размещают в сети фотографии, видео или заметки в форме блогов (влогов¹), о которых потом сожалеют. Репутация пользователя в Интернете вызывает все большую обеспокоенность в связи с ростом количества социальных сетей и профилей. Цифровой след сказывается на действиях организаций, отказывающих людям в стажировках, поступлении в учебные заведения или трудоустройстве после проверки того, что соискатели размещали в Интернете.

Повышение доступности и возможность быстро общаться с тысячами пользователей сделали сеть Интернет предпочтительным инструментом для отдельных лиц или организаций, стремящихся распространять социальные сообщения повсюду, осуществляющих тем самым цифровой активизм. Независимые активисты во всем мире используют Интернет и цифровые инструменты для создания своего сообщества, общения с другими единомышленниками за пределами их физического окружения, а также для лоббирования, сбора средств и организации мероприятий, которые могут быть запрещенными.

Помимо распространения сообщений цифровые активисты могут использовать возможности глобальной сети для выражения своих интересов и призывов к переменам. Для обычных граждан возможность делиться своими историями, жизненными ситуациями и проблемами помогает лучше понять, что происходит. Сами же сообщения оказывают давление на ОГВ, которые могут принять меры по вопросам, обычно не освещаемым традиционными СМИ.

Инструменты, используемые цифровыми активистами, обширны и постоянно меняются по мере развития ИТ; наиболее популярными являются: видеоплощадки, блоги, социальные сети, мессенджеры, мобильные устройства.

Веб-сайты с высокой посещаемостью являются центрами онлайн-активизма, где люди могут общаться с другими людьми по всему миру на интересующие их темы. Facebook² и YouTube доказали свою эффективность в распространении информации, получении поддержки, представлении визуально привлекательной информации, которая в противном случае могла бы остаться незамеченной традиционными СМИ. В мобилизации людей на протесты и объединения ведущую роль также играют другие социальные сети и мессенджеры.

¹ Влог – разновидность видеодневника, ведущегося на видео- и стриминговых сервисах в сети Интернет.

² Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

Блоги, по сути являющиеся формой гражданской журналистики для масс, обеспечивают эффективное средство нефилтрованного общения с аудиторией на любую тему и могут использоваться в многочисленных онлайн-кампаниях. Сайты микроблогов используются для распространения информации о проблеме или мероприятиях активистов. Функция хештега¹, позволяющая людям вносить свои сообщения в многопользовательский разговор, вводя ключевое слово или фразу, которым предшествует хештег, часто используется в качестве цифрового инструмента для распространения сообщений.

Наличие встроенной камеры на большинстве мобильных телефонов привело к кардинальным изменениям в том, как общество реагирует на глобальные события и транслирует доказательства в защиту социальной справедливости (например, документирование нарушения закона со стороны различных ОГВ, массовых беспорядков и т. д.).

В качестве средства обхода государственного вмешательства, когда дело доходит до онлайн-протестов, многие люди используют прокси-серверы, которые действуют как посредники между пользователем и сайтом. Используя Интернет для решения проблем и приобретения ресурсов, краудсорсинговые² платформы помогают отдельным лицам и инициативам мобилизовать глобальное сообщество и создавать возможности для сотрудничества между группами (иначе) не связанных между собой людей. Хотя цифровой активизм может многое предложить сообразительному участнику кампании, он имеет ограничения в отношении того, сколько эффективных изменений возможно произвести и является ли концепция всех деяний законной.

Как отмечалось ранее, с февраля 2021 г. расширилось число обязанностей для владельцев интернет-ресурсов в направлении борьбы с деструктивными информационными материалами. Так, введена обязанность размещения документа, устанавливающего правила использования ресурса с указанием в них не противоречащих законодательству Российской Федерации требований к распространению информации. Согласно правилам, объявления (сообщения) пользователей не должны отображать, облегчать или продвигать неприемлемый контент. Владельцы ресурсов должны стремиться к тому, чтобы информация, которая транслируется и распространяется через их платформы, была уместной, уважительной по отношению к другим, неоскорбительной и безопасной для пользователей. Объявления, содержащие шокирующий, жестокий или дискриминационный контент, недопустимы.

Примеры запрещенного контента и практики в отношении неприемлемых материалов:

¹ Хештег – ключевое слово (одно или несколько), пометка, обеспечивающая более быстрый поиск информации. Перед словом ставится символ – #.

² Краудсорсинг (англ. crowd – толпа, sourcing – использование ресурсов) – передача определенных производственных функций кругу лиц без заключения трудового договора по типу субподрядной работы, чтобы задействовать их знания, опыт и творческие способности.

– шокирующий контент (чрезмерно жестокий или сенсационный, способный напугать пользователя). Сюда входят объявления и темы, связанные с кровавым содержанием (автомобильная авария), насилием (например, реклама с пистолетом, направленным на человека); угрозы насилия; оскорбительная и ненормативная лексика; информация, предполагающая, что человеку может быть причинен вред или опасность, он может быть заражен болезнью или стать жертвой заговора;

– острые события (контент, связанный с деликатными событиями, которые могли произойти): отсутствие раскаяния или сочувствия к шокирующему или трагическому событию; попытка извлечь выгоду из события;

– дискриминирующая информация (любое обращение с человеком, группой лиц или обществом как с незначительным или второстепенным, пропаганда маргинализации), признаки дискриминации: расовое или этническое происхождение, возраст, национальность, религия, инвалидность, статус ветерана, политический статус, пол, гендерная идентичность, сексуальная ориентация;

– недопустимое обращение с животными (шокирующие материалы о жестоком обращении с животными, пропаганда такого обращения): жестокое обращение с животными в развлекательных целях (бои); продажа или продвижение продукции, полученной путем истребления исчезающих видов животных; блоги или форумы, предлагающие информацию о том, как получить продукты от исчезающих видов.

Многие провайдеры (владельцы интернет-ресурсов) полностью полагаются на своих сотрудников, выполняющих функции модераторов, при проверке стороннего или созданного пользователями контента, в то время как другие просто реагируют на жалобы пользователей и удаляют оскорбительные или неприемлемые изображения, рекламу или видео без проведения предварительной модерации. Однако модерация сама по себе не может масштабироваться для удовлетворения указанных потребностей и законодательных требований с достаточным качеством или скоростью, что приводит к плохому взаимодействию с пользователем, высоким затратам на достижение масштаба или даже к потере репутации бренда. В этом аспекте востребовано техническое решение проблемы в автоматизированном режиме – использование API-модерации (API, англ. аббр. application programming interface – программный интерфейс приложения) размещаемых пользователями материалов. Современные технологии используют многоуровневую иерархическую таксономию¹ для маркировки категорий неприемлемых или оскорбительных материалов. Каждая категория верхнего уровня имеет ряд категорий базового уровня, например:

– порнография: сексуальные ситуации, нагота, графическое изображение мужской/женской наготы, сексуальная активность, иллюстрированная откровенная нагота, секс-игрушки;

¹ Таксономия – наука о классификации сложных иерархических систем.

- насилие: графическое насилие или кровь, физическое насилие, оружие, травма;
- экстремизм: нацистская партия, белое превосходство.

В марте 2022 г. Правительство Великобритании представило в парламенте проект закона «О безопасности в Интернете» (англ. Online Safety Bill)¹, призванного повысить ответственность технологических компаний за удаление со своих платформ противозаконного контента, связанного с пропагандой терроризма или насилия, порнографией, агрессивным поведением в сети и сексуальным насилием над детьми. Документ вводит три типа контента: нелегальный (незаконный); опасный для детей; опасный для взрослых. В пределах указанных типов применяются дополнительные подкатегории:

1. Незаконный контент. Сюда относится информация, владение, просмотр, доступ, публикация или распространение которой составляют: преступление, связанное с терроризмом или сексуальной эксплуатацией и насилием над детьми; правонарушение, связанное с пособничеством самоубийству, угрозами убийства, страхом или провокацией насилия, преследованием, разжиганием ненависти по признаку расы, религии или сексуальной ориентации, преследованием, запугиванием людей насилием, нарушением общественного порядка по расовому или религиозному признаку, с наркотиками, с огнестрельным оружием, содействие незаконной иммиграции, с сексуальной эксплуатацией, с мошенничеством и финансовыми услугами; любое другое правонарушение, жертвой которого является физическое лицо или физические лица («приоритетный контент»), за исключением правонарушений, связанных с нарушением прав интеллектуальной собственности, нарушением законов о защите прав потребителей, безопасности или качества товаров или оказанием услуги лицом, не обладающим соответствующей квалификацией.

2. Контент, опасный для детей. Включает материалы, относящиеся к «приоритетному контенту»: несущие риск причинения значительного ментального, физического и иного вреда большому числу детей, за исключением случаев, когда правонарушения вытекают из потенциального финансового воздействия.

3. Контент, опасный для взрослых. Включает информацию: относящуюся к «приоритетному контенту» (жестокое обращение, не являющееся правонарушением, а также сведения о расстройствах пищевого поведения, членовредительстве и самоубийстве); представляющую материальный риск причинения значительного вреда большому числу людей, за исключением случаев, когда воздействие вытекает из потенциального финансового воздействия информации, безопасности или качества товаров, представленных в ней, или способа, которым услуга, представленная в материалах, может быть выполнена.

¹ В Великобритании обсудят в парламенте проект закона «О безопасности в интернете» // Daily Digital Digest. URL: <https://3d-news.ru/1062173/v-velikobritanii-obsudyat-v-parlamente-proekt-zakona-o-bezopasnosti-v-internete> (дата обращения: 19.04.2023).

На официальном сайте Общественного уполномоченного по защите семьи¹ размещена информация о результатах заседания общественного совета при Роскомнадзоре по вопросам борьбы с деструктивным контентом. Отмечается, что экспертами проведена работа по выявлению и классификации видов деструктивного контента. Выделено шесть условных категорий информации:

- 1) наносящая непосредственный вред жизни и здоровью ребенка (суицидальный контент, селфхарм², группы анорексии);
- 2) наносящая вред психическому здоровью ребенка, провоцирующая нервные расстройства (группы и каналы, содержащие шок-контент, депрессивный контент; эзотерика, оккультизм; группы, пропагандирующие эксперименты над психикой);
- 3) склоняющая к преступным действиям и насилию (крипипасты³, колумбайн⁴, сообщества маньяков и серийных убийц, АУЕ⁵, оффники⁶, сатанисты);
- 4) наносящая урон морально-этическому состоянию, разрушающая семейные ценности, настраивающая ребенка против родителей (сообщества «яжемать», феминистки, чайлдфри, аморальный юмор);
- 5) развращающая, склоняющая ребенка к смене ориентации или пола, пропагандирующая иные виды извращений (ЛГБТ, смена пола, аниме, фурри⁷, соцсеть Amino, группы гей-знакомств, «Фикбук»⁸ и фанфики⁹ в целом);
- 6) манипулятивная, ставящая цель получения материальной выгоды (ставки на спорт, букмекерские конторы, онлайн-казино, вейпы, снюсы, электронные сигареты, онлайн-игры).

Базовым инструментарием продвижения и втягивания в опасную информационную среду и субкультуры выступают мессенджеры, социальные сети и компьютерные игры. Действующие интернет-протоколы

¹ URL: <https://ouzs.ru> (дата обращения: 19.04.2023).

² Селфхарм (англ. self-harm) – умышленное причинение самому себе телесных повреждений острыми предметами в виде порезов, царапин и т. п.

³ Крипипаста – интернет-фольклор, представляющий собой страшные рассказы (истории и т. п.), цель которых – напугать читателя.

⁴ Колумбайн (иное название – «скулшутинг» (англ. school shooting – школьная стрельба) – массовые расстрелы в школах. Организация признана экстремистской на территории Российской Федерации.

⁵ Организация признана экстремистской на территории Российской Федерации.

⁶ Оффники – представители субкультуры (футбольные, околофутбольные фанаты), которые при любой возможности ищут повод для драки.

⁷ Фурри – поп-культурное движение, поклонники антропоморфных (человекообразных) животных в сериалах.

⁸ «Фикбук» (иное название – «Книга фанфиков») – сайт, на котором бесплатно размещаются произведения разных литературных жанров, написанные пользователями.

⁹ Фанфик – любительское литературно-художественное произведение, основанное на популярных оригинальных сюжетах и произведениях.

не дают Роскомнадзору возможности блокировки отдельных страниц социальных сетей, поэтому российский законодатель идет по пути воздействия на распространителей деструктивных материалов и коммуникации с площадками. Предлагается ряд изменений в законодательство об информационных правоотношениях, а также в административное и уголовное законодательство.

Повсеместное использование Интернета сигнализирует о необходимости оценки потенциала негативных последствий, которые он оказывает на личность и общество. Возникает обеспокоенность конфиденциальностью и безопасностью, нарушениями законодательства, негативным влиянием на общение и цивилизованность, коммерциализацией публичной сферы, а также в связи с другими последствиями деструктивного характера.

В конечном счете негативные последствия использования Интернета складываются в интегративный общественный вред, который может стать предметом государственного регулирования. Положения, законы и другие правовые меры, регулирующие развитие и использование сети Интернет, представляют собой дополнительный фактор, определяющий влияние, которое Интернет может оказать на культуру и общество.

Вопросы для повторения и самостоятельного контроля

1. Что представляет собой деструктивный материал?
2. Какая информация запрещается к распространению на основании 149-ФЗ?
3. К какой информации незамедлительно должен быть ограничен доступ на основании 149-ФЗ?
4. Виды информации, причиняющей вред здоровью и (или) развитию детей согласно 436-ФЗ.
5. К какой информации согласно 436-ФЗ должен быть ограничен доступ среди детей определенных возрастных категорий?
6. В обязанности владельцев социальных сетей входит мониторинг данных сетей на наличие в них запрещенных материалов. Какие это материалы?
7. Какие действия пользователя могут стать причиной доступа к информации деструктивного содержания?
8. Какая информация относится к незаконной (запрещенной, опасной) и может быть получена абонентами через интернет-провайдеров?

ГЛАВА 2

ОБЗОР СОЦИАЛЬНЫХ СЕТЕЙ И МЕССЕНДЖЕРОВ КАК ИСТОЧНИКОВ ДЕСТРУКТИВНОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ

§ 2.1. Социальные сети в Интернете: понятие, анализ возможностей, виды деструктивного материала

Термин «социальная сеть» в обычном значении – это сообщество людей, связанных общими интересами, общим делом или имеющих другие причины для непосредственного общения между собой. Социальная сеть – это социальная структура, состоящая из узлов (примерами узлов выступают отдельные люди, группы людей или сообщества), связанных между собой одним или несколькими способами посредством социальных взаимоотношений.

Социальная сеть – это сайт, построенный на основе персональных анкет пользователей, которые могут быть связаны между собой. Кроме хранения ПДн и связей социальная сеть позволяет пользователям обмениваться сообщениями и мультимедийным контентом (фотографиями, музыкой, видео, текстовыми документами)¹.

С технической точки зрения и со стороны пользователя социальной сетью в Интернете считается ПО в сети Интернет, позволяющее пользователям создавать свои профили и связываться с другими участниками в виртуальном пространстве. Подобные интернет-ресурсы позволяют пользователю присоединять людей к своей сети, выходить на других людей через своих знакомых, посылать сообщения, размещать фотографии, тексты и любой другой контент.

Одной из угроз, присутствующих в социальных сетях, как было указано выше, является наличие деструктивной информации (деструктивного контента).

Социальные сети имеют массовое распространение среди пользователей сети Интернет. По данным на 2021 г., общее число активных пользователей сети Интернет в мире насчитывает порядка 4,7 млрд человек, в России этот показатель составляет 98–99 млн².

¹ Леонтьев В. П. Социальные сети: ВКонтакте, Facebook и другие... М. : ОЛМА Медиа Групп, 2012. С. 5.

² Digital 2021: Global Overview Report // DataReportal. URL: <https://datareportal.com/reports/digital-2021-global-overview-report> (дата обращения: 19.04.2023).

В Российской Федерации сетью Интернет пользуются более 86 % городского населения в возрасте от 15 до 74 лет¹. Растет доля пользователей, имеющих доступ к сети Интернет: в 2015 г. – 72,1 %, в 2019 г. – 76,9 %².

Более половины времени интернет-потребления приходится на три направления: социальные сети (21 %), видеоконтент (18 %) и мессенджеры (15 %)³.

Возможности, реализуемые социальными сетями, достаточно обширны и разнообразны:

- создание профиля пользователя с размещением в нем персональной информации (Ф. И. О., пол, возраст, учебное заведение (школа, вуз и т. п.), место работы (службы), фотографии, интересы, увлечения и т. п.);
- создание сообществ (групп) по интересам (увлечениям, тематикам);
- обмен мультимедийным контентом различного формата и содержания (фотографии, видеофайлы и т. п.);
- прослушивание музыки;
- ведение бизнес-аккаунтов компаний (организаций) или официальных страниц ОГВ и др.

Согласно статистическим исследованиям, самыми популярными ресурсами онлайн-аудитории на всех платформах в России являются видеосервис YouTube, социальная сеть «ВКонтакте», мессенджеры WhatsApp и Telegram (подробно речь о мессенджерах пойдет в следующем параграфе этой главы), социальная сеть TikTok⁴.

Исследования We Are Social и Hootsuite, Statista и Napoleon Cat показывают, что наиболее популярными в мире являются социальные сети Facebook⁵ с аудиторией порядка 2,7–2,9 млрд пользователей, Instagram⁶ (1,2–1,4 млрд), TikTok (0,7–1,0 млрд) и видеохостинг YouTube (2,2–2,5 млрд). Сравнительные показатели популярности социальных сетей в России и мире представлены в табл. 1.

¹ Статистические таблицы, 2020 г. // Росстат. URL: https://www.gks.ru/free_doc/new_site/business/it/ikt20/Статистические%20таблицы%202020%20г..html (дата обращения: 19.04.2023).

² Информационное общество в Российской Федерации, 2020 г. : статистический сборник // Росстат ; Национальный исследовательский университет «Высшая школа экономики». М. : НИУ ВШЭ, 2020. URL: <https://rosstat.gov.ru/storage/mediabank/lqv3ToRk/info-ob2020.pdf> (дата обращения: 20.04.2023).

³ Интернет // Mediascope. URL: <https://mediascope.net/services/media/media-audience/internet/description> (дата обращения: 19.04.2023). Режим доступа: через запрос о составлении отчета.

⁴ Там же.

⁵ Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

⁶ Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

Таблица 1

Сравнение популярности социальных сетей (в млн пользователей)

Источник данных	Социальная сеть					
	Facebook ¹	YouTube	Instagram ²	TikTok	«Одноклассники»	«ВКонтакте»
Statista ³ (активных пользователей в месяц в мире)	2 958	2 514	2 000	1 051	–	–
We Are Social и Hootsuite ⁴ (всего пользователей в мире)	2 740	2 291	1 221	689	–	–
Napoleon Cat ⁵ (всего пользователей в России)	69,4	–	62,9	–	–	–
Brand Analytics ⁶ (авторов в месяц в России)	8,5	38,1	5,1	–	2,9	23,8

Приложения на пользовательских устройствах интернет-аудитории (в том числе детской и подростковой), которые потенциально могут содержать деструктивный материал, можно разделить на следующие категории:

- социальные сети и мессенджеры;
- мобильные или компьютерные игры;
- развлечения посредством (и без) приложений сети Интернет.

¹ Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

² Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

³ Most popular social networks worldwide as of January 2023, ranked by number of monthly active users // Statista. URL: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (дата обращения: 19.04.2023).

⁴ Digital 2021: The latest insights into the 'State of Digital' // We Are Social. URL: <https://wearesocial.com/uk/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital> (дата обращения: 19.04.2023).

⁵ Social media users in Russian Federation, November 2021 // NapoleonCat. URL: https://napoleoncat.com/stats/social-media-users-in-russian_federation/2021/11/ (дата обращения: 19.04.2023).

⁶ Черный В. Социальные сети в России: цифры и тренды, осень 2021 г. // Brand Analytics. URL: <https://br-analytics.ru/blog/social-media-russia-2021/> (дата обращения: 19.04.2023).

Рассмотрим каждую из перечисленных категорий подробнее:

1. Социальные сети. К таким ресурсам относятся: «ВКонтакте», «Одноклассники», Facebook¹, Twitter, Snapchat, Instagram², TikTok, Clubhouse.

«ВКонтакте» – самая крупная социальная сеть в русскоязычном сегменте Интернета, создана в 2006 г. Страна происхождения: Россия. Принадлежит компании VK. Аудитория – более 100 млн пользователей в месяц, число сообщений ежедневно – 15 млрд³. Возможности ресурса: создание профиля пользователя с персональной информацией, создание сообщества, мультимедийных материалов, групп в мессенджере платформы для общения, прослушивание музыки и др. Контент изобилует рекламой, включает встроенные покупки. В обычный день ресурс посещают пользователи в возрасте 12+ и проводят в нем примерно 45 мин⁴. Администрация социальной сети регулярно модерирует страницы на наличие информационных угроз и деструктивного контента, однако материалы сомнительного содержания продолжают присутствовать внутри площадки.

«Одноклассники» – социальная сеть, популярная среди взрослой части населения (возрастной категории старше 30 лет). Создана в 2006 г. Страна происхождения: Россия. Принадлежит компании VK. Аудитория – примерно 41 млн пользователей в месяц⁵. В средний день ресурс посещают пользователи в возрасте 12+ и проводят в нем более 30 мин⁶. Возможности сети в целом аналогичны «ВКонтакте».

Facebook⁷ – социальная сеть, создана в 2004 г. Страна происхождения: США. Считается крупнейшей в мире⁸. Возможности ресурса: создание профиля пользователя с размещением в нем разнообразной персональной информации, обмен сообщениями, мультимедийным материалом, создание сообществ и т. п.

4 марта 2022 г. принято решение о блокировке доступа к сети Facebook на территории Российской Федерации на основании 272-ФЗ⁹.

¹ Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

² Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

³ О нас // «ВКонтакте». URL: <https://vk.com/about> (дата обращения: 19.04.2023).

⁴ Интернет // Mediascope. URL: <https://mediascope.net/services/media/media-audience/internet/description> (дата обращения: 19.04.2023). Режим доступа: через запрос о составлении отчета.

⁵ Что такое «Одноклассники»? // Проект «Одноклассники». URL: <https://insideok.ru/info> (дата обращения: 19.04.2023).

⁶ Интернет // Mediascope. URL: <https://mediascope.net/services/media/media-audience/internet/description> (дата обращения: 19.04.2023). Режим доступа: через запрос о составлении отчета.

⁷ Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

⁸ Digital 2022: Another year of bumper growth // We Are Social. URL: <https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2> (дата обращения: 19.04.2023).

⁹ Приняты ответные меры на ограничение доступа к российским СМИ // Роскомнадзор. URL: <https://rkn.gov.ru/news/rsoc/news74156> (дата обращения: 19.04.2023).

*Instagram*¹ – платформа для обмена фотографиями и видео с элементами социальной сети. Страна происхождения: США. Фото и видео с содержанием насилия встречаются редко.

Данный ресурс также заблокирован на территории Российской Федерации с 4 марта 2022 г. на основании 272-ФЗ.

До блокировки опасность представляли (однако не исключено, что такой контент присутствует до сих пор) «челленджи» – вызовы по требованиям, в которых отдельные пользователи совершали нечто странное, необычное, а затем передавали эстафету другим, либо «гивы» (англ. giveaway – раздача) – способ привлечь аудиторию, часто связанный с агрессивной рекламой и попытками получить от пользователя денежные средства.

TikTok – платформа для размещения коротких мобильных видео. Создана в 2018 г. Страна происхождения: КНР. Принадлежит компании ByteDance. Количество активных пользователей – около 1 млрд². Интеллектуальный посыл контента в содержательном плане сводится к минимуму. Приложение с легкостью «убивает» время в бесполезных развлечениях. Контент проходит несущественную модерацию, на ресурсе встречается ряд информационных угроз: откровенные видео под популярные музыкальные композиции, провокационные челленджи, нецензурная лексика.

Twitter – социальная сеть, которая строится на основе ведения микроблога, ограниченного 280 символами. Аудио- и видеоконтент ограничен 140 с. Создан в 2006 г. Страна происхождения: США. Принадлежит компании Twitter, Inc. Количество активных пользователей – 436 млн³. Возможности ресурса: создание твитов (наименование сообщений), их пересылка, цитирование, выделение понравившихся сообщений, размещение мультимедийного материала.

С 1 марта 2022 г. доступ к ресурсу заблокирован на территории Российской Федерации по требованию Генеральной прокуратуры Российской Федерации.

Clubhouse – социальная сеть, основанная на создании голосовых комнат и ведении в них голосового общения. Создана в мае 2020 г. Страна происхождения: США. Разработана компанией Alpha Exploration Co. По данным на февраль 2021 г., сеть имела аудиторию более 2 млн пользователей⁴. Ее особенностью является

¹ Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

² Digital 2022: Another year of bumper growth // We Are Social. URL: <https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2> (дата обращения: 19.04.2023).

³ Там же.

⁴ Clubhouse app: what is it and how do you get an invite to the exclusive audio app? // The Guardian. URL: <https://www.theguardian.com/technology/2021/feb/17/clubhouse-app-invite-what-is-it-how-to-get-audio-chat-elon-musk> (дата обращения: 20.04.2023).

отсутствие работы камеры через приложение. Вход (или добавление нового пользователя) осуществляется только по приглашению («инвайту», англ. invite – приглашать) зарегистрированного пользователя (всего он имеет два приглашения).

Сервис отличается усиленной конфиденциальностью: чаты удаляются в автоматическом режиме после окончания беседы, что отличает данный контент от подкаста или стрима. Требование указать при регистрации ПДн, а также предоставить приложению доступ к списку контактов на мобильном устройстве представляет очевидную угрозу ИБ пользователя. Помимо этого, сервис является потенциально опасным для молодежной аудитории, так как с одного аккаунта несколько человек могут слушать беседу с одного же устройства и участвовать в ней. То, что обсуждается пользователями социальной сети, практически невозможно проконтролировать, а голосовые комнаты могут создаваться для распространения деструктивного контента.

2. Игры. Интегративный показатель сетевой активности пользователей поднимает игры на второе место по популярности. Примерно 27 % своего времени подростки проводят в любимой игре на мобильном устройстве. Многие игры имеют возрастные ограничения, однако получить доступ к играм не составляет труда, например путем скачивания на торрент-трекере или при игре онлайн. Некоторые сюжеты игр содержат большое количество жестокости, откровенных сцен с обнажением, имитацией полового акта, матерной бранью (к примеру, Grand Theft Auto, Mass Effect, «Ведьмак», God of War, Far Cry). Опасность мобильных игр заключается в направленности на невнимательность или незнание пользователя (например, ребенка) при выборе элементов игры (нажатие на появляющиеся баннеры, всплывающие части программы), вследствие чего выбранное может переадресовывать на страницу для оплаты или показывать рекламу для более взрослой аудитории (казино, ставки, сетевые ресурсы для взрослых). Продолжительность нахождения в игре составляет от одного до четырех и более часов в день.

3. Развлечения. Видеохостинг Youtube, а также Instagram¹ и TikTok утвердились в качестве лидеров развлекательного контента среди аудитории. Среднее время, проводимое пользователем на данных интернет-ресурсах в течение суток, составляет не менее трех часов.

YouTube – лидер по популярности использования среди пользователей сети Интернет. Ресурс создан в 2005 г. Страна происхождения: США. Принадлежит компании Google LLC. Возможности видеохостинга: просмотр уже созданных другими пользователями видеороликов, а также создание собственных, коммен-

¹ Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

тирование и оценивание видеоматериалов, онлайн-вещание, создание коротких видео. Большое количество рекламы присутствует как в самих видеоматериалах, так и в виде баннеров.

Встречаются видеоролики, имеющие сексуальный подтекст, содержащие фрагменты жестокости. Алгоритмы платформы достаточно быстро определяют подобный контент и блокируют его, но в завуалированном виде такой материал может оставаться. Однако стримы блогеров практически не блокируются.

Из рассмотренного материала очевидны популярность социальных сетей и их большое количество. Причины такой распространенности происходят из психологических особенностей человека. Социализация, потребность в общении, доступность развлекательного контента – все это способствует неугасающей популярности таких ресурсов. Однако проблема наличия в них негативного контента и деструктивных материалов, несмотря на все попытки и стремления бороться с их появлением, не теряет актуальности.

Таким образом, социальные сети – популярное средство для распространения деструктивного контента. В них создаются тематические группы, которые распространяют (продвигают, идеализируют и пр.): идеи убийства (группы о серийных убийцах, насильниках и маньяках), сатанизм, нацизм, национализм, расизм, крайние взгляды, суицидальные намерения, религиозные и квазирелигиозные объединения (секты). Все обозначенное может склонять несовершеннолетнего и (или) психически несформированное, внушаемое лицо к совершению правонарушений (мелкое хулиганство, нарушение правил дорожного движения, драки, распространение экстремистских материалов и др.) и преступлений (вандализм, хулиганство, участие в деятельности запрещенных организаций, причинение вреда здоровью различной тяжести и др.).

§ 2.2. Мессенджеры: понятие, анализ возможностей, виды деструктивного материала

Наиболее популярными средствами коммуникации на сегодняшний день являются программы для обмена короткими сообщениями – мессенджеры (англ. messenger – посыльный, курьер, разносчик). На заре развития мобильной связи основными средствами обмена сообщениями были SMS (аббр., англ. short message service – короткое сообщение, смс) и MMS (аббр., англ. multimedia messaging service – служба мультимедийных сообщений), которые позволяли пересылать текстовые и мультимедийные данные соответственно. В эпоху Интернета их практически полностью заменили мессенджеры, объединив в себе вышеперечисленные функции.

Мессенджер представляет собой ПО, предназначенное для обмена мгновенными сообщениями. Подобные программы устанавливаются в качестве приложения на компьютере и мобильном устройстве (планшете или смартфоне)¹.

Общими возможностями, которые характерны практически для всех современных мессенджеров, являются:

- отправка текстовых сообщений (стандартная функция любого мессенджера);
- отправка файлов (документы, изображения, архивы и пр.) и мультимедийных данных (фотоизображения, речевая информация в виде записанного человеческого голоса, видеосообщения);
- создание групп или чатов, к которым могут присоединяться пользователи программы (количество участников таких групп зависит от мессенджера, например в WhatsApp – до 512, а для Telegram может достигать 200 тыс.);
- отправка своего местоположения: функция позволяет использовать геопозицию по данным из мобильного устройства и пересылать ее другому пользователю;
- совершение аудио- и видеозвонков через приложение;
- шифрование данных при их пересылке: многие мессенджеры имеют подобную функциональность (например, WhatsApp, Telegram, Signal), передаваемые данные (текст, фото, видео и т. д.) криптографически изменяются, что не дает постороннему лицу ознакомиться с их содержанием;
- иная функциональность конкретного мессенджера.

В Российской Федерации, согласно данным ВЦИОМ², чаще всего пользуются WhatsApp (87 %), Telegram (55 %) и Viber (37 %).

Распределение популярности по континентам и государствам, согласно данным MessengerPeople³, можно обозначить следующим образом (рис.): наиболее популярным мессенджером является WhatsApp (распространен в странах Южной Америки и Африки, в России и государствах постсоветского пространства); следующим по распространенности является Facebook Messenger (Северная Америка, Австралия, Северная Африка, некоторые государства Европы); Viber (страны Восточной Европы); WeChat (азиатские страны, пре-

¹ Цифровая экономика: Концептуальные основы правового регулирования бизнеса в России : монография / отв. ред. В. А. Лаптев, О. А. Тарасенко. М. : Проспект, 2021.

² Российская аудитория социальных сетей и мессенджеров: изменения на фоне спецоперации // ВЦИОМ. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/rossiiskaja-auditorija-socialnykh-setei-i-messendzherov-izmeneniya-na-fone-specoperacii> (дата обращения: 20.04.2023).

³ WhatsApp, WeChat and Facebook Messenger Apps – Global usage of Messaging Apps, Penetration and Statistics // Messenger People. URL: <https://www.messengerpeople.com/global-messenger-usage-statistics/#APAC> (дата обращения: 20.04.2023).

имущественно Китай); Telegram популярен в Средней Азии; в Японии используют мессенджер Line. Сравнение популярности мессенджеров в мире представлено в табл. 2.

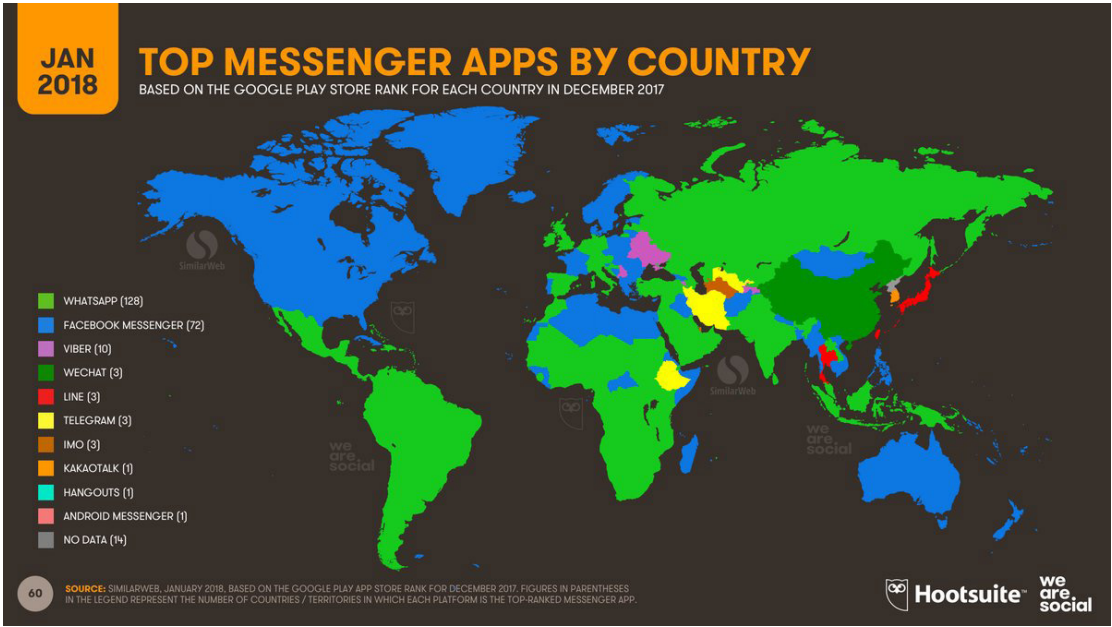


Рис. Распределение популярных мессенджеров по континентам (данные на декабрь 2017 г.)

Таблица 2

Сравнение популярности мессенджеров
(в млн пользователей)¹

Источник данных	Мессенджер				
	WhatsApp	Weixin/ WeChat	Facebook Messenger	SnapChat	Telegram
Statista (активных пользователей в месяц в мире)	2 000	1 263	988	557	550

¹ Most popular global mobile messenger apps as of January 2022, based on number of monthly active users // Statista. URL: <https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps> (дата обращения: 20.04.2023).

WhatsApp – самый популярный мессенджер в России, им пользуются примерно 70 % населения¹. Создан в 2009 г. Страна происхождения: США². Возможности мессенджера: отправка сообщений, реагирование на сообщение с использованием эмодзи, создание групп до 512 пользователей, исчезающие сообщения, сквозное шифрование, создание бизнес-аккаунтов, аудио- и видеозвонки. Есть приложения для мобильных устройств и компьютеров большинства основных ОС.

Потенциальная опасность данного мессенджера заключается в том, что проконтролировать переписку практически невозможно (например, для несовершеннолетнего). Рассылать сообщения, как, впрочем, и в любом другом мессенджере, может кто угодно (представители преступного сообщества, группы с деструктивным контентом и т. д.).

В WhatsApp приобрела популярность игра «Момо» – аналог «Синего кита», в котором незнакомцы при переписке с детьми присылают картинки со сценами насилия. В СМИ подобные группы именуются «группами смерти», их кураторы ментально воздействуют на несовершеннолетних и призывают их к деструктивным действиям, суициду.

Telegram – второй по популярности в России мессенджер (согласно опросу ВЦИОМ³), считающийся наиболее безопасным, поскольку для сообщений используются алгоритмы шифрования (однако оно осуществляется не на устройстве, а на сервере). Создан в 2013 г. Страны происхождения: Россия, Объединенные Арабские Эмираты. Как компания Telegram зарегистрирован на Британских Виргинских островах, а как LLC (компания с ограниченной ответственностью) – в Дубае. Возможности мессенджера: групповые чаты до 200 тыс. пользователей; секретные чаты (удаляются по времени, нет возможности сделать скриншот в приложении на iOS); создание ботов, которые позволяют выполнять команды пользователей; создание каналов, в которых пользователи могут размещать разнообразную информацию (от текста до видеофайлов). На сегодняшний день телеграм-каналы используются как официальными СМИ, ОГВ, так и различными компаниями (для ведения бизнес-аккаунтов), а также, конечно, отдельными гражданами. Существует альтернативное приложение, написанное официальными разработчиками мессенджера, – Telegram X.

В политике безопасности приложения сообщается, что мессенджер не контролирует и не несет ответственности за размещаемый контент. Пользователи имеют право информировать службу поддержки

¹ Личные встречи не вышли из моды // ВЦИОМ. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/lichnye-vstrechi-ne-vyshli-iz-mody> (дата обращения: 20.04.2023).

² О WhatsApp // WhatsApp. URL: <https://www.whatsapp.com/about> (дата обращения: 20.04.2023).

³ Российская аудитория социальных сетей и мессенджеров: изменения на фоне спецоперации // ВЦИОМ. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/rossiiskaja-auditorija-socialnykh-setei-i-messendzherov-izmeneniya-na-fone-sпецоперации> (дата обращения: 20.04.2023).

о каких-либо нарушениях. Также мессенджер был неоднократно уличен в наличии информации деструктивного содержания и активно используется преступниками¹.

Viber – третий по популярности в России мессенджер. Согласно опросу ВЦИОМ, им пользуются 37 % респондентов². Создан в 2010 г. Страна происхождения: Израиль. Принадлежит компании Rakuten, Inc. (Япония). Ежемесячная аудитория, по собственным данным мессенджера, составляет сотни миллионов пользователей³. Возможности практически аналогичны любым мессенджерам. Число пользователей в группах – до 250. Отличительной функцией является специальный тариф Viber Out, который позволяет осуществлять VoIP (аббр., англ. Voice over Internet Protocol – букв. «голос по интернет-протоколу») – звонки на любые номера (мобильные и (или) городские) по всему миру, при этом наличие приложения Viber на устройстве адресата не обязательно. Имеются приложения для мобильных устройств и компьютеров большинства основных ОС.

Weixin/WeChat – мессенджер, созданный в 2011 г. Страна происхождения: КНР. Принадлежит компании Tencent Holdings Limited (КНР). Популярен в азиатских странах. Помимо стандартных возможностей мессенджер имеет обширную функциональность, по своим характеристикам и объему реализованного больше напоминающую медиаплатформу. В WeChat поддерживаются: обмен контактами через Bluetooth; платежная система WeChat Pay (оплата покупок, перевод денежных средств); перевод текста через камеру мобильного устройства; групповые чаты до 500 участников; использование приложения для идентификации личности (документы при себе иметь не нужно); возможность заказа такси; присутствие различных площадок для продаж или аренды (например, жилья). Про какие-либо меры защиты вроде шифрования информации нет.

SnapChat – мессенджер, созданный в 2011 г. Страна происхождения: США. Принадлежит компании Snap Inc. (США). Мультимедийное приложение (позволяет пересылать в основном фото- и видеоконтент), особенностью которого является то, что пересланные сообщения удаляются через определенный промежуток времени (как правило, 24 ч). Возможно добавлять фильтры, рисовать на изображениях, уведомлять отправителя в случае, если кто-то делает скриншот переписки.

¹ Суходолов А. П., Бычкова А. М. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Телеграм» в распространении наркотиков // Всероссийский криминологический журнал. 2019. Т. 13. № 1. С. 5–17; Гарагашева Е. П., Молина О. В., Тальчук О. В. Роль телеграм-каналов в пропаганде самоубийства // Университетская медицина Урала. 2021. Т. 7. № 2 (25). С. 44–45.

² Российская аудитория социальных сетей и мессенджеров: изменения на фоне спецоперации // ВЦИОМ. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/rossiiskaja-auditorija-socialnykh-setei-i-messendzherov-izmeneniya-na-fone-specoperacii> (дата обращения: 20.04.2023).

³ О Viber // Viber. URL: <https://www.viber.com/ru/about> (дата обращения: 20.04.2023).

Threema – мессенджер, созданный в 2012 г. Страна происхождения: Швейцария. Принадлежит компании Threema GmbH (Швейцария). Аудитория – примерно 10 млн пользователей. Поддерживает все стандартные и распространенные функции мессенджеров: групповые чаты до 256 участников, обмен мультимедийными данными, отправка местоположения и т. п. Считается одним из наиболее защищенных в плане обмена сообщениями: применяется криптографическое преобразование (сквозное шифрование); отсутствует необходимость привязывать номер телефона или электронную почту к приложению; для идентификации пользователя используется генератор случайных чисел. Мессенджер можно размещать на собственных серверах компаний. Также приложение не позволяет самостоятельно удалять сообщения по истечении периода, определенного собеседниками, и не дает делать скриншот переписки.

Wickr Me – мессенджер, созданный в 2013 г. Страна происхождения: США. Принадлежит компании Wickr, Inc. (дочерняя компания Amazon Web Services, Inc., США). Данные по аудитории отсутствуют. Существует несколько версий ПО: стандартная, для любых пользователей (указанная выше одноименная); для предприятий (*Wickr Pro*); больших компаний (*Wickr Enterprise*); вооруженных сил (*Wickr RAM*). Особенностью приложения является то, что, как и в *Threema*, не требуется привязка электронной почты или номера телефона, поскольку для каждого пользователя генерируется уникальный идентификатор. Для защиты переписки применяются передовые криптографические алгоритмы шифрования: AES 256, SHA 256, ECDH 521, RSA 4096 TLD. Ключи шифрования хранятся на устройстве пользователя. Метаданные из сообщения удаляются при отправке. Разработчики мессенджера сотрудничают с силовыми структурами, например в США.

Signal – мессенджер, созданный в 2014 г. Страна происхождения: США. Разрабатывается некоммерческими фондами Signal Foundation и Signal Messenger LLC. Аудитория насчитывает примерно 105 млн пользователей. По умолчанию имеется принудительное сквозное шифрование (криптографически изменяется все, что пересылается, будь то переписка между двумя пользователями или в групповых чатах), в отличие от Telegram, в котором функция реализуется при создании конфиденциального чата. В приложении помимо стандартных функций и шифрования возможны: создание исчезающих сообщений, видео-конференц-связь до восьми участников, групповые чаты до тысячи пользователей, размытие лиц на пересылаемых снимках.

ICQ – мессенджер с богатой историей. Создан в 1996 г. Страна происхождения: Израиль. Принадлежит компании VK (Россия). Точные данные об аудитории неизвестны, фигурируют различные цифры – чаще всего около 10 млн пользователей. Функциональность в основном стандартная, но некоторые отличительные черты присутствуют: возможно создавать группы до 25 тыс. участников, осуществлять видеозвонки до 30 участников, переводить голосовое сообщение в текст, создавать ботов. Информации о безопасности передачи данных или модерации от деструктивных материалов не обнаружено.

Перечисленные мессенджеры не конечны, существует немало количество иных: Facebook Messenger¹ (в Российской Федерации не так популярен; имеет сквозное шифрование, которое необходимо активировать; собирает большое количество данных о пользователе и передает их на серверы Facebook²); «VK Мессенджер» от одноименной социальной сети (численность аудитории неизвестна; шифрования нет; все чаты сохраняются на серверах VK); Wire (со сквозным шифрованием, используется в корпоративном секторе); Briar (со сквозным шифрованием, отсутствует голосовая связь, представлен не на всех известных ОС) и др.

Таким образом, количество современных мессенджеров довольно велико, а возможности, которые они позволяют реализовать в целях общения и не только, также обширны. Средства защиты – наличие шифрования, секретных чатов и т. п. – помогают пользователям, однако вызывают трудности в работе правоохранительных органов: оперативно вычислить лицо, которое использует мессенджер не для обычного общения, а для занятия противоправной деятельностью и распространения негативных материалов, становится сложнее.

Как нами уже упоминалось, преступники часто используют защищенные мессенджеры, например при реализации наркотических веществ, пропаганде суицида, подготовке к совершению террористических актов, распространении иных материалов деструктивного содержания.

Вопросы для повторения и самостоятельного контроля

1. Что понимается под современной социальной сетью в сети Интернет?
2. Какие возможности социальные сети дают пользователям?
3. Какие категории приложений (ресурсов), которыми пользуется интернет-аудитория, возможно выделить как потенциально содержащие деструктивный материал (контент)?
4. Дайте характеристику, описание современных социальных сетей: разновидности, функциональность, особенности.
5. Что такое мессенджеры?
6. Какие возможности мессенджеры дают пользователям?
7. Дайте характеристику, описание современных мессенджеров: разновидности, функциональность, особенности.
8. Социальные сети и мессенджеры как источники деструктивных материалов. Виды угроз при использовании.

¹ Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

² Принадлежит компании Meta Platforms Inc., признанной на территории Российской Федерации экстремистской организацией.

ГЛАВА 3 ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОИСКУ И ПРОТИВОДЕЙСТВИЮ РАСПРОСТРАНЕНИЮ ДЕСТРУКТИВНОГО КОНТЕНТА

§ 3.1. Правовые методы противодействия

Выделим некоторые практические способы и методы противодействия распространению деструктивного материала и поведению, проявляющемуся из-за его воздействия на субъект:

- формирование негативного образа и эмоционального неприятия преступных организаций, действий их лидеров, адекватное реагирование на любые пропагандистские акции со стороны последних;
- прямое разоблачение, противопоставление истины преступным инсинуациям;
- распространение правдивой, достоверной информации о тех или иных обстоятельствах;
- развитие психологического позитивного мышления вместо разрушительного, раскрытие позитивных жизненных смыслов, развитие способности к целеполаганию;
- проведение нравственно-правового закаливания (формирование правовой культуры, навыков критического анализа, сопротивления негативному влиянию, развитие стойкости при неблагоприятных обстоятельствах, умения противостоять влиянию других лиц);
- перекрытие каналов распространения информации деструктивного содержания от злоумышленников через СМИ и сеть Интернет, досудебная их блокировка;
- мониторинг СМИ и информационных ресурсов сети Интернет, выявление информации, содержащей сведения, приводящие к радикализации молодежи, определение лиц, распространяющих ее, и последующее их задержание;
- международное взаимодействие правоохранительных органов и обмен между ними разнообразной информацией, аккумулирование практики расследования преступлений.

Рассмотрим процедуру и порядок ограничения доступа к интернет-ресурсу, содержащему информацию, распространение которой на территории Российской Федерации запрещено. Согласно п. «а» ст. 5 постановления Правительства Российской Федерации № 1101 МВД России уведомляет Роскомнадзор об обнаружении URL-ресурса, который содержит информацию, распространяемую посредством сети Интернет, о способах, методах разработки, изготовления и использования наркотиче-

ских средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, а также о способах и местах культивирования наркосодержащих растений.

Данные действия предусматриваются ст. 15.1 149-ФЗ. Блокировка может осуществляться в трех случаях:

- 1) в досудебном порядке;
- 2) на основании постановления судебного пристава-исполнителя (п. 3 ч. 5 ст. 15.1 149-ФЗ);
- 3) на основании вступившего в законную силу судебного решения (п. 2 ч. 5 ст. 15.1 149-ФЗ).

Приведем алгоритм взаимодействия и блокировки противоправного контента в сети Интернет:

1. На основании п. 6 постановления Правительства Российской Федерации № 1101 на официальном сайте Роскомнадзора по адресу <https://eais.rkn.gov.ru/feedback> размещается электронная форма, которую должны заполнить представители ОГВ и иные заявители:

- в поле «Тип информации» из предложенного выбирается тип контента;
- в поле «Указатель страницы сайта в сети Интернет» указывается конкретный URL-адрес сайта, на котором обнаружена информация, подлежащая блокировке (не рекомендуется указывать адреса из поисковых запросов сайтов, например Google, «Яндекс» и т. п.);
- в поле «Скриншот» добавляется скриншот в формате .pdf, .jpeg или .png; размер файла – не более 1 Мб;
- в поле «Вид информации» отмечается конкретный вид информации, размещенной на указанном URL-адресе сайта;
- в поле «Доступ к информации» из выпадающего списка выбирается разновидность информации: свободная, ограниченная либо платная;
- в поле «Дополнительная информация» указываются необходимые дополнительные сведения, которые нужны для доступа к обозначаемому ресурсу;
- в разделе «Заявитель» и в соответствующих полях необходимо указать данные о заявителе: Ф. И. О., год рождения, место работы (службы), страну и регион местонахождения, контактный адрес электронной почты.

2. Информация из указанной формы направляется в уполномоченный Правительством Российской Федерации ФОИВ (МВД России, Роскомнадзор, Роспотребнадзор, ФНС России и Росалкогольрегулирование) для принятия решения о наличии либо отсутствии запрещенной или ограниченной информации.

Критерии оценки вышеуказанных материалов и (или) информации регламентируются межведомственным приказом¹.

В случае работы с Роскомнадзором подразделениями МВД России напрямую *алгоритм передачи сведений* следующий:

1. Подготовка официального письма с указанием в нем данных о каком-либо ресурсе и размещенной в нем информации с признаками запрещенной либо подлежащей ограничению: конкретный URL-адрес сайта, указание вида, формы и основания блокировки. К документу прилагается скриншот указанной страницы в сети Интернет.

2. Направление письма в адрес Роскомнадзора.

Алгоритм может использоваться не только для обмена информацией, но и для удаления контента. Производится это на основании ч. 1 ст. 15.3 149-ФЗ в случае обнаружения в ИТКС, в том числе в сети Интернет, призывов: к осуществлению экстремистской деятельности; участию в массовых (публичных) мероприятиях, проводимых с нарушением закона; распространению недостоверных общественно значимых сведений, создающих угрозу причинения вреда жизни и (или) здоровью граждан.

Роскомнадзор обязан незамедлительно уведомить редакцию сетевого издания (в случае, если оно было зарегистрировано в качестве СМИ) о необходимости удаления размещенной на его платформе информации, что издание обязано выполнить. Если данное требование не исполняется, то доступ к сетевому изданию, в котором размещается запрещаемая информация, ограничивается через оператора связи и (или) провайдера хостинга.

Информация о заблокированном ресурсе попадает в единую автоматизированную информационную систему «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». Указанный реестр размещен по адресу <https://eais.rkn.gov.ru>, его ведение осуществляется Роскомнадзором.

¹ Приказ Роскомнадзора, МВД России, Роспотребнадзора, ФНС России от 18 мая 2017 г. № 84/292/351/ММВ-7-2/461@ «Об утверждении Критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, Федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети Интернет, а также сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие запрещенную информацию, в единую автоматизированную информационную систему „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”» // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru/File/GetFile/0001201706290015?type=pdf> (дата обращения: 20.04.2023).

Проверить ограничение доступа к сайтам и (или) страницам сайтов сети Интернет можно по адресу <https://blocklist.rkn.gov.ru>.

Федеральный список экстремистских материалов ведется, публикуется и размещается в сети Интернет Министерством юстиции Российской Федерации на основании ст. 13 Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности», п. 7 Положения о Министерстве юстиции Российской Федерации, утвержденного Указом Президента Российской Федерации от 13 октября 2004 г. № 1313. Размещен он по адресу <https://minjust.gov.ru/ru/extremist-materials>.

Единый федеральный список организаций, в том числе иностранных и международных, признанных в соответствии с законодательством Российской Федерации террористическими, ведется ФСБ России и доступен по адресу <http://www.fsb.ru/fsb/npd/terror.htm>.

Помимо перечисленного, Роскомнадзором совместно с Союзом журналистов России ведется Перечень информационных ресурсов, регулярно распространяющих недостоверную информацию. Этот список составлен на основании решений Генеральной прокуратуры Российской Федерации в целях исполнения положений ст. 15.3 149-ФЗ, адрес следующий: <https://rkn.gov.ru/mass-communications/p1104>.

§ 3.2. Технические методы противодействия

Находить информацию в сети Интернет технически возможно несколькими способами:

- а) путем написания конкретного электронного адреса в строке браузера (веб-обозревателя);
- б) путем написания обычного запроса через поисковые системы;
- в) используя расширенные возможности вышеуказанных поисковых систем;
- г) автоматизированно – при помощи специальных программных продуктов.

Рассмотрим данные действия подробнее:

1. Поиск информации через браузер состоит из написания в браузере конкретного искомого URL-адреса и получения ответа в виде загрузки и отображения содержания запрашиваемой страницы. Этот способ используется, если адрес известен. Наиболее распространенные браузеры: Google Chrome, «Яндекс.Браузер», Mozilla Firefox, Opera, Microsoft Edge, Safari.

2. Поиск информации путем написания обычного запроса через поисковые системы («Яндекс», Google, Bing, Yahoo!, Baidu и др.) состоит из следующих действий:

– открытие страницы поисковой системы и написание в поисковой строке запроса (названия страниц, связанных с искомым словом и (или) словосочетанием);

– отображение в поисковой системе предложений с гиперссылками проиндексированных интернет-страниц;

- поиск искомого и (или) выбор из предложенных страниц;
- загрузка содержания выбранной страницы.

Этот способ используется, если точный URL-адрес неизвестен, однако могут быть известны ключевые слова, названия страницы или содержание контента страницы.

3. Поиск информации пользователем путем использования расширенных возможностей поисковых систем, например Google Dorking или Google Hacking. Последовательность действий: открытие страницы поисковой системы и написание в поисковой строке запроса с добавлением оператора (это ключевое слово или фраза, несущие особое значение для поисковой системы) и (или) команды.

Примеры команд расширенного поиска Google:

- а) site – поиск по конкретному сайту;
- б) inurl – обозначение того, что искомые слова должны быть частью адреса страницы или сайта;
- в) allintitle – поиск всех слов из поискового запроса;
- г) intitle – оператор поиска в заголовке самой страницы;
- д) ext или filetype – поиск файлов конкретного типа по расширению;
- е) cache – поиск сохраненной (удаленной) страницы, хранящейся в кеше поисковой системы.

Примеры операторов, которые задаются спецсимволами для создания расширенного поискового запроса:

а) | – оператор OR или его аналог «вертикальный слеш» (логическое «или») указывает, что нужно отобразить результаты, содержащие хотя бы одно из слов, перечисленных в запросе;

б) – – оператор «минус» используется для исключения из выдачи результатов с указанными после минуса словами;

в) + – оператор «плюс» означает обязательное включение в поиск слов, указанных после оператора;

г) * – оператор «звездочка» означает пропуск одного или нескольких слов в запросе;

д) " " – оператор «двойные кавычки» означает поиск с вхождением фразы точно в указанной форме;

е) # или @ – операторы «решетка» или «коммерческое at» означают поиск результатов с указанным хештегом или ником и т. д.

Примеры расширенных поисковых запросов, команды которых должны вводиться на английском языке, а сам поисковый запрос может вводиться на русском: «#winter»; «cache:www.URL-адрес.ru»; «inurl:instagram @nik»; «site:www.vk.com»; «оружие –АК-47»; «место встречи * нельзя».

Использование подобных операторов и команд возможно и в других поисковых системах («Яндекс», Mail.ru, Bing, Yahoo! и др.).

Последовательность выдачи результатов такого поиска аналогична предыдущему способу поиска информации в сети Интернет через поисковые системы. Различие состоит в том, что ответы на запросы будут выдаваться более точно и менее обширно, так как размещенный оператор и поставленная команда будут конкретизировать искомое.

4. Поиск информации в автоматизированном режиме при помощи специального ПО. К таковым возможностям относятся некоторые специальные веб-страницы (поисковые системы), ПО, разработанное для анализа информации в глобальной сети и предоставления искомых результатов в форме текстов, графиков, иллюстраций. Такой поиск информации, основанный на данных, размещенных в открытых источниках, называется OSINT (англ. Open Source INtelligence – букв. «открытые источники разведки»).

Примеры поисковых систем: Carrot (<https://search.carrot2.org/#/search/web>) – сортирует результаты поиска по тематическим папкам и показывает в виде круговой диаграммы и тримапа¹; Social Search (<https://www.social-searcher.com>) – производит поиск по упоминаниям в социальных сетях и поисковых системах (производит поиск и по «ВКонтакте»); Watson News Explorer (<https://news-explorer.mybluemix.net>) – банк данных новостей по всему миру, при помощи которого возможно анализировать личности, компании, конкретные темы; WhatsMyName Web (<https://www.whatsmyname.app>) – инструмент по поиску имен пользователей в Интернете; Censys (<https://censys.io>) – позволяет находить подключенные к Интернету устройства (серверы, доменные имена).

Примеры ПО: Maltego – программа, предназначенная для анализа разнообразных данных (метаданные, упоминания об искомом объекте) из открытых источников и выстраивающая логические связи в виде графов и иного наглядного представления; Срееру – инструмент, позволяющий из открытых данных определять местоположение искомого объекта (программа обращается к социальным сетям); Nmap – бесплатная утилита, позволяющая анализировать сеть и находить сведения об IP- и DNS-адресах, обнаруживать конкретные виды ОС, подключенные хосты и другие программные решения.

Использование сотрудником ОВД указанных ресурсов позволит быстро и эффективно находить конкретную информацию, лицо и (или) группу лиц, размещающих информацию разнообразного содержания (в том числе и деструктивного), анализировать данные об искомом объекте, устанавливая его связи в сети либо на каком-либо отдельном ресурсе, в некоторых случаях определять их местонахождение, а в итоге – предпринимать меры по блокировке ресурса.

¹ Тримап – метод визуализации информации с использованием вложенных фигур.

Вопросы для повторения и самостоятельного контроля

1. Какие практические способы и методы противодействия распространению деструктивного контента в сети Интернет существуют?
2. Согласно нормам какого НПА утверждаются процедура и порядок ограничения доступа к интернет-ресурсу, содержащему информацию, распространение которой запрещено на территории Российской Федерации?
3. Блокировка интернет-ресурса может осуществляться согласно 149-ФЗ. Обозначьте, в каких случаях это возможно.
4. Обозначьте алгоритм действий сотрудника ОВД по передаче сведений об интернет-ресурсе, нарушающем требования законодательства и содержащем информацию, распространение которой в Российской Федерации запрещено, напрямую с Роскомнадзором.
5. Какие существуют практические способы поиска информации в сети Интернет?
6. Как называются запросы, которые задаются спецсимволами для создания расширенного поискового запроса?
7. Какие существуют специальные программы для поиска информации в сети Интернет?
8. На каких ресурсах можно ознакомиться с перечнем сайтов и (или) страниц сайтов сети Интернет, размещавших информацию, распространение которой на территории Российской Федерации запрещено, а также заблокированных в установленном порядке?

ЗАКЛЮЧЕНИЕ

Цифровой мир сегодня – существенная часть жизни многих граждан. Для молодежной аудитории он выступает ключевым фактором социализации и личностного развития. Глобальная сеть трансформировалась в пространство не только новых возможностей, но и рисков и угроз, которые сопряжены с видами деструктивной информации и, как следствие, разрушительного поведения.

Высокие темпы цифровизации и особенности глобального информационного пространства, недостаточный уровень цифровой грамотности и позитивной цифровой культуры, возрастно-психологические особенности отдельных групп в широкой аудитории пользователей и потребителей интернет-информации деструктивного содержания или воздействия делают их уязвимыми к опасностям и угрозам информационной безопасности, которая может перерасти в личную, психологическую или общественную безопасность. Ее ресурсы, формы и последствия потребления разнообразны: социальные сети, видеохостинги, отдельные сайты и блоги; тексты и сообщения, видео, аудио, интерактив; побуждение к совершению противоправных действий, оправдание противоправного или аморального поведения, содержание сведений экстремистского и террористического характера, пропаганда насилия, популяризация наркотиков и алкоголя и др.

Борьба с информацией деструктивного содержания в сети Интернет сегодня выступает одним из приоритетных направлений деятельности государств. Практически все технологически развитые страны мира стремятся решить указанную проблему путем реформирования национального законодательства, расширения зоны ответственности или участия государственных структур и отдельных организаций. По нашему мнению, борьба с деструктивной информацией должна стать общей задачей для государственных органов, общественных организаций и гражданского общества, при этом средства и ресурсы противостояния указанной угрозе в зависимости от субъекта, их применяющего, должны быть максимально разнообразны. Некоторые из них (техника применения и ключевые векторы атак в целях противостояния указанным рискам и угрозам) были приведены в этом учебном пособии.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативные правовые акты

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных законами о поправках к Конституции Российской Федерации от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 14.03.2020 № 1-ФКЗ; с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_28399 (дата обращения: 20.04.2023).
2. Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» (ред. от 29.12.2022) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_1511 (дата обращения: 20.04.2023).
3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 29.12.2022) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 20.04.2023).
4. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (ред. от 29.12.2022) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_108808 (дата обращения: 20.04.2023).
5. Федеральный закон от 30 декабря 2020 г. № 530-ФЗ «О внесении изменений в Федеральный закон „Об информации, информационных технологиях и о защите информации“» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_372700 (дата обращения: 20.04.2023).
6. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_216363 (дата обращения: 20.04.2023). – Режим доступа: по написанию.
7. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_389271 (дата обращения: 20.04.2023).
8. Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе „Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распро-

странение которой в Российской Федерации запрещено» (ред. от 24.12.2022) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_137077 (дата обращения: 20.04.2023).

9. Приказ Роскомнадзора, МВД России, Роспотребнадзора, ФНС России от 18 мая 2017 г. № 84/292/351/ММВ-7-2/461 «Об утверждении Критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, Федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети Интернет, а также сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие запрещенную информацию, в единую автоматизированную информационную систему „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» // Официальный интернет-портал правовой информации. – URL: <http://publication.pravo.gov.ru/File/GetFile/0001201706290015?type=pdf> (дата обращения: 20.04.2023).

Непериодические издания

10. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд., перераб. и доп. – М. : РИОР : Инфра-М, 2022. – 336 с.

11. Бирюкова, Т. А. Комментарий к Федеральному закону от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (постатейный) / Т. А. Бирюкова, Ю. В. Егоров, Н. А. Захарова [и др.] ; под ред. Н. Н. Ковалевой // НПП «Гарант-сервис». – 2013. – URL: <https://base.garant.ru/57622377> (дата обращения: 20.04.2023). – Режим доступа: заказ через систему «Гарант».

12. Бухарин, С. Н. Методы и технологии информационных войн : монография / С. Н. Бухарин, В. В. Цыганов. – М. : Академический проект, 2020. – 382 с.

13. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. – 3-е изд., перераб. и доп. – М. : Юрайт, 2022. – 161 с.

14. Информационное общество в Российской Федерации, 2020 г. : статистический сборник // Росстат ; Национальный исследовательский университет «Высшая школа экономики». – М. : НИУ ВШЭ, 2020. – URL: <https://rosstat.gov.ru/storage/mediabank/lqv3ToRk/info-ob2020.pdf> (дата обращения: 20.04.2023).

15. Леонтьев, В. П. Социальные сети: ВКонтакте, Facebook и другие... / В. П. Леонтьев. – М. : ОЛМА Медиа Групп, 2012. – 256 с.
16. Макаров, С. Прекрасный, опасный, кибербезопасный мир: Все, что важно знать детям и взрослым о безопасности в интернете / С. Макаров. – М. : [б. и.], 2022. – 568 с. – URL: https://www.company.rt.ru/social/book_cybersecurity/files/_SMakarov_fullBook_light.pdf (дата обращения: 20.04.2023).
17. Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете : [учебно-методическое пособие] / Г. У. Солдатова, С. В. Чигарькова, А. А. Дренева [и др.]. – М. : Когито-Центр, 2019. – 176 с.
18. Профилактика терроризма и экстремизма в молодежной среде / [М. А. Кочубей и др. ; под общ. ред. А. П. Новикова]. – СПб. : Русь, 2018. – 96 с.
19. Радаев, В. В. Миллениалы: Как меняется российское общество / В. В. Радаев. – М. : Издательский дом Высшей школы экономики, 2019. – 224 с.
20. Цифровая экономика: Концептуальные основы правового регулирования бизнеса в России : монография / отв. ред. В. А. Лаптев, О. А. Тарасенко. – М. : Проспект, 2021. – 488 с.

Научные статьи

21. Васкэ, Е. В. Психолого-правовой анализ деструктивных проявлений в сети Интернет / Е. В. Васкэ, О. И. Горюнова // Вестник Нижегородского университета имени Н.И. Лобачевского. – 2018. – № 6. – С. 104–110.
22. Гарагашева, Е. П. Роль телеграм-каналов в пропаганде самоубийства / Е. П. Гарагашева, О. В. Молина, О. В. Тальчук // Университетская медицина Урала. – 2021. – Т. 7. – № 2 (25). – С. 44–45.
23. Мосечкин, И. Н. Виктимологические аспекты противодействия вооруженным нападениям на учебные заведения (school-shooting) / И. Н. Мосечкин // Виктимология. – 2019. – № 1 (19). – С. 46–53.
24. Суховская, Д. Н. Социологическое исследование поведенческой моды поколения Z: зумеры и практики филантропии / Д. Н. Суховская // Вестник Томского государственного университета. Серия: Философия. Социология. Политология. – 2022. – № 66. – С. 160–178.
25. Суходолов, А. П. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Телеграм» в распространении наркотиков / А. П. Суходолов, А. М. Бычкова // Всероссийский криминологический журнал. – 2019. – Т. 13. – № 1. – С. 5–17.
26. Тазин, И. И. Правовое обеспечение информационно-психологической безопасности несовершеннолетних / И. И. Тазин // Вестник Томского государственного педагогического университета. – 2012. – № 6 (121). – С. 220–225.

Электронные источники

27. Академик : сайт. – URL: <https://dic.academic.ru> (дата обращения: 20.04.2023).
28. Альянс по защите детей в цифровой среде : сайт. – URL: <https://internetforkids.ru> (дата обращения: 20.04.2023).
29. Всероссийский центр общественного мнения (ВЦИОМ) : сайт. – URL: <https://wciom.ru> (дата обращения: 20.04.2023).
30. Лига безопасного интернета : сайт. – URL: <https://ligainternet.ru> (дата обращения: 20.04.2023).
31. Министерство внутренних дел Российской Федерации : сайт. – URL: <https://мвд.рф> (дата обращения: 20.04.2023).
32. Научная электронная библиотека eLIBRARY.RU : сайт. – URL: <https://elibrary.ru> (дата обращения: 20.04.2023).
33. НПП «Гарант-сервис» : сайт. – URL: <https://garant.ru> (дата обращения: 20.04.2023).
34. О Viber // Viber : сайт. – URL: <https://www.viber.com/ru/about> (дата обращения: 20.04.2023).
35. О WhatsApp // WhatsApp : сайт. – URL: <https://www.whatsapp.com/about> (дата обращения: 20.04.2023).
36. О нас // ВКонтакте : сайт. – URL: <https://vk.com/about> (дата обращения: 19.04.2023).
37. Общественный уполномоченный по защите семьи : сайт. – URL: <https://ouzs.ru> (дата обращения: 19.04.2023).
38. Портал детской безопасности МЧС России «Спас-Экстрим» : сайт. – URL: <https://spas-extreme.mchs.gov.ru> (дата обращения: 20.04.2023).
39. СПС «КонсультантПлюс» : сайт. – URL: <https://www.consultant.ru> (дата обращения: 20.04.2023).
40. Федеральная служба государственной статистики : сайт. – URL: <https://rosstat.gov.ru> (дата обращения: 20.04.2023).
41. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций : сайт. – URL: <https://rkn.gov.ru> (дата обращения: 20.04.2023).
42. Цифровая библиотека IPRsmart (IPRsmart One) : сайт. – URL: <https://www.iprbookshop.ru> (дата обращения: 20.04.2023).
43. Что такое «Одноклассники»? // Проект «Одноклассники» : сайт. – URL: <https://insideok.ru/info> (дата обращения: 19.04.2023).
44. About YouTube : сайт. – URL: <https://about.youtube> (дата обращения: 20.04.2023).
45. Brand Analytics : сайт. – URL: <https://br-analytics.ru> (дата обращения: 20.04.2023).
46. Daily Digital Digest : сайт. – URL: <https://3dnews.ru> (дата обращения: 20.04.2023).

- 
- 
47. DataReportal : сайт. – URL: <https://datareportal.com> (дата обращения: 20.04.2023).
 48. Google Книги : сайт. – URL: <https://books.google.com> (дата обращения: 20.04.2023).
 49. Mediascope : сайт. – URL: <https://mediascope.net> (дата обращения: 20.04.2023).
 50. MessengerPeople : сайт. – URL: <https://www.messengerpeople.com> (дата обращения: 20.04.2023).
 51. NapoleonCat : сайт. – URL: <https://napoleoncat.com> (дата обращения: 20.04.2023).
 52. Statista : сайт. – URL: <https://www.statista.com> (дата обращения: 20.04.2023).
 53. Telegram FAQ // Telegram : сайт. – URL: <https://telegram.org/faq?setln=ru> (дата обращения: 20.04.2023).
 54. The Guardian : сайт. – URL: <https://www.theguardian.com> (дата обращения: 20.04.2023).
 55. We Are Social : сайт. – URL: <https://wearesocial.com> (дата обращения: 20.04.2023).



Учебное издание

Цимбал Виталий Николаевич,
кандидат юридических наук

Толстых Марина Юрьевна,
кандидат технических наук

ПРОТИВОДЕЙСТВИЕ ДЕСТРУКТИВНОМУ КОНТЕНТУ В СЕТИ ИНТЕРНЕТ



Корректор *Титова В. П.*
Компьютерная верстка *Гридчина Т. А.*

Формат 210×210 мм.

Усл. печ. л. 4,62.

Подписано в печать 28.04.2023. Заказ № 337.

Тираж 25 экз.

Отпечатано в Полиграфическом центре
Московского университета МВД России имени В.Я. Кикотя
<https://мосу.мвд.пф>, e-mail: support_mosu@mvd.ru