

Дата поступления рукописи в редакцию: 10.07.2026 г.

DOI: 10.24412/2076-1503-2026-8-849-853

Дата принятия рукописи в печать: 02.08.2026 г.

ОРЕШНИКОВА Ксения Сергеевна,
преподаватель кафедры публичного права, ФГАОУ ВО
«Санкт-Петербургский государственный университет
аэрокосмического приборостроения»,
e-mail: oreshnikova.ksenia@guap.ru

КИБЕРБУЛЛИНГ КАК ПРОБЛЕМА СОВРЕМЕННОГО ОБЩЕСТВА: ПРАВОВЫЕ И СОЦИАЛЬНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ

Аннотация. В статье исследуется феномен кибербуллинга – систематической травли в цифровой среде, приобретающей в условиях всеобщей информатизации массовый характер. Цель исследования – определить правовые и социальные механизмы противодействия кибербуллингу с учётом российского и зарубежного опыта. Для достижения цели проанализированы психологические предпосылки агрессивного онлайн-поведения (эффект онлайн-растормаживания, «тёмная тетрада» личности), рассмотрены резонансные случаи (Аманда Тодд, Рина Паленкова), показана связь кибербуллинга со скулшутингом. Особое внимание уделено нормативному регулированию: проанализированы положения Конституции РФ, Уголовного кодекса РФ, Кодекса РФ об административных правонарушениях, а также Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона № 152-ФЗ «О персональных данных». Выявлены пробелы в законодательстве, в частности отсутствие специальных составов правонарушений и механизмов оперативного реагирования. Обоснована необходимость введения обязательной идентификации пользователей при регистрации на социальных платформах, создания цифрового реестра нарушителей и усиления ответственности интернет-площадок. Практическая значимость исследования заключается в возможности использования его выводов при совершенствовании информационного и административного законодательства, а также в разработке профилактических программ. Статья предлагает комплекс мер, включающих правовые, организационные и воспитательные инструменты.

Ключевые слова: кибербуллинг, цифровая травля, анонимность, онлайн-растормаживание, тёмная тетрада, скулшутинг, правовое регулирование, идентификация пользователей, ответственность интернет-платформ.

ORESHNIKOVA Ksenia Sergeevna,
Lecturer at the Department of Public Law, Saint-Petersburg State
University of Aerospace Instrumentation

CYBERBULLYING AS A PROBLEM OF MODERN SOCIETY: LEGAL AND SOCIAL ASPECTS OF COUNTERACTION

Annotation. The article examines the phenomenon of cyberbullying – systematic harassment in the digital environment, which has become widespread in the context of universal informatisation. The purpose of the study is to identify legal and social mechanisms for counteracting cyberbullying, taking into account Russian and foreign experience. To achieve this goal, the psychological prerequisites for aggressive online behaviour (online disinhibition effect, «dark tetrad» of personality) are analysed, resonant cases (Amanda Todd, Rina Palenkova) are considered, and the connection between cyberbullying and school shooting is shown. Special attention is paid to normative regulation: the provisions of the Constitution of the Russian Federation, the Criminal Code of the Russian Federation, the Code of Administrative Offences of the Russian Federation, as well as Federal Law No. 149-FZ «On Information, Information Technologies and Protection of Information» and Federal Law No. 152-FZ «On Personal Data» are analysed. Gaps in legislation are identified, in particular the absence of special offences and mechanisms for prompt response. The necessity of introducing mandatory user identification during registration on social platforms, creating a digital register of

violators, and strengthening the responsibility of Internet platforms is substantiated. The practical significance of the study lies in the possibility of using its conclusions to improve information and administrative legislation, as well as in the development of preventive programmes. The article proposes a set of measures including legal, organisational and educational instruments.

Key words: *cyberbullying, digital harassment, anonymity, online disinhibition, dark tetrad, school shooting, legal regulation, user identification, platform responsibility.*

Введение

В эпоху цифровой трансформации интернет из технического инструмента превратился в среду обитания значительной части человечества. По данным Международного союза электросвязи, в 2025 году число пользователей сети превысило 5,5 млрд, причём более 60 % из них активно используют социальные сети и мессенджеры [11]. Однако наряду с неоспоримыми преимуществами цифровое пространство породило новые формы девиантного поведения, среди которых особое место занимает кибербуллинг – систематическая травля, унижение и преследование человека с использованием электронных средств связи.

Первоначально интернет воспринимался как пространство свободы и анонимности, что нашло отражение в известной метафоре Питера Штейнера «в интернете никто не знает, что ты собака». Однако именно анонимность стала мощным триггером агрессивных проявлений. Как справедливо отмечает И.В. Никулина, кибербуллинг представляет собой родовое понятие по отношению к троллингу, киберсталкингу, клевете и другим формам цифровой агрессии [6]. В отличие от традиционного школьного буллинга, ограниченного территорией учебного заведения, кибербуллинг не имеет пространственных и временных границ, вторгается в личное пространство жертвы и создаёт ощущение тотальной незащищённости.

Особую тревогу вызывает связь кибербуллинга с тяжкими преступлениями, включая скулшутинг – вооружённые нападения на образовательные учреждения. Исследования показывают, что большинство нападавших ранее сами подвергались травле, в том числе цифровой [1]. Таким образом, противодействие кибербуллингу выходит за рамки сугубо социальной проблемы и становится важной государственной задачей, требующей адекватного правового и организационного ответа.

Цель настоящей работы – на основе комплексного анализа психологических, социальных и правовых аспектов кибербуллинга разработать рекомендации по совершенствованию нормативного регулирования и практических мер противодействия. Для достижения поставленной цели решаются следующие задачи: 1) раскрыть сущность и основные формы кибербуллинга; 2) выявить психологические механизмы, способствующие агрессивному поведению в сети; 3) проанализировать

российское и зарубежное законодательство в данной сфере; 4) предложить конкретные изменения в правовом регулировании и организационные меры.

Материалы и методы исследований

В качестве нормативной основы исследования использованы: Конституция Российской Федерации (ст. 2, 18, 23, 24, 29, 46); Уголовный кодекс РФ (ст. 128.1, 130, 137, 151, 319); Кодекс РФ об административных правонарушениях (ст. 5.61 – оскорбление, ст. 13.11 – нарушение законодательства о персональных данных); Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; а также подзаконные акты, регулирующие деятельность интернет-площадок (например, Правила регистрации на портале «Госуслуги» и требования к идентификации пользователей).

В качестве эмпирического материала привлечены статистические данные о распространённости кибербуллинга (исследования Минцифры РФ, данные ВЦИОМ), а также описания резонансных случаев, получивших широкое освещение в средствах массовой информации и научных публикациях.

Методологическую основу составили: формально-юридический метод (анализ норм законодательства); сравнительно-правовой метод (сопоставление российского и зарубежного регулирования, в частности опыта Китая, ЕС и США); системный анализ (рассмотрение явления во взаимосвязи психологических, социальных и правовых факторов); а также метод теоретического моделирования (при разработке предложений по совершенствованию законодательства). Такое сочетание методов позволило не только описать феномен кибербуллинга, но и сформулировать практически реализуемые пути его преодоления.

Результаты и обсуждения

1. Понятие, формы и психологические механизмы кибербуллинга

Кибербуллинг представляет собой умышленные агрессивные действия, систематически совершаемые в отношении лица (группы лиц) с использованием электронных средств коммуникации. К наиболее распространённым формам относятся: троллинг (провокационное поведение с це-

лью вызвать негативные эмоции), киберсталкинг (навязчивое преследование), разглашение конфиденциальной информации (доксинг), создание унизительных материалов (демотиваторы, мемы), а также угрозы и оскорбления в комментариях и личных сообщениях [6].

Основную роль в формировании кибербуллинга играет феномен онлайн-растормаживания, описанный Дж. Суллером в 2004 г. Исследователь выделил несколько факторов: анонимность, отсутствие невербальных сигналов, асинхронность коммуникации, диссоциация личности (восприятие виртуального «я» как отдельного от реального). В совокупности эти факторы ослабляют внутренние психологические барьеры, снижают эмпатию и ответственность за свои действия [7]. Позднее У. Филлипс и Э. Бакелс связали троллинговое поведение с «тёмной тетradой» личности (нарциссизм, макиавеллизм, психопатия, садизм), причём наиболее сильная корреляция выявлена именно с садизмом [8]. Это означает, что часть агрессоров осознанно получает удовольствие от причинения страданий, что многократно усиливает общественную опасность явления.

В исследовании В.Л. Назарова, Н.В. Авербуха и А.В. Буйначевой обосновывается принципиальная значимость типологического разграничения форм кибербуллинга для понимания его природы. Авторы проводят разграничение между внутришкольным кибербуллингом, при котором участники конфликта принадлежат к одному коллективу, и внешкольным, предполагающим столкновение людей, не связанных реальным знакомством. Это разграничение не является формальным: в первом случае агрессия в цифровой среде выступает продолжением уже сложившихся межличностных отношений и воспроизводит их внутреннюю динамику, тогда как во втором речь идет о качественно иной социальной конфигурации, лишенной предшествующего контекста реального взаимодействия [5].

2. Социальные последствия: от личной трагедии до массовых преступлений

Статистика ВЦИОМ за 2024 г. свидетельствует, что с кибербуллингом сталкивались 42 % опрошенных российских подростков, причём у 12 % травля носила систематический характер и продолжалась более полугода [10]. Негативные последствия включают депрессию, тревожные расстройства, суицидальные мысли и поведение. А.М. Басханов и К.П. Грицианова обращают внимание на оценку данной проблемы профессиональным сообществом, ссылаясь на результаты опроса, проведенного Центром исследований киберзапугивания. Согласно этим данным, 94 % сотрудников школьных служб и 82 % сотрудников

полиции квалифицируют инциденты киберзапугивания как серьезные и участвовавшие в последнее время [2].

Драматичным подтверждением выступает история канадской школьницы Аманды Тодд (2012 г.), которая стала жертвой шантажа и последующей многолетней травли, приведшей к самоубийству. Выяснилось, что преступник действовал системно, вовлекая десятки несовершеннолетних [3]. В России резонанс вызвала гибель Рины Паленковой (2015 г.), после смерти которой её страница в соцсети стала объектом массового глумления, распространялись фотографии с места трагедии, публиковались личные данные семьи. Мать погибшей отмечала, что для многих это была «мода» и форма развлечения, тогда как для семьи – невосполнимая утрата [12].

Ещё более опасным последствием является скулшутинг. Как показал анализ случаев в Керчи (2018), Казани (2021) и Перми (2021), нападавшие ранее подвергались буллингу в коллективах и в сети. Исследователь Р.Г. Ардашев подчёркивает, что накопленные обида и отчаяние со временем перерастают в стремление к мести, что делает кибербуллинг не только самостоятельным деликтом, но и предпосылкой тяжких преступлений [1].

3. Правовое регулирование в Российской Федерации: состояние и пробелы

Действующее российское законодательство содержит разрозненные нормы, которые в той или иной степени могут применяться к кибербуллингу. Конституция РФ гарантирует защиту чести и достоинства (ст. 21, 23), право на неприкосновенность частной жизни (ст. 23) и судебную защиту (ст. 46). Уголовный кодекс предусматривает ответственность за клевету (ст. 128.1), оскорбление (ст. 130 – до декриминализации в 2011 г., ныне – административная ответственность), нарушение неприкосновенности частной жизни (ст. 137), доведение до самоубийства (ст. 110) и др. КоАП РФ содержит ст. 5.61 (оскорбление) и ст. 13.11 (нарушение законодательства о персональных данных).

Однако все эти нормы являются общими и не учитывают специфику цифровой среды. Например, для привлечения к ответственности по ст. 5.61 КоАП необходимо установить факт оскорбления в адрес конкретного лица, однако в условиях анонимности и массовых комментариев доказать это крайне сложно. Кроме того, отсутствует специальный состав правонарушения, охватывающий именно систематическое преследование в сети. Закон «Об информации, информационных технологиях и о защите информации» регулирует порядок распространения информации, но не содержит обязанности провайдеров оперативно реагировать на жалобы о травле. Закон «О пер-

сональных данных» защищает персональные сведения, но не распространяется на унижительные высказывания или угрозы, не содержащие персональных данных.

Особую проблему представляет анонимность. Как показывает опыт Китая, где с 2010 г. введена обязательная идентификация по паспорту для всех интернет-сервисов, а с 2025 г. – система обезличенной аутентификации с уникальным виртуальным идентификатором, такой подход существенно снижает количество агрессивных высказываний [9]. В России регистрация на многих платформах по-прежнему допускает использование псевдонимов, что создаёт у пользователей иллюзию безнаказанности.

4. Предложения по совершенствованию правового и организационного противодействия

На основе проведённого анализа представляется целесообразным внедрение следующих мер.

В законодательной сфере:

Дополнить КоАП РФ специальной статьёй, устанавливающей ответственность за систематическое преследование (кибербуллинг) в информационно-телекоммуникационных сетях, с дифференциацией санкций в зависимости от тяжести последствий.

Внести изменения в Федеральный закон № 149-ФЗ, обязав владельцев социальных сетей и мессенджеров оперативно рассматривать жалобы на противоправный контент и блокировать его в течение 24 часов, а также раскрывать данные нарушителей по запросу правоохранительных органов.

Разработать и утвердить Правила идентификации пользователей при регистрации на публичных интернет-платформах, предусматривающие возможность использования электронной подписи или подтверждения личности через портал «Госуслуги». При этом необходимо сохранить право граждан на псевдоним в закрытых сообществах, но с чётким разграничением публичной и приватной коммуникации.

В организационной сфере:

Создать на базе МВД России специализированное подразделение по мониторингу и пресечению кибербуллинга, работающее в режиме 24/7, с возможностью приёма обращений через единый портал.

Ввести обязательное психологическое сопровождение для жертв кибербуллинга, а также программы реабилитации для несовершеннолетних нарушителей.

Активизировать профилактическую работу в образовательных учреждениях: внедрение уроков цифровой грамотности, формирование навыков

безопасного поведения в сети, обучение распознаванию ранних признаков травли.

Предлагаемые меры не должны восприниматься как тотальный контроль, но как необходимый баланс между свободой слова и защитой личности. Как справедливо отмечает В.А. Латынцева, цифровизация требует адекватного правового сопровождения, при котором технология остаётся инструментом реализации публичных интересов, а не заменяет их [4].

Заключение

Кибербуллинг представляет собой сложное междисциплинарное явление, сочетающее психологические, социальные и правовые аспекты. Анонимность и отсутствие прямого контакта создают благоприятную среду для агрессии, а последствия выходят далеко за пределы цифрового пространства, провоцируя суициды и массовые преступления. Действующее российское законодательство содержит лишь фрагментарные нормы, не обеспечивающие эффективной защиты жертв и не позволяющие привлечь нарушителей к ответственности.

Для изменения ситуации необходимо комплексное реформирование законодательства в части введения специальных составов правонарушений, усиления ответственности интернет-платформ, введения обязательной идентификации пользователей, а также создания специализированных организационных структур. Параллельно требуется масштабная профилактическая работа, направленная на воспитание цифровой культуры и правосознания. Только сочетание правовых, организационных и воспитательных мер позволит снизить масштабы кибербуллинга и обеспечить безопасность граждан в цифровой среде.

Список литературы:

- [1] Ардашев Р.Г. Скулшутинг как социальное явление // Гуманитарный вестник. – 2020. – № 3 (82). – С. 22–28. – DOI 10.18698/2306-8477-2020-3-732..
- [2] Басханов А.М., Грицианова К.П. Кибербуллинг – новая угроза обществу // Евразийская адвокатура. – 2024. – № 5 (70). – С. 124–129. – DOI 10.52068/2304-9839_2024_70_5_124..
- [3] История Аманды Тодд: случай кибербуллинга и суицида // Журнал здоровья подростков. – 2013. – Т. 52, № 5. – С. 576–578. – DOI 10.1016/j.jadohealth.2013.01.023..
- [4] Латынцева В.А. Состояние правового регулирования цифровых технологий в государственном управлении // Юридический мир. – 2023. – № 3. – С. 41–46. – DOI 10.18572/1811-1475-2023-3-41-46..

[5] Назаров В.Л., Авербух Н.В., Буйначева А.В. Связь между типом межличностного поведения и стратегиями участников кибербуллинга: жертвы и свидетели // Образование и наука. – 2025. – Т. 27, № 1. – С. 130–167. – DOI 10.17853/1994-5639-2025-1-130-167..

[6] Никулина И.В. Кибербуллинг: понятие, формы и профилактика // Вестник Томского государственного университета. – 2022. – № 479. – С. 125–131. – DOI 10.17223/15617793/479/15..

[7] Сулер Дж. Эффект онлайн-растормаживания // Киберпсихология и поведение. – 2004. – Т. 7, № 3. – С. 321–326. – DOI 10.1089/1094931041291295..

[8] Филлипс У., Бакелс Э. Тёмная тетрада личности и троллинг // Личность и индивидуальные различия. – 2016. – Т. 94. – С. 23–27. – DOI 10.1016/j.paid.2015.11.043..

[9] Чжан Л., Ван Х. Управление интернет-идентичностью в Китае: от регистрации по реальному имени к анонимной аутентификации // Телекоммуникационная политика. – 2025. – Т. 49, № 1. – С. 102–115. – DOI 10.1016/j.telpol.2024.102115..

[10] ВЦИОМ. Подростки в интернете: угрозы и защита. – М.: ВЦИОМ, 2024. – 45 с. – URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/podrostki-v-internete-ugrozy-i-zashchita>.

[11] Международный союз электросвязи. Статистика пользователей интернета в мире, 2025. – Женева : МСЭ, 2025. – 78 с. – URL: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> (дата обращения: 15.05.2026).

[12] Шевчук Я. Интернет-травля: взгляд изнутри // Новая газета. – 2015. – 15 дек. – URL: <https://novayagazeta.ru/articles/2015/12/15/67284-internet-travlya-vzglyad-iznutri>.

References:

[1] Ardashev R.G. Skulshuting as a social phenomenon // Humanitarian Bulletin. – 2020. – № 3 (82). – S. 22-28. – DOI 10.18698/2306-8477-2020-3-732..

[2] Baskhanov A.M., Gritsianova K.P. Cyberbullying is a new threat to society // Eurasian Bar. – 2024. – № 5 (70). – S. 124-129. – DOI 10.52068/

2304-9839_2024_70_5_124..

[3] Amanda Todd's Story: A Case of Cyberbullying and Suicide // Journal of Adolescent Health. – 2013. – Т. 52, NO. 5. – S. 576-578. – DOI 10.1016/j.jadohealth.2013.01.023..

[4] Latyntseva V.A. State of legal regulation of digital technologies in public administration // Legal world. – 2023. – № 3. – S. 41-46. – DOI 10.18572/1811-1475-2023-3-41-46..

[5] Nazarov V.L., Averbukh N.V., Buinacheva A.V. The relationship between the type of interpersonal behavior and the strategies of cyberbullying participants: victims and witnesses // Education and science. – 2025. – Т. 27, NO. 1. – S. 130-167. – DOI 10.17853/1994-5639-2025-1-130-167..

[6] Nikulina I.V. Cyberbullying: concept, forms and prevention // Bulletin of Tomsk State University. – 2022. – № 479. – S. 125-131. – DOI 10.17223/15617793/479/15..

[7] Suler J. Online Disinhibition Effect // Cyberpsychology and Behavior. – 2004. – Т. 7, NO. 3. – S. 321-326. – DOI 10.1089/1094931041291295..

[8] Phillips W., Buckels E. Dark personality tetrad and trolling // Personality and individual differences. – 2016. – Т. 94. – S. 23-27. – DOI 10.1016/j.paid.2015.11.043..

[9] Zhang L, Wang H. Managing Internet Identity in China: From Registration by Real Name to Anonymous Authentication // Telecommunications Policy. – 2025. – Т. 49, NO. 1. – S. 102-115. – DOI 10.1016/j.telpol.2024.102115..

[10] VTSIOM. Teenagers on the Internet: threats and protection. – М.: VTSIOM, 2024. – 45 с. – URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/podrostki-v-internete-ugrozy-i-zashchita>.

[11] International Telecommunication Union. Statistics of Internet users in the world, 2025. – Geneva: ITU, 2025. – 78 p. – URL: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> (access date: 15.05.2026).

[12] Shevchuk Ya. Internet harassment: a look from the inside // Novaya Gazeta. – 2015. – 15 дек. – URL: <https://novayagazeta.ru/articles/2015/12/15/67284-internet-travlya-vzglyad-iznutri>.

