АДМИНИСТРАТИВНОЕ ЗАКОНОДАТЕЛЬСТВО И АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ

Николай Николаевич НОВГОРОДОВ,
ORCID 0009-0006-3012-8736
Санкт-Петербургский университет МВД России (г. Калининград)
инспектор комендантского отделения Калининградского филиала
novgorodovnikolay1972@gmail.com

Научная статья
УДК 342.951:[351.75:004.738.5]

ОБЩЕСТВЕННЫЙ ПОРЯДОК В СЕТИ ИНТЕРНЕТ

КЛЮЧЕВЫЕ СЛОВА. Интернет, информационно-телекоммуникационные технологии, общественный порядок, правонарушение, девиантное поведение, социальные и правовые нормы, взаимодействие, информация, жертва агрессии.

АННОТАЦИЯ. ***Введение****. Интенсивность развития информационно-телекоммуникационных технологий предопределила возникновение новых вызовов безопасности обмена информацией в глобальной сети Интернет. Современные коммуникационные платформы предоставляют пользователям возможность выражать свои мысли и мнения, однако такая свобода нередко оборачивается противоправными явлениями. Актуальность изучения адаптивности правовых норм в контексте обеспечения безопасности граждан в цифровой среде не вызывает сомнений. В статье категория «общественный порядок» применительно к сети Интернет рассматривается как система социальных и правовых норм, исследуются ее структурные элементы: как правовые нормы, обеспечивающие общественный порядок, так и некоторые девиантные проявления в интернет-общении коммуникантов.* ***Методы****. При проведении исследования, результаты которого представлены в настоящей статье, применялись логический, системный, функциональный, системно-структурный, социологический и аксиологический методы.* ***Результаты****. Автор, допуская существование общественного порядка в сети Интернет, выявляет его цели и задачи, формулирует дефиницию этого понятия. Роль государства в обеспечении общественного порядка в сети Интернет определяется как стремление к достижению гармонии между правом граждан на свободный доступ к информации и их безопасностью в цифровой среде.*

ВВЕДЕНИЕ

Интенсивное развитие информационно-телекоммуникационных сетей, в том числе сети Интернет, придало импульс развитию новых технологий, предоставив неограниченные возможности гражданскому обществу в области сетевого взаимодействия с использованием всех инструментов мировой паутины [1, с. 194]. Вместе с тем оно расширило механизм реализации гражданами права на поиск, получение и распространение социальной информации, а также свободы выражения мысли и слова, формирования собственных убеждений и высказывания своего мнения публично.

Однако сегодня Интернет, являющийся общественным пространством, ставящий своей целью удовлетворение основных потребностей коммуникантов (передача-получение информации, для реализации чего необходимо исключение всякой вседозволенности, а также неукоснительное соблюдение правил допустимого сетевого взаимодействия, направленных на обеспечение общественного порядка, уважительного отношения к обществу, государству, его государственным институтам и символам), стал полем для незаконной деятельности [2, с. 31]. Распространение экстремистских материалов, разжигающих расовое неприятие, национальную рознь, пропаганда наркотиков, деструктивные молодежные течения, подталкивающие к членовредительству и суициду, клевета, мошенничество, незаконное распространение персональных данных и сведений о частной жизни, нарушение авторских прав – вот далеко не полный перечень правонарушений, совершаемых злоумышленниками в сети Интернет.

Nikolay N. NOVGORODOV,
ORCID 0009-0006-3012-8736
Saint Petersburg University of the Ministry of the Interior of Russia (Kaliningrad, Russia)
Inspector of the Commandant's Department of the Kaliningrad Branch
novgorodovnikolay1972@gmail.com

PUBLIC ORDER ON THE INTERNET

KEYWORDS. Internet, information and telecommunication technologies, public order, offense, deviant behavior, social and legal norms, interaction, information, victim of aggression.

ANNOTATION. ***Introduction***. *The intensive development of information and telecommunication technologies has predetermined the emergence of new challenges to the security of information exchange on the global Internet. Modern communication platforms provide users with the opportunity to express their thoughts and opinions, but such freedom often turns into illegal phenomena. The relevance of studying the adaptability of legal norms in the context of ensuring the safety of citizens in the digital environment is beyond doubt. In the article, the category of «public order» in relation to the Internet is considered as a system of social and legal norms, its structural elements are examined: both legal norms that ensure public order and some deviant manifestations in the Internet communication of communicants.* ***Methods***. *In conducting the study, the results of which are presented in this article, logical, systemic, functional, systemic-structural, sociological and axiological methods were used.* ***Results***. *The author, admitting the existence of public order on the Internet, identifies its goals and objectives, formulates a definition of this concept. The role of the state in ensuring public order on the Internet is defined as the desire to achieve harmony between the right of citizens to free access to information and their security in the digital environment.*

В целях правового урегулирования поведения людей и пресечения противоправных действий в сети Интернет государством было внесено в действующее законодательство значительное количество изменений и дополнений [3, с. 25]. В рамках проведенного нами исследования были изучены потенциал обеспечения сетевого общественного порядка, его основные задачи и правовая регламентация.

МЕТОДЫ

Методологическую основу исследования составили: логический метод, который использовался как при накоплении и изложении материала, так и при формировании основных целей и выводов; системный метод, с помощью которого общественный порядок рассматривался через взаимодействующие факторы как совокупность или система общественных отношений, социальных и правовых норм; функциональный метод, который способствовал определению и рассмотрению норм права и социальных явлений (выраженных в девиантологических особенностях сетевого взаимодействия); системно-структурный метод, обеспечивший изучение регулирующих элементов в единой системе и иерархическом построении; социологический метод, посредством которого правовая регламентация была исследована через специфику социального интернет-взаимодействия коммуникантов, являющихся субъектами права; аксиологический метод, позволивший определить безопасность граждан в качестве одной из основных целей массового взаимодействия в сети Интернет.

РЕЗУЛЬТАТЫ

В настоящее время рассмотрение понятия «общественный порядок» применительно к сети Интернет приобретает особую актуальность, главным образом в связи с ростом числа противоправных деяний в сфере информационно-телекоммуникационных технологий. В опубликованной МВД России статистике за 2024 год наблюдается сохранение тенденции к увеличению количества таких преступлений (+13,1% по сравнению с показателем 2023 года). Их доля в общем объеме преступности возросла до 40%. Больше всего среди таких преступлений дистанционных мошенничеств и краж. Раскрываемость преступлений, совершенных с использованием сети Интернет, составила 23,2%[1].

Категория «общественный порядок» в действующем российском законодательстве не получила нормативного закрепления, а в научной среде нет единого подхода к определению этого понятия. Например, С.В. Синицина и З.Г. Кушугулова при формулировании дефиниции предлагают разграничивать общественный порядок, то есть «систему общественных отношений с гарантированной политической системой государства неприкосновенностью», и правопорядок – «нравственное состояние общества, обычаев и традиций, норм общественных организаций и др.» [4, с. 18]. Считаем подобное разграничение некорректным, поскольку правовая основа гражданского общества и государства объединяет их усилия, направленные на укрепление общественного порядка, что улучшает регулирование общественных отношений с помощью правовых механизмов. В результате повышается социальный и правовой статус многих граждан, сближаются возможности гражданского общества и государства в нормативном регулировании.

Другое определение дает Н.М. Конин. Он рассматривает общественный порядок как «комплексную совокупность установленных государством правил (норм) жизни и деятельности (поведения) граждан» в обществе, быту и на производ-

[1] Краткая характеристика состояния преступности в Российской Федерации за 2024 год // МВД России: сайт // URL: https://мвд.рф/folder/101762 (дата обращения: 23.03.2024).

стве[1]. Данной дефиниции, по нашему мнению, не достает выраженности специфики общественного порядка, который фактически сводится к совокупности правил, при этом упускается из виду область общественных отношений.

Более точное определение понятия общественного порядка как объекта правового регулирования и охраны сформулировано еще в конце прошлого века выдающимся отечественным ученым профессором Д.Н. Бахрахом: это «система волевых общественных отношений, регулируемая нормами права, морали, правилами общежития и обычаями, возникающими и развивающимися в общественных местах»[2]. Похожую трактовку предлагает П.Н. Шевченко. Общественный порядок – это «система социальных и правовых общественных отношений, возникающих и развивающихся между людьми в общественных местах» [5, с. 40]. В данных дефинициях в большей степени отражается и правовая основа, и социальная сторона общественного порядка, что отвечает потребностям правоохранительных органов, а также открывает возможности использования этих формулировок в законодательстве.

Представляется очевидным, что одной из составных частей общественного порядка является правопорядок, представляющий собой состояние общественных отношений, обеспечиваемое соблюдением закона – урегулированностью социальных связей, выраженной в законности (правовых нормах). То есть правовой порядок складывается на основе отношений, урегулированных правом, устанавливается соблюдением режима законности в обществе и является их результатом. Понятие же общественного порядка гораздо шире, так как важная роль в его обеспечении принадлежит всем правовым нормам, регулирующим социальные отношения в обществе [6, с. 398].

Таким образом, общественный порядок представляет собой совокупность правил и норм, регулирующих поведение людей в общественных местах и обеспечивающих их безопасность, а также уважение к правам и свободам других людей [7, с. 165]. Принимая данное определение, полагаем, что, во-первых, целью общественного порядка является социальное взаимодействие граждан, выраженное в обеспечении спокойной обстановки для их повседневной жизни, нормальных условий труда и отдыха, деятельности предприятий, учреждений, организаций и властных структур. Во-вторых, существует тесная взаимосвязь между общественным порядком и общественным местом: общественный порядок определяет правила поведения людей в таком месте, а оно, в свою очередь, является площадкой для применения этих правил. Соответственно, общественный порядок устанавливает нормы поведения в общественных местах. Данная взаимосвязь общественного порядка и общественных мест является ключевым аспектом создания безопасной и благоприятной среды для жизни и деятельности людей. Уважение к общественному порядку и соблюдение его норм в общественных местах способствует формированию комфортной и дружественной атмосферы для всех участников общественных отношений. И наоборот, его нарушение снижает качество жизни граждан, вызывая у них чувство незащищенности [8, с. 223].

Необходимость защиты общественного порядка не только в реальном, но и в виртуальном пространстве обусловила потребность в доктринальном определении соответствующего явления. Обеспечение режима общественного порядка в сети Интернет гарантировано нормами как административного[3], так и уголовного[4] законодательства. Действительно, непрерывность информационных потоков предопределяет особенности общения и информационного взаимодействия в межличностных отношениях в виртуальном мире, что нередко приводит к девиантному поведению в интернет-пространстве, где граница между социальными и правовыми нормами очень тонка [9, с. 78]. Полагаем, что общественный порядок в Интернете должен регулироваться не только правовыми, но и социальными нормами, которые быстрее реагируют на стремительные изменения, происходящие в общественной жизни. Иллюстрацией тому могут служить нижеприведенные примеры присущей интернет-среде «девиантной активности», нарушающей режим общественного порядка в глобальной сети [10].

1. Воздействие на потенциальных жертв с целью их обмана для последующего хищения их денег, иного имущества, персональных данных и т.д. Общее название такого явления – ***скамерство*** (от англ. scam – мошенничество, афера).

30-летняя жительница Краснодара, увидев на сайте бесплатных объявлений заметку о продаже самоката, решила его приобрести. После длительной переписки с продавцом в мобильном мессенджере она перевела мошеннику 8000 рублей, но доставки товара так и не дождалась. В другом случае 38-летний житель Красноармейского района Волгограда разместил на торговой площадке в сети Интернет объявление о продаже электрического счетчика. Спустя несколько часов ему пришло сообщение с предложением купить у него этот товар. В ходе переписки со злоумышленником он получил ссылку на подставной сайт, на котором указал реквизиты, а также CVV-код банковской карты. Выполнив все условия, мужчина обнаружил списание со своего счета более 6000 рублей[5].

Исследуя скамерство как разновидность сетевого обмана, О.А. Толпыгина и А.Ю. Мохвин предполагают, что обязательным условием успешной

[1] Конин Н.М. Административное право России в вопросах и ответах: Учебное пособие. М.: Проспект, 2010. С. 72-73.
[2] Административная ответственность граждан за правонарушения / Под ред. Д.Н. Бахраха. Пермь, 1978. С. 40.
[3] Например, нормами, закрепленными в ч. 3 ст. 20.1, ст.ст. 20.3, 20.3.1, 20.3.2, 20.3.3, 20.3.4, 5.61, 5.61.1, 5.62, 13.15, 13.48 КоАП РФ, и др.
[4] Например, нормами, закрепленными в ст.ст. 110, 110.1, 110.2, 111, 112, 115, 116, 117, 119, 126, 127, 127.2, 128.1, 133, 150 УК РФ, и др.
[5] Плешков А. Скам на барахолке. Дистанционное мошенничество на торговых площадках глазами аналитика SOC // BIS Journal. 2020. № 4 (39). 18.12.2020 // URL: https://ib-bank.ru/bisjournal/post/1473.

реализации подобного рода мошенничества является «эмоциональная привязанность» жертвы к скамеру [11, с. 293]. Способом реализации обмана может быть рассылка вредоносного программного обеспечения, которое устанавливается на устройство жертвы без ее ведома. Такое явление получило название ***фишинг*** (от англ. fishing – рыбная ловля). Фишинговые атаки могут осуществляться в различных формах:

- *почтовый фишинг* – массовая отправка электронных писем на все имеющиеся у мошенников адреса электронной почты, в социальные сети;

- *целевой фишинг* – отправка вредоносных персонализированных электронных писем конкретным лицам либо в специально подобранные компании;

- *уэйлинг* (от англ. whaling – китобойный промысел) – использование давления на высокопоставленных руководителей для получения конфиденциальной информации;

- *SMS-фишинг (смишинг)* – проведение фишинговой атаки с помощью текстовых сообщений;

- *голосовой фишинг* – передача автоматического голосового сообщения;

- *SEO-мошенничество* (от англ. Search Engine Optimization – поисковая оптимизация) – отправка писем сотрудникам якобы от лица руководителя;

- *клон-фишинг* – создание вредоносных копий сообщений от легитимного отправителя;

- *Evil Twin фишинг* (англ. Evil Twin – злой двойник) – создание копии легитимной сети Wi-Fi;

- *фишинг в социальных сетях* – создание фальшивых аккаунтов, якобы принадлежащих известным компаниям;

- *фишинг в поисковых системах* – создание фейковых веб-сайтов в легитимных поисковых системах;

- *фарминг* (от англ. pharming – занятие сельским хозяйством, животноводством) – скрытая переадресация потенциальной жертвы на ложный IP-адрес;

- *кетфишинг* (от англ. catfish – сом, дословно – ловля сома) – это вид обмана, при котором злоумышленник не взламывает аккаунт, а создает ложный и распространяет через него негативную провокационную информацию.

Главное различие между вариантами фишинга заключается в охвате аудитории. Фишинговые письма, как правило, рассылаются большой группе людей в надежде, что какая-то часть из них попадется на уловку. Примером крупного проявления фишинга в социальных сетях стало мошенничество, организованное в отношении пользователей сайта, предназначенного для бронирования жилья с помощью Интернета. Злоумышленники рассылали через популярный мессенджер сообщения, посредством которых получали доступ к аккаунтам пользователей. Завладев информацией о бронированиях, преступники предлагали оплатить проживание по счетам, которые были поддельными[1].

Более точечно целеориентирована такая форма интернет-мошенничества, как китфишинг. Она предназначается для организации атак на руководителей высшего звена и высокопоставленных служащих организаций. В данном случае злоумышленник заранее тщательно изучает свою жертву, собирая информацию о ее роли, обязанностях и привычках, чтобы адаптировать атаку для получения максимального эффекта. В качестве примера китфишинга можно привести атаку на сотрудников «Microsoft»: злоумышленники, похищая учетные данные пользовательских аккаунтов, получали доступ к привязанным банковским картам[2].

Следует согласиться с точкой зрения М.М. Моргуновой о том, что «обман является движущей силой механизма фишинга» [12, с. 139]. При этом незаконное получение персональных данных может происходить как через самого их владельца, так и через посредника (лицо, которое в силу должностных обязанностей имеет доступ к чужим сведениям).

2. Информационное воздействие на аудиторию при помощи распространения в постах, комментариях, отзывах и т.д. фейковых суждений «независимых специалистов или экспертов», формирующих «нужное» общественное мнение. Такое явление получило название ***астротурфинг*** (происходит от названия американской компании «AstroTurf» – бренда синтетических ковровых покрытий, созданных, чтобы имитировать натуральную траву). Астротурфингом для имитации общественной поддержки пользовалась, например, команда избирательного штаба кандидата в президенты США Дж. Маккейна, подобного рода технологии применяли в маркетинге торговая сеть «Wal-Mart» и компания «Sony»[3].

По мнению П.Л. Лихтера, исследующего технологии астротурфинга, необходимо «отграничивать правомерные маркетинговые практики от противоправных деяний по искажению информации о товаре или компании как при помощи финансирования мероприятий по влиянию на общественное мнение с привлечением крупных научных центров, так и деятельности физических лиц по продвижению положительных или негативных отзывов в сети Интернет о товарах, работах, услугах определенных компаний». Для отграничения технологий астротурфинга от добросовестного поведения на рынке П.Л. Лихтер предлагает выявлять следующие признаки: «создание подставных аккаунтов; сфабрикованная массовая рассылка; использование ботов для «накручивания» лайков, рассылки по чатам и каналам; платный характер публикации отзыва или мнения; использование методов, вызывающих конфликты, страх» и т.п. [13, с. 131-133].

[1] Виды фишинговых атак // Unisender. Словарь маркетолога: сайт // URL: https://www.unisender.com/ru/glossary/chto-takoe-fishing-i-kak-ot-nego-zashchititsya/#anchor-1.

[2] Group-IB обнаружила фишинг-киты, нацеленные на 260 брендов // Хабр: сайт. 07.04.2021 // URL: https://habr.com/ru/companies/F6/articles/551236/.

[3] Астротурфинг управления общественным мнением // URL: https://vk.com/@anad1-astroturfing-upravleniya-obschestvennym-mneniem).

Мы согласны с тем, что с помощью астротурфинга достигаются не позитивные политические, идеологические, экономические цели, в том числе в маркетинге и торговле, а цели противоправного содержания. Так, Г.И. Авцинова [14, с. 31-32] и К.С. Князев [15] в своих работах приводят сведения о возможностях манипулирования с помощью инструментов астротурфинга мнением людей в сети Интернет с целью инициирования их деструктивной общественной активности, такой как гражданское неповиновение, протестные акции, несанкционированные митинги и т.д.

3. Воздействие на потенциальных жертв с целью издевательства, травли, систематического унижения и т.д. Общее название подобных действий – ***кибербуллинг*** (от англ. bullying – запугивание, издевательство). Это «вид травли, преднамеренные агрессивные действия, осуществляемые индивидом или группой людей на протяжении некоторого времени с помощью современных средств связи и интернет-технологий» [16, с. 175]. Основными характеристиками кибербуллинга являются: умышленность, регулярность, неравенство сил, широкий круг участников, негативное психологическое воздействие ситуации на всех вовлеченных субъектов, отсутствие видимости эмоциональной реакции жертвы, возможность круглосуточной травли, независимость от времени, места, статуса жертвы. Кибербуллинг не заканчивается сам по себе. Его особенности заключаются в анонимности и дистанцированности агрессора (он чувствует себя менее уязвимым). Поводы для кибербуллинга могут быть различными: хобби и увлечения, уровень доходов, принадлежность к какой-либо группе или субкультуре, религиозные убеждения, национальная принадлежность, культурные традиции, политические взгляды, сексуальная ориентация, особенности характера, здоровья или внешности. Например, жительница Сочи, регистрируясь под различными именами, публиковала на странице бывшего молодого человека и страницах его знакомых информацию о его нетрадиционной сексуальной ориентации. Жертва не выдержала травли и решила покончить жизнь самоубийством. Свои намерения молодой человек исполнил: он был найден повесившимся[1].

В настоящее время данный вид киберагрессии представляет собой острую социальную проблему – «чуму цифровой цивилизации»[2], его масштабы катастрофически велики. К числу частных случаев проявления кибербуллинга относят:

- *хейтинг* (от англ. hating – ненавидеть) – вид буллинга, при котором публикуются повторяющиеся оскорбительные необъективные комментарии с целью унижения или запугивания жертвы. Он является, по сути, полноценной травлей. Здесь также стоит упомянуть такой термин, как *«хейт-спич»* (от англ. hate – ненависть, speech – речь). Это язык ненависти и вражды, проявляющейся, как правило, в форме межнациональной розни, ксенофобии, расизма, сексизма или гомофобии. При этом стоит отличать хейт от здоровой критики: задача интернет-хейтеров состоит в том, чтобы словесно дискредитировать кого-то или что-то, при этом унизив человека или испортив мнение, например, о продукте. Примером хейтинга служит история с болеющей онкологическим заболеванием актрисой. Хейтеры не поверили и обвинили ее во лжи[3];

- *троллинг* (от англ. trolling – ловля рыбы на блесну) – вид буллинга, социальная провокация, издевательство над жертвой ради забавы. Сюда также можно отнести грубые, оскорбительные комментарии, иррациональную критику, фотокарикатуры («фотожабы»), слухи, сплетни, откровенные оскорбления. В настоящее время распространен троллинг девушек, находящихся в затруднительном положении, как наиболее уязвимой категории пользователей глобальной сети. Сообщества мам, находящихся в декрете, ресурсы, посвященные женским увлечениям, проблемам или правам нередко подвергаются атакам провокаторов. Дело в том, что временно находящаяся в зависимом положении либо попавшая в сложную ситуацию женщина зачастую истощена морально, а потому становится беззащитной перед атаками «троллей»[4]. Разновидностью троллинга является *грифинг* (от англ. жаргонизма griefer, производного от grief – горе). Это манера участия в компьютерной игре, предполагающая умышленное создание помех другим игрокам, поведение, «портящее» игровой процесс в сетевых онлайн-играх. С виртуальными играми связан и *вайп* (от англ. wipe – стирать) – необратимое удаление всей информации о персонаже и даже полное обнуление игрового мира. Например, проявление грифинга в популярной компьютерной онлайн-игре «Майнкрафт» выражается в игровом вандализме: в разрушении чужих построек, хранилищ предметов, внесении в них вредных или несанкционированных изменений, лишающих пользователей полученного ими игрового имущества. Гриферство в «Майнкрафт» стало массовым явлением. Формируются даже «профессиональные» команды гриферов, они стали большой проблемой для администраторов серверов, стремящихся поддерживать игроков-«строителей»[5];

- *фрейпинг* (от англ. fraping – фальсификация) – вид буллинга, при котором злоумышленник получает доступ к аккаунту человека и от его имени публикует негативную информацию или нежелательный контент с целью выставить жертву

[1] Осторожно: кибербуллинг! // Darker. 2025. № 9 // URL: https://darkermagazine.ru/page/ostorozhno-kiberbulling.
[2] Журавель Д., Шкуро А. Кибербуллинг: чума цифровой цивилизации // Vegetarian: сайт. 26.08.2020 // URL: https://vegetarian.ru/articles/kiberbulling-chuma-tsifrovoy-tsivilizatsii.html.
[3] Как Интернет стал питательной средой для ненависти и как с ней бороться // URL: https://vk.com/@knife.media-sdohni-mraz-kak-internet-stal-pitatelnoi-sredoi-dlya-nenavis.
[4] Разновидности и формы киберагрессии // Educators: сайт. 03.03.2021 // URL: https://educators.co.il/raznovidnostiiformy.
[5] Как выглядит грифер в майнкрафте // Своими силами: сайт // URL: https://pk.papa-zil.ru/kak-vyglyadit-grifer-v-maynkrafte.html.

в глупом виде. Пример фрейпинга обнаруживается в нашумевшем скандале, связанном со взломом аккаунта Д.А. Медведева (в то время Председателя Правительства Российской Федерации) в 2014 году, в результате чего на его странице появились сообщения провокационного содержания[1];

- *флейминг* (от англ. flame – огонь, пламя) – «спор ради спора», формат коммуникации в социальных сетях, в чатах и интернет-форумах, представляющий собой бесцельный обмен агрессивными репликами, направленный не на прояснение позиций и достижение консенсуса, а на выплеск эмоций участников;

- *флуд* (от англ. flood – наводнение, поток) – бессмысленные посты, символы и сообщения на площадке коммуницирования, не относящиеся к теме обсуждения общающейся на ней группы пользователей. Флуд может распространяться как отдельными лицами (самым простым и наиболее «безобидным» его проявлением, по нашему мнению, является отправка подряд множества сообщений, которые можно объединить в одно), так и автоматизированной программой (ботом), рассылающим до тысячи сообщений в минуту. Цель – вредительство, реализуемое для того, чтобы исключить или ограничить общение на конкретном сетевом ресурсе;

- *холивар* (от англ. holywar – священная война) – продолжительная и принципиальная эмоционально-категоричная дискуссия (спор) на различных интернет-ресурсах между непримиримыми оппонентами, часто перерастающая в потоки оскорбительных высказываний и клеветы по отношению друг к другу. Одним из наиболее ярких проявлений холивара стала так называемая «война браузеров» «Chrome», «Firefox» и «Opera». В этом споре активно участвуют как обычные пользователи, так и профессиональные программисты. Если для первых дело, скорее, в привычках, удобстве и личных предпочтениях, то вторые приводят серьезные аргументы в пользу предпочитаемого интернет-обозревателя. На форуме «GameDev.ru» спор сторонников «Opera» и «Firefox» начался в 2006 году и продолжается до сих пор[2];

- *диссинг* (от англ. dissing – дразнить, оскорблять) – распространение клеветы, недостоверных, оскорбительных слухов, выставляющих жертву в негативном свете. Например, мать двоих детей С. стала жертвой анонимного автора, который выкладывал в Интернет ложные сведения о ее личной жизни, что привело к разрыву отношений со многими друзьями и знакомыми[3];

- *социальная изоляция (бойкот)* – вид буллинга, предполагающий полное игнорирование жертвы на всех площадках массового коммуницирования и исключение ее из социальной жизни в глобальной сети. Поводом может стать любое несоответствие (нередко – мнимое) бойкотируемого «стандартам» группы общения. Например, одноклассники «удаляют» ученика из общего чата класса, в результате чего он оказывается оторванным от новостей, совместных планов и мероприятий.

4. Навязчивое систематическое взаимодействие с жертвой с целью преследования в киберпространстве. Такое явление получило общее название ***киберсталкинг*** (от англ. stalk – навязчиво преследовать). Возможно не только психологическое давление на жертву, но и противоправное использование чужих личных данных для обогащения. Пример: А. – социально активная девушка. У нее есть аккаунты в различных соцсетях. Личные сообщения и квитанции по платежам приходят на ее основную почту. Секретный вопрос к паролю на почте: имя первой собаки? А. собралась в отпуск. Купила билеты, о чем рассказала во всех социальных сетях. Киберсталкер Б. решил испортить А. отпуск. Он изучил ее ленту и наткнулся на ностальгический пост о собаке Мухтаре. Электронный адрес девушки был указан в соцсети. Б. безуспешно пытался подобрать пароль, потом нажал кнопку «Забыли пароль» и увидел секретный вопрос. Ответ на него ему уже был известен. Первым делом Б. отменил покупку билетов и сохранил себе деловую корреспонденцию и личные фотографии жертвы. Отпуск А. был испорчен, счета оказались заблокированными. А. потеряла деловую переписку и вместе с ней – тайные коммерческие сведения. Другой пример: В. работает на престижной должности и активно пользуется социальными сетями. Киберсталкер следит за сведениями, выкладываемыми В. в сети. Так преследователь узнал несколько историй из жизни В., имена друзей детства и то, что у него есть мама – добрейшей души женщина. Киберсталкер звонит матери В., представляется его коллегой и рассказывает, что В. просил забрать у нее деньги. За ними, мол, заедет курьер, чтобы передать их затем В. Мошенник прибывает под видом курьера и исчезает с крупной суммой денег[4]. К проявлениям киберсталкинга относят следующие виды интернет-агрессии:

- *харассмент* (от англ. harassment – домогательство) – психологическое давление, преследование и домогательства в сети, в том числе пошлые шутки и комментарии с сексуальным подтекстом, предложения сексуального характера, отправка скабрезных фотографий, принуждение жертвы путем шантажа к непристойным действиям, травля и дискриминация по расовому или религиозному признакам. Отметим, что о харассменте, несмотря на его схожесть с другими формами киберагрессии, говорят в более широком понимании – это любое поведение, которое унижает человека, доставляет дискомфорт и нарушает его личные границы: дискриминация, домогательства (включая сексуальные) и злоупотребление вла-

[1] Денисова М. Как не стать жертвой кибербуллинга // The Girl: сайт. 13.03.2019 // URL: https://thegirl.ru/articles/kak-ne-stat-jertvoy-kiberbullinga/?ysclid=ls688mglqn293933607.
[2] Холивар! Opera vs Firefox // URL: https://gamedev.ru/flame/forum/?id=12318.
[3] Терехов В.С. Кибербуллинг: причины, признаки, как справиться // Здоровая семья: сайт. 12.08.2023 // URL: https://zdorovaya-semya.ru/articles/kiberbulling.
[4] Что такое киберсталкинг и как от него защититься // Лаборатория Касперского: сайт // URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-cyberstalking.

стью. Проявлениями интернет-харассмента могут, например, быть: насмешки и оскорбительные комментарии по поводу вероисповедания, обычаев, традиций; унизительные клички, связанные с цветом кожи или расовой принадлежностью; рисунки, письма, репосты в социальных сетях, пропагандирующие расовое неравенство; намеки, шутки, имеющие оскорбительный или сексуальный подтекст; сообщения с угрозами или предложениями вступить в сексуальную связь; оскорбления, связанные с возрастом, социальным статусом, физическими особенностями; публикация в сообщениях оскорбительной символики, элементов одежды и т.д.[1]. В России под харассментом чаще всего подразумевают сексуальное насилие (понуждение к действиям сексуального характера) [17, с. 200];

- *секстинг* (от англ. sex и texting – секс по переписке) – это обмен сообщениями сексуального характера. «Согласно российскому законодательству, – пишет А.Н. Аянян, исследующая девиантные практики в виртуальной среде, – если речь идет об обмене сообщениями сексуального характера между взрослыми дееспособными людьми по обоюдному согласию…, подобного рода пользовательская активность не может быть отнесена к девиантным практикам». Но «если в секстинг взрослыми лицами вовлекаются несовершеннолетние либо лица, не отдающие отчета в своих действиях, либо к подобной практике привлекают с помощью манипуляций и шантажа, либо это носит нежелательный навязчивый характер, например дикпик (рассылка изображений гениталий), то подобного рода пользовательская активность, носит не только девиантный, но в ряде случаев и противоправный характер» [18, с. 29-30]. Так, жертвой секстинга стал Г., которому несовершеннолетняя знакомая присылала огромное количество сообщений интимного содержания, пикантные видео и фото. В половые отношения данные граждане не вступали. Однако на момент переписки девушка не достигла совершеннолетия, что стало основанием для признания действий Г. противоправными. Инициатором переписки он не являлся, тем не менее было возбуждено уголовное дело, мужчину обвинили в совершении преступления, предусмотренного ст. 135 УК РФ «Развратные действия в отношении несовершеннолетней»[2]. Секстинг в современном понимании – «это действия лица или группы лиц, – пишет А.Е. Боргдорф, – в электронно-телекоммуникационной сети, направленные на установление близких, доверительных или же романтических отношений ради получения фотографий интимного характера в целях пересылки и удовлетворения личных сексуальных потребностей» [19, с. 401]. Не углубляясь в моральные аспекты данного явления, считаем, что негативная сторона секстинга заключается в навязчивых вульгарных, непристойных сообщениях, пересылаемых посредством сетей массового взаимодействия;

- *аутинг* (от англ. outing – прогулка, здесь – публичное разоблачение) – разглашение (угроза разглашения) приватной компрометирующей информации о человеке для его дискредитации, обнародование информации о нестандартной гендерной идентичности преследуемого без его согласия. Для описания сути этого явления иногда используют термин «диффамация» (от лат. defamatio – порочить), им обозначают распространение правдивых сведений, которые жертва по различным причинам скрывает от огласки. Широкий общественный резонанс получила история атаки на учительницу из Санкт-Петербурга, в результате которой ее уволили из школы с обвинением в нетрадиционной ориентации. Инициатором «разоблачения» стал И., который собрал досье из найденных в Интернете материалов. Он решил использовать их для борьбы с людьми, недостойными, по его мнению, преподавать[3].

Обобщая вышеизложенное, следует подчеркнуть, что различного вида девиации, проявляющиеся в интернет-пространстве, зарождают в пользователе недоверие, страх, ответную агрессию, понижают коммуникативную заинтересованность, препятствуют удовлетворению основных потребностей коммуникантов, связанных с передачей и получением информации, что подтверждает их существенное негативное влияние на режим общественного порядка в сети Интернет.

Итак, согласно приведенной нами ранее дефиниции общественный порядок регулируется не только нормами права, закрепленными в действующем законодательстве, но и социальными нормами, нарушение которых характеризуется девиантологическими особенностями сетевого взаимодействия коммуникантов. С учетом того, что целью общественного порядка в целом является регулирование социального взаимодействия граждан, предлагаем под целью общественного порядка в сети Интернет понимать обеспечение безопасности обмена информацией и коммуникации. Исходя из этого, под общественным порядком в сети Интернет предлагаем понимать совокупность общественных отношений, охраняемых социальными и правовыми нормами в целях благоприятного и безопасного взаимодействия пользователей, защиты их прав, свобод и законных интересов, складывающихся на всех интернет-ресурсах массового взаимодействия (иными словами, во всех общественных местах Интернета).

ЗАКЛЮЧЕНИЕ

Наряду со стремительным развитием информационно-коммуникационных технологий эволюционируют и формы информационного взаимодействия интернет-пользователей, которые значительное время проводят в виртуальном про-

[1] Кораблёва К. Харассмент – Что Это Такое? // Psylib. Библиотека психологии: сайт. 09.12.2020 // URL: https://psylib.org/kharassment/.
[2] Катаева В. Друг семьи пал жертвой секстинга // Рамблер: сайт. 11.08.2020 // URL: https://woman.rambler.ru/other/44643894-drug-semi-pal-zhertvoy-sekstinga/.
[3] Низеенко Е. Троллинг, аутинг, лайкинг и другие проблемы эпохи соцсетей // LiveInternet: сайт. 29.11.2015 // URL: https://www.liveinternet.ru/users/shadow3dx/post378135524/.

странстве. В связи с этим наблюдаются тенденции к росту количества правонарушений, совершаемых в сети Интернет, а также к появлению в нем новых девиаций, с которыми общество ранее не сталкивалось. Следовательно, объектом административно-правовой охраны в данном случае выступает общественный порядок, складывающийся не только в реальном мире, но и в интернет-пространстве в процессе массового взаимодействия коммуникантов путем получения или передачи информации. С учетом положений ст. 29 Конституции Российской Федерации, гарантирующей информационную свободу и запрещающей пропаганду «социального, расового, национального, религиозного или языкового превосходства», главной задачей государства в сфере информационно-телекоммуникационных технологий является поиск оптимального баланса между правом граждан на информацию и их безопасностью в цифровом пространстве [20, с. 70]. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Голоманчук Э.В., Васильева И.П. Интернет и социальные сети: их плюсы, минусы и последствия в развитии человечества // Модели, системы, сети в экономике, технике, природе и обществе. 2015. № 2 (14). С. 193-200.

2. Алексеева А.П., Ничуговская О.Н. Киберпреступность: основные черты и формы проявления // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2017. № 1. С. 27-34.

3. Алексеева А.П. Перспективы развития уголовного законодательства в киберсфере // Подготовка сотрудников полиции к использованию информационных технологий в борьбе с преступностью. Сборник научных трудов по материалам Всероссийской межвузовской научно-практической конференции. Т. 2. Волгоград: ВА МВД России, 2017. С. 24-31.

4. Синицина С.В., Кушугулова З.Г. Понятие общественный порядок, общественная безопасность, правовой порядок, их анализ, соотношение и определение родового объекта административного правонарушения, предусмотренного ч. 1 ст. 20.25 Кодекса Российской Федерации об административных правонарушениях // Законность и правопорядок в современном обществе. 2014. № 22. С. 16-20.

5. Шевченко П.Н. К вопросу о содержании понятия «общественный порядок» // Вестник Московского университета МВД России. 2012. № 11. С. 37-40.

6. Рощупкина Д.С. Соотношение категорий правопорядка и общественного порядка // Вестник науки. 2024. Т. 2. № 1 (70). С. 396-399.

7. Мелихов А.И., Працко Г.С. Проблемы управления обеспечением коллективной безопасности в классической философии // Модернизация российского общества и образования: новые экономические ориентиры, стратегии управления, вопросы правоприменения и подготовки кадров. Материалы Национальной научной конференции (с международным участием). Таганрог: ТИУиЭ, 2024. С. 165-168.

8. Никоноров Е.А., Никоноров А.А. Понятие общественного места в российском законодательстве // Вестник экономической безопасности. 2018. № 2. С. 222-227.

9. Алексеева А.П. Киберпреступность: насколько реальна угроза // Научно-методический электронный журнал «Концепт». 2017. № Т31. С. 76-80.

10. Шаров А.А. Специфика девиантной активности молодежи в интернет-среде // Ученые записки. Электронный научный журнал Курского государственного университета. 2019. № 3 (51). С. 255-261.

11. Мохвин А.Ю., Толпыгина О.А. Скамерство как разновидность сетевого мошенничества. Коммуникативные стратегии скамеров // Вестник науки. 2019. Т. 3. № 6 (15). С. 291-294.

12. Могунова М.М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник Саратовской государственной юридической академии. 2020. № 4 (135). С. 135-141.

13. Лихтер П.Л. Технологии астротурфинга с точки зрения права // Правовая парадигма. 2020. Т. 19. № 4. С. 131-136.

14. Авцинова Г.И. Астротурфинг как технология организации гражданского неповиновения // Траектории политического развития России: институты, проекты, акторы. Материалы всероссийской научной конференции с международным участием. М.: МПГУ, 2019. С. 31-32.

15. Князев К.С. Астротурфинг и призывы в сети Интернет к участию в общенациональных уличных протестах в Российской Федерации // Гуманитарные, социально-экономические и общественные науки. 2021. № 11-1. С. 48-50.

16. Нахаева А.В. Кибербуллинг: причины, виды и последствия // Психология личности: актуальные исследования: Сборник научных трудов. Магнитогорск: МГТУ им. Г.И. Носова, 2020. С. 174-179.

17. Серебренникова А.В. Харассмент: уголовно-правовое понятие // Проблемы экономики и юридической практики. 2020. Т. 16. № 3. С. 198-201.

18. Аянян А.Н. Девиантные практики в виртуальной среде (на примере секстинга) // Психолого-педагогические модели и технологии развития личности в цифровой среде. Сборник материалов Межвузовской научно-практической конференции. М.: МИП, 2022. С. 28-31.

19. Боргдорф А.Е. Уголовно-правовые аспекты онлайн секстинга и груминга в эпоху цифровой среды // Интеллектуальные ресурсы – региональному развитию. 2022. № 1. С. 399-404.

20. Дизер О.А. Административно-правовая охрана общественного порядка и общественной безопасности в условиях формирования цифрового пространства // Вестник Уфимского юридического института МВД России. 2020. № 3 (89). С. 63-70.

REFERENCES

1. Golomanchuk E.V., Vasil'yeva I.P. Internet i sotsial'nyye seti: ikh plyusy, minusy i posledstviya v razvitii chelovechestva // Modeli, sistemy, seti v ekonomike, tekhnike, prirode i obshchestve. 2015. № 2 (14). S. 193-200.
2. Alekseyeva A.P., Nichugovskaya O.N. Kiberprestupnost': osnovnyye cherty i formy proyavleniya // Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy. 2017. № 1. S. 27-34.
3. Alekseyeva A.P. Perspektivy razvitiya ugolovnogo zakonodatel'stva v kibersfere // Podgotovka sotrudnikov politsii k ispol'zovaniyu informatsionnykh tekhnologiy v bor'be s prestupnost'yu. Sbornik nauchnykh trudov po materialam Vserossiyskoy mezhvuzovskoy nauchno-prakticheskoy konferentsii. T. 2. Volgograd: VA MVD Rossii, 2017. S. 24-31.
4. Sinitsina S.V., Kushugulova Z.G. Ponyatiye obshchestvennyy poryadok, obshchestvennaya bezopasnost', pravovoy poryadok, ikh analiz, sootnosheniye i opredeleniye rodovogo ob"yekta administrativnogo pravonarusheniya, predusmotrennogo ch. 1 st. 20.25 Kodeksa Rossiyskoy Federatsii ob administrativnykh pravonarusheniyakh // Zakonnost' i pravoporyadok v sovremennom obshchestve. 2014. № 22. S. 16-20.
5. Shevchenko P.N. K voprosu o soderzhanii ponyatiya «obshchestvennyy poryadok» // Vestnik Moskovskogo universiteta MVD Rossii. 2012. № 11. S. 37-40.
6. Roshchupkina D.S. Sootnosheniye kategoriy pravoporyadka i obshchestvennogo poryadka // Vestnik nauki. 2024. T. 2. № 1 (70). S. 396-399.
7. Melikhov A.I., Pratsko G.S. Problemy upravleniya obespecheniyem kollektivnoy bezopasnosti v klassicheskoy filosofii // Modernizatsiya rossiyskogo obshchestva i obrazovaniya: novyye ekonomicheskiye oriyentiry, strategii upravleniya, voprosy pravoprimeneniya i podgotovki kadrov. Materialy Natsional'noy nauchnoy konferentsii (s mezhdunarodnym uchastiyem). Taganrog: TIUiE, 2024. S. 165-168.
8. Nikonorov Ye.A., Nikonorov A.A. Ponyatiye obshchestvennogo mesta v rossiyskom zakonodatel'stve // Vestnik ekonomicheskoy bezopasnosti. 2018. № 2. S. 222-227.
9. Alekseyeva A.P. Kiberprestupnost': naskol'ko real'na ugroza // Nauchno-metodicheskiy elektronnyy zhurnal «Kontsept». 2017. № T31. S. 76-80.
10. Sharov A.A. Spetsifika deviantnoy aktivnosti molodezhi v internet-srede // Uchenyye zapiski. Elektronnyy nauchnyy zhurnal Kurskogo gosudarstvennogo universiteta. 2019. № 3 (51). S. 255-261.
11. Mokhvin A.Yu., Tolpygina O.A. Skamerstvo kak raznovidnost' setevogo moshennichestva. Kommunikativnyye strategii skamerov // Vestnik nauki. 2019. T. 3. № 6 (15). S. 291-294.
12. Mogunova M.M. Tekhnologiya osushchestvleniya i pravovaya reglamentatsiya nezakonnogo ovladeniya personal'nymi bankovskimi dannymi (fishing) // Vestnik Saratovskoy gosudarstvennoy yuridicheskoy akademii. 2020. № 4 (135). S. 135-141.
13. Likhter P.L. Tekhnologii astroturfinga s tochki zreniya prava // Pravovaya paradigma. 2020. T. 19. № 4. S. 131-136.
14. Avtsinova G.I. Astroturfing kak tekhnologiya organizatsii grazhdanskogo nepovinoveniya // Trayektorii politicheskogo razvitiya Rossii: instituty, proyekty, aktory. Materialy vserossiyskoy nauchnoy konferentsii s mezhdunarodnym uchastiyem. M.: MPGU, 2019. S. 31-32.
15. Knyazev K.S. Astroturfing i prizyvy v seti Internet k uchastiyu v obshchenatsional'nykh ulichnykh protestakh v Rossiyskoy Federatsii // Gumanitarnyye, sotsial'no-ekonomicheskiye i obshchestvennyye nauki. 2021. № 11-1. S. 48-50.
16. Nakhayeva A.V. Kiberbulling: prichiny, vidy i posledstviya // Psikhologiya lichnosti: aktual'nyye issledovaniya: Sbornik nauchnykh trudov. Magnitogorsk: MGTU im. G.I. Nosova, 2020. S. 174-179.
17. Serebrennikova A.V. Kharassment: ugolovno-pravovoye ponyatiye // Problemy ekonomiki i yuridicheskoy praktiki. 2020. T. 16. № 3. S. 198-201.
18. Ayanyan A.N. Deviantnyye praktiki v virtual'noy srede (na primere sekstinga) // Psikhologo-pedagogicheskiye modeli i tekhnologii razvitiya lichnosti v tsifrovoy srede. Sbornik materialov Mezhvuzovskoy nauchno-prakticheskoy konferentsii. M.: MIP, 2022. S. 28-31.
19. Borgdorf A.Ye. Ugolovno-pravovyye aspekty onlayn sekstinga i gruminga v epokhu tsifrovoy sredy // Intellektual'nyye resursy – regional'nomu razvitiyu. 2022. № 1. S. 399-404.
20. Dizer O.A. Administrativno-pravovaya okhrana obshchestvennogo poryadka i obshchestvennoy bezopasnosti v usloviyakh formirovaniya tsifrovogo prostranstva // Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii. 2020. № 3 (89). S. 63-70.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Новгородов Н.Н. Общественный порядок в сети Интернет // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2025. № 2 (80). С. 75-83.