

DOI: 10.17803/1729-5920.2024.217.12.068-083

Э. Л. СидоренкоМосковский государственный институт
международных отношений (Университет) МИД России
г. Москва, Российская Федерация

Цифровое насилие в отношении детей: понятие, виды и особенности квалификации

Резюме. В работе предложен системный анализ современных форм цифрового насилия в отношении детей. Основываясь на его типовых параметрах, автор выделяет ключевые тренды развития цифрового насильственного воздействия на несовершеннолетних (экспоненциальный рост, расширение технологической базы, хабиутализацию, высокую латентность и коммерциализацию, сочетание онлайн- и офлайн-форм, организованность). На базе нескольких правовых и криминологических критериев приводится типология цифрового насилия и оценивается состоятельность авторской концепции в ее сравнении с подходами международных организаций и крупных национальных экспертных центров. Значительное внимание в работе уделено юридической оценке отдельных проявлений цифрового насилия в отношении детей (кибербуллинг, stalking, доксинг, фрейпинг, хеппислепинг, цифровой сексторции, онлайн-грумминг, порномести, флейминг, зумбомбинг и цифровому изнасилованию), рассмотрены алгоритмы их квалификации и оценена степень адаптивности уголовно-правовых норм к современным цифровым вызовам и угрозам. Основываясь на принципах функциональной эквивалентности, автор применяет существующие модели квалификации насильственных преступлений к особенностям совершения цифровых посягательств и указывает на возможные направления развития уголовного законодательства и судебной практики. Квинтэссенцией работы является идея о необходимости и своевременности разработки универсальной модели уголовно-правовой и криминологической превенции цифрового насилия в отношении детей, в которой одновременно были бы учтены как его общие криминогенные факторы и предпосылки (неправомерное использование персональных данных, кибератаки и утечки данных, отсутствие основ цифровой гигиены), так и содержательные особенности отдельных видов цифрового насилия.

Ключевые слова: цифровое насилие; квалификация; кибербуллинг; stalking; доксинг; фрейпинг; хеппислепинг; цифровая сексторция; онлайн-грумминг; порномест; флейминг; зумбомбинг; цифровое изнасилование

Для цитирования: Сидоренко Э. Л. Цифровое насилие в отношении детей: понятие, виды и особенности квалификации. *Lex russica*. 2024. Т. 77. № 12. С. 68–83. DOI: 10.17803/1729-5920.2024.217.12.068-083

Digital Violence against Children: The Concept, Types And Qualifications

Elina L. SidorenkoMoscow State Institute of Foreign Relations (MGIMO)
of the Ministry of Internal Relations of Russia
Moscow, Russian federation

Abstract. The work proposes a systematic analysis of modern forms of digital violence against children. Based on its typical parameters, the author identifies key trends in the development of digital violent influence on minors (exponential growth, expansion of the technological base, habitalization, high latency and commercialization, a combination of online and offline forms, organization). Based on several legal and criminological criteria, the author provides the typology of digital violence and assesses the consistency of the author's concept in its comparison with the approaches of international organizations and national expert centers. Considerable attention is paid

© Сидоренко Э. Л., 2024

to the legal assessment of individual manifestations of digital violence against children (cyberbullying, stalking, doxing, fraping, heppislapping, digital sextortion, online grooming, revenge porn, flaming, zumbombing and digital rape). The author analyzes algorithms for their qualifications and determines the degree of adaptability of criminal law to modern digital challenges and threats. Based on the principles of functional equivalence, the author applies existing models of qualification of violent crimes to the peculiarities of committing digital attacks and dwells on possible directions for the development of criminal legislation and judicial practice. The quintessence of the work is the idea of the need and timeliness of developing a universal model of criminal law and criminological prevention of digital violence against children, which would simultaneously take into account both its general criminogenic factors and prerequisites (misuse of personal data, cyberattacks and data leaks, lack of foundations of digital hygiene), and the content features of certain types of digital violence.

Keywords: digital violence; qualification; cyberbullying; stalking; doxing; fraping; heppislapping; digital sextortion; online grooming; porn revenge; flaming; zumbombing; digital rape

Cite as: Sidorenko EL. Digital Violence against Children: The Concept, types and qualifications. *Lex russica*. 2024;77(12):68-83. (In Russ.). DOI: 10.17803/1729-5920.2024.217.12.068-083

К постановке проблемы

Несмотря на негативную качественную и количественную трансформацию цифровой преступности, приобретение ею организованных форм и транснационального характера, современные наука и практика пока не приблизились к унифицированному толкованию ее видов и форм. В первую очередь это касается цифрового насилия.

Ввиду отсутствия четких понятийных границ термина «цифровое насилие» и невозможности в отдельных случаях дать правовую оценку его проявлениям официальный учет такого рода фактов не ведется ни в России, ни за рубежом.

По данным экспертного центра PewResearch Center, 40 % пользователей Интернета хотя бы раз пострадали от цифрового насилия, а 73 % становились его свидетелями¹. Чаще всего — в 66 % случаев — цифровое насилие происходило в социальных сетях. Вместе с тем эксперты указывают на гендерную специфику его проявления: мужчины, как правило, подвергаются угрозам и оскорблению, а женщины — сексуальным домогательствам и онлайн-сталкингу; при этом только половина жертв знакома с обидчиком. Наиболее уязвимыми считаются женщины в возрасте от 18 до 24 лет (на них приходится около 70 % случаев давления в Ин-

тернете). 54 % женщин, которые сообщали о том, что они подверглись цифровому насилию, были знакомы с обидчиком².

Согласно прогнозам зарубежных исследователей, к 2025 г. около 23 % пользователей Интернета столкнутся с цифровым насилием, а количество его жертв может достигнуть 9 млн человек³. При этом основными факторами роста рассматриваемых правонарушений эксперты называют: расширение цифровых инструментов и методов цифрового насилия и их сочетание с офлайн-преследованием; повышение уровня мобильности потенциальных жертв и расширение доступа преступников к личной информации⁴.

Особенно тревожной выглядит статистика цифрового преследования. По данным «Лаборатории Касперского», «в 2022 году с преследованием при помощи стalkerских программ (ПО) столкнулись 29 312 уникальных пользователей во всем мире. Полученные данные свидетельствуют об устойчивом росте числа стalkerских атак на протяжении всего 2022 года. В среднем каждый месяц 3 333 пользователя становились новыми жертвами цифровых шпионов. Чаще всего потерпевшими становятся жители России, Бразилии и Индии. Независимо от региона, самым распространенным приложением для преследования является

¹ URL: <https://www.forbes.ru/forbes-woman/492411-cto-takoe-doksing-i-sekstorsen-slovar-cifrovogo-nasilia>.

² Handbook of Research on Digital Violence and Discrimination Studies / F. Özsungur (ed.). IGI Global, 2022. DOI: 10.4018/978-1-7998-9187-1.

³ URL: <https://www.vpnrank.com/resources/cyberstalking-statistics/>.

⁴ Пособие по противодействию гендерному кибернасилию / ООН (UNWomenTurkey) // URL: https://eca.unwomen.org/sites/default/files/Field%20Office%20ECA/Attachments/Publications/2021/3/cyber%20violence_RUS.pdf.

Reptilicus, от которого пострадало 4 065 пользователей»⁵.

По данным ООН, наибольшую угрозу в цифровом пространстве представляет насилие в отношении детей. Они, как правило, сталкиваются с такими формами воздействия, как кибербуллинг и домогательства; онлайн-сексуальная эксплуатация и насилие; воздействие на психику насильственным и сексуальным контентом; пропаганда суицида и самоповреждений; торговля людьми и вербовка в криминальные или экстремистские группы; экономическая эксплуатация и мошенничество⁶.

В докладе ООН «Поведение детей школьного возраста в отношении здоровья» было отмечено, что около 16 % детей в возрасте от 11 до 15 лет подверглись киберзапугиванию за год по сравнению с 13 % четыре года назад. Центр по поиску пропавших и эксплуатируемых детей США получил в 2021 г. около 29 млн сообщений о подозреваемых случаях детской сексуальной эксплуатации, что на 35 % больше, чем в 2020 г.⁷

По данным WeProtect Global Alliance (2023), цифровое насилие в отношении детей характеризуется следующими тенденциями:

- рост объема материалов с насилием над детьми (с 2019 г. зафиксировано увеличение их объема на 87 %);

- рост количества случаев создания таких материалов с помощью искусственного интеллекта (ИИ), что усложняет выявление и ограничение распространения этих материалов;

- ускорение скорости виктимизации детей (общение на социальных игровых платформах может перерасти в высокорисковые ситуации груминга всего за 19 секунд; среднее время, необходимое для завершения груминга, составляет около 45 минут);

- рост объема самогенерируемого сексуального контента для детей (в период с 2020 по 2022 г. было зафиксировано четырехкратное

увеличение числа случаев самогенерируемого сексуального контента среди детей 7–10 лет; вовлечение детей в создание подобных материалов происходит через платформы, где они могут чувствовать себя в безопасности, что требует особых подходов к повышению их осведомленности о возможных угрозах);

- широкое распространение финансового сексуального шантажа (с 2021 по 2022 г. количество отчетов о финансовом сексуальном шантаже возросло со 139 до более 10 000 случаев);

- активное использование ИИ для создания контента с насилием над детьми⁸.

Для предотвращения онлайн-угроз разработан ряд международных и региональных документов, однако в большинстве своем они имеют фрагментарный характер и не ориентированы на системное внедрение. К сожалению, Россия здесь не является исключением.

Одним из самых опасных трендов цифрового насилия в российском сегменте Интернета выступает расширение и ужесточение травли детей и подростков. Эксперты мониторингового центра «Безопасность 2.0» зафиксировали рост травли подростков на 30 % ежеквартально. Факты цифрового насилия выявлены на всех крупных интернет-площадках, пользующихся популярностью у подростков и детей: «ВКонтакте», TikTok, Instagram и YouTube. В топ-5 российских регионов по наибольшему количеству случаев сетевой травли вошли Москва, Московская область, Санкт-Петербург, Приморский край и Крым⁹.

Как показали исследования «VK Добро» и «Дети Mail.ru», каждый пятый ребенок в России (22 %) сталкивался с кибербуллингом несколько раз, с каждым десятым (11 %) такое случалось однажды¹⁰.

Следует обратить внимание и на данные о вовлеченности несовершеннолетних в цифровое насилие. По экспертным оценкам, непосредственное участие в осуществлении кибер-

⁵ О состоянии стalkerского ПО в 2022 г. // URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/03/07183404/RU_The-State-of-Stalkerware_2022.pdf.

⁶ Office of the Special Representative of the Secretary-General on Violence Against Children (SRSG-VAC). A safer digital environment for children // URL: https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/a_safer_digital_environment_for_children.pdf.

⁷ A focus on adolescent peer violence and bullying in Europe, central Asia and Canada. Health Behaviour in School-aged Children international report from the 2021/2022 survey // URL: <https://iris.who.int/handle/10665/376323>.

⁸ URL: <https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-Press-Release.pdf>.

⁹ URL: <https://www.gazeta.ru/social/2021/11/11/14192821.shtml>.

¹⁰ URL: <https://tass.ru/obschestvo/17888733?ysclid=m345ljsu8k702140354>.

буллинга принимает около 8 % пользователей: так, около 4,5 % от общего числа пользователей составляют лица, производящие массовую публикацию постов с негативными намерениями (буллеры, хулиганы), и около 3,4 % от общего числа пользователей публикуют единичные посты с оскорблениями¹¹.

В целом можно выделить ряд устойчивых признаков и трендов цифрового насилия в отношении детей:

1) наблюдается экспоненциальный рост цифрового насилия наряду с расширением масштабов и форм интернет-коммуникаций;

2) используются комплекс цифровых сервисов и программное оборудование для совершения цифрового насилия и его сокрытия (например, сталкеры для осуществления слежения используют от 3 до 10 цифровых средств наблюдения и контроля);

3) наблюдается хабиутализация («опривычивание») цифрового насилия: респонденты отмечают, что сталкиваются с различными его формами и не исключают возможности быть вовлеченными в совершение цифрового насилия в отношении третьих лиц;

4) сохраняется высокая латентность цифрового насилия ввиду отсутствия у несовершеннолетних пользователей культуры поведения в Сети и алгоритмов реагирования на факты цифрового давления;

5) наблюдается институализация и коммерциализация отдельных форм цифрового насилия (в частности, признаки нелегальной индустрии приобретают цифровой сексуальный шантаж и домогательства);

6) цифровое давление нередко перетекает в применение физического и психологического насилия офлайн;

7) развиваются групповые формы цифрового насилия (особенно в части кибербуллинга и сексуального шантажа).

Понятие цифрового насилия

в международном и национальном праве

Невозможность эффективно противостоять росту цифрового насилия объясняется рядом факторов технического, организационного и даже ценностного характера, не последнее место среди которых занимает отсутствие единого теоретико-методологического подхода к оценке этого явления.

Несмотря на широкое употребление в праве термина «насилие», до сих пор не выработано его единое определение — во многом из-за широкой вариативности форм. Развитие цифровых технологий многократно расширило спектр проявлений насилия и поставило науку перед необходимостью более взвешенного отношения как к выделению его признаков, так и к разработке моделей его уголовно-правовой превенции.

В теории уголовного права понятие и признаки насилия всегда находились в фокусе научных исследований (Л. Д. Гаухман¹², А. А. Пионтковский¹³, В. Н. Кудрявцев¹⁴ и др.).

Не погружаясь в детальное рассмотрение доктринальных подходов, следует отметить, что в своем анализе исследователи так или иначе сосредотачивают внимание на следующих его признаках: насилие имеет общественно опасный характер; направлено против человека или группы лиц; применяется против воли или вопреки воле потерпевшего в целях реализации целей посягающего; причиняет физические и (или) психические страдания.

Раскрывая содержание цифрового насилия, важно основываться именно на этих признаках и выделять разновидности такого насилия исходя из вариативности его проявлений.

Отсутствие единого подхода к определению понятия цифрового насилия не могло не сказаться на качестве его научной проработки. В зависимости от подхода к определению системообразующих признаков искомого понятия

¹¹ Chatzakou D., Kourtellis N., Blackburn J., De Cristofaro E., Stringhini G., Vakali A. Mean birds: detecting aggression and bullying on Twitter // Proceedings of the ACM on Web Science Conference. Troy, New York, USA, 2017. P. 13–22.

¹² Гаухман Л. Д. Проблемы уголовно-правовой борьбы с насильственными преступлениями в СССР / под ред. И. С. Ноя. Саратов, 1981; Он же. Борьба с насильственными посягательствами. М., 1969.

¹³ Меньшагин В. Д., Пионтковский А. А. Курс советского уголовного права. Особенная часть. М., 1955. Т. 1.

¹⁴ Насильственная преступность / под ред. В. Н. Кудрявцева и А. В. Наумова. М., 1997. С. 3; Подгайный А. М. К вопросу о понятии и формах криминального насилия над личностью // «Черные дыры» в российском законодательстве. 2006. № 4. С. 429–431.

в основу дифференциации закладываются различные критерии: особенности технологий¹⁵, отношения преступника и жертвы¹⁶, характер применяемого воздействия¹⁷ и др. В частности, на уровне международных и зарубежных экспертных организаций цифровое насилие толкуется фрагментарно и ориентировано на решение прикладных задач вне их связи с формированием единой системы профилактики и предупреждения.

Фонд ООН в области народонаселения определяет цифровое насилие как акт насилия, который совершается, сопровождается, усугубляется и усиливается частично или полностью с помощью информационно-коммуникационных технологий или цифровых медиа в отношении лица по признаку его пола¹⁸.

ЮНИСЕФ определяет его как травлю с использованием цифровых технологий. Это повторяющееся поведение, направленное на то, чтобы запугать, разозлить или пристыдить тех, на кого направлено действие¹⁹.

Согласно выводам 67-й сессии Комиссии ООН по положению женщин, насилие с использованием технологий представляет собой любое действие, которое совершается, сопровождается, усугубляется или усиливается посредством использования информационно-коммуникационных технологий или других цифровых инструментов, которое влечет или может повлечь за собой физический, сексуальный, психологический, социальный, политический или экономический вред или другие нарушения прав и свобод²⁰.

Шире к понятию цифрового насилия подходит Организация экономического сотрудничества и развития. Она понимает под ним агрессивные действия, направленные на жертву с использованием электронных технологий. Цифровое насилие включает намеренные акты, совершаемые индивидуумом или группой людей через цифровые устройства, повторяющиеся во времени и направленные против человека, который не может легко защитить себя²¹.

Совет Европы определяет этот термин как воздействие на лицо, которое приводит (или может привести) к физическому, сексуальному, психологическому или экономическому вреду или страданиям и может включать эксплуатацию обстоятельств, особенностей или уязвимостей отдельного лица²². Европейский институт по вопросам гендерного равенства дополняет данное определение указанием на повторяющийся характер действий и их совершение в социальных сетях²³.

Обобщение существующих подходов позволяет определить цифровое насилие как онлайн-воздействие на лицо либо группу лиц против либо вопреки их воли. Оно совершается с помощью информационно-коммуникационных технологий для причинения вреда или угрозы его причинения физическим лицам, что приводит или может привести к причинению психологического, физического и экономического ущерба.

К правовым признакам цифрового насилия следует относить:

— способ совершения преступлений — использование информационно-телекоммуника-

¹⁵ *García T., Garnelo M., Kim J., Rosales M.* Applying Behavioral Insights to Address Digital Violence Against Women and Girls. Survey Findings. UN Women for the Americas and the Caribbean and The Behavioral Insights Team. 2021 // URL: https://lac.unwomen.org/sites/default/files/2023-10/en-applyingbehavioralinsights-nov26-v4_michelle_silva.pdf.

¹⁶ *Anderson C. A., Bushman B. J., Donnerstein E., Hummer T. A., Warburton W.* SPSSI Research Summary on Media Violence // *Analyses of Social Issues and Public Policy*. 2015. Vol. 15. Issue 1. P. 4–19.

¹⁷ *Аптюшина О. В.* Насильственная преступность и IT-технологии // *Lex russica*. 2019. № 9. С. 77–84.

¹⁸ URL: https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-Submission_UNFPA.pdf.

¹⁹ URL: <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>.

²⁰ Цифровые технологии и права женщин: тема сессии Комиссии ООН по положению женщин // URL: <https://news.un.org/ru/story/2023/03/1438172>. См. также: Состояние дел в области сбора доказательств и данных о насилии в отношении женщин с использованием современных технологий : Записка Структуры ООН по вопросам гендерного равенства и расширения прав и возможностей женщин. Конференция европейских статистиков. Группа экспертов по гендерной статистике. Женева, Швейцария, 10–12 мая 2023 г. // URL: https://unece.org/sites/default/files/2023-05/E6_WP20_Rafin_RU.pdf.

²¹ URL: [https://one.oecd.org/document/EDU/WKP\(2022\)8/en/pdf](https://one.oecd.org/document/EDU/WKP(2022)8/en/pdf).

²² URL: <https://www.coe.int/en/web/cyberviolence>.

²³ URL: https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf.

ционных сетей. К таким сетям постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» относит «сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью любых компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо обмен информацией (передачу сообщений) между компьютерными устройствами»²⁴.

Цифровое насилие может совершаться различными способами, как правило, путем направления сообщений конкретному лицу или группе лиц с использованием социальных сетей, мессенджеров, иных приложений и программ, включая технологии Bluetooth, AirDrop, поддерживающих функцию передачи данных, рассылки определенному или неопределенному кругу лиц (например, в мессенджере), размещения на личных страницах и на страницах групп пользователей, в том числе в социальных сетях и мессенджерах, ссылки для загрузки (скачивания) файлов и др.;

— характер воздействия: совершение действий против либо вопреки воле потерпевшего;

— последствия: причинение юридически значимого ущерба в виде психического (реже — физического) вреда личности.

Правовые признаки цифрового насилия дополняются рядом криминологических показателей:

— средовые особенности (коммуникативное виртуальное пространство);

— особенности взаимоотношений субъектов (анонимность, феномен растормаживания; невозможность физического избегания ситуации или оказания сопротивления, отсутствие обратной связи, значительное число свидетелей)²⁵;

— особые механизмы виктимизации жертв и способов причинения вреда.

Виды цифрового насилия в отношении детей и их уголовно-правовая оценка

Отсутствие универсального определения цифрового насилия сказалось и на подходах к установлению его разновидностей.

Современные доктринальные оценки отличаются обилием неологизмов, калькированных терминов и авторских произвольных интерпретаций в отсутствие единого критерия разграничения соответствующих понятий. Во многом это объясняется тем, что феноменологическое поле изучаемого понятия находится на стадии своего формирования, и во многом его определение опирается на эмпирические методы наблюдения и включения.

Разнообразие подходов к установлению видов цифрового насилия характерно и для международного сообщества. В частности, Всемирная организация здравоохранения (ВОЗ) выделяет следующие виды онлайн-насилия в отношении детей:

— онлайн-домогательства: взрослые используют онлайн-коммуникации для установления доверительных отношений с ребенком с целью манипуляции и дальнейшего сексуального насилия;

— создание и распространение контента с изображением насилия над детьми: включает изображения и видео с участием обнаженных или частично одетых детей, а также с сексуальными действиями, записанными для последующего распространения;

— кибербуллинг: повторяющиеся акты агрессии, включая угрозы, клевету и использование языка ненависти, направленные на унижение или запугивание ребенка;

— передачу интимного контента без согласия: случаи распространения изображений или видео сексуального характера, часто с целью вымогательства денег или сексуальных услуг²⁶.

²⁴ Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» // СПС «КонсультантПлюс».

²⁵ Жмуров Д. В. Жертвы кибербуллинга: состояние проблемы // Российский следователь. 2023. № 1. С. 45–50.

²⁶ URL: <https://cdn.who.int/media/docs/default-source/documents/child-maltreatment/online-violence-final.pdf>.

Аналитики ЮНИСЕФ указывают следующие виды подгруппы цифрового насилия:

- 1) распространение ложной информации (ложных слухов) или публикацию унижительных фотографий в социальных сетях;
- 2) отправку оскорбительных сообщений или угроз через платформы обмена сообщениями;
- 3) имитацию личности для отправки оскорбительных сообщений от ее имени;
- 4) публичные формы коммуникации для оскорблений (публикацию оскорбительных сообщений);
- 5) создание веб-сайтов или страниц в социальных сетях, посвященных издевательствам над жертвой, для насмешек²⁷.

В докладе «Прекращение мучений: борьба с травлей от школьного двора до киберпространства» специальный представитель Генеральной Ассамблеи ООН выделил пять видов онлайн-насилия:

- 1) отправку оскорбительных или угрожающих сообщений, которая включает публикацию или отправку электронных сообщений, изображений или видео, направленных на запугивание, преследование или унижение человека;
- 2) распространение ложных слухов или унижающей информации о жертве в Интернете;
- 3) вербальное насилие (оскорбления, угрозы или унижительные комментарии в социальных сетях, чатах и на других онлайн-платформах), которое может включать как прямые нападки, так и косвенные, например публичное унижение или высмеивание;
- 4) сексуальное насилие — сексуальные домогательства или угрозы сексуального характера через электронные средства связи;
- 5) социальное исключение — исключение ребенка из онлайн-сообществ, групп или бесед²⁸.

Более системный подход предложен Комиссией Европейского Союза. Она выделяет основные формы насилия, сексуальные формы кибербуллинга и специфические виды цифрового насилия в отношении детей.

К первой группе относятся: распространение оскорбительных сообщений; публикация унижающих материалов; киберпреследование (сталкинг); создание ложных профилей; флейминг (споры в онлайн-среде, которые намерен-

но разжигают агрессию); хеппислеппинг (нападение на жертву с последующей видеозаписью инцидента); секстинг (отправка интимных изображений или сообщений, которые могут быть впоследствии использованы для шантажа или унижения).

Сексуальными формами кибербуллинга предлагается считать: ревендж-порн (месть порнографией) (распространение интимных изображений или видео без согласия жертвы с целью причинения эмоционального вреда); сексторшен (принуждение к отправке сексуальных материалов с последующим шантажом их публикацией в Сети).

К третьей группе насилия относятся: цифровой обман (использование ложных данных для введения жертвы в заблуждение с целью распространения ложной информации или унижения); изоляция в онлайн-среде; групповое нападение онлайн (совместные действия нескольких агрессоров, направленные на травлю одного человека)²⁹.

В попытках систематизировать разные проявления цифрового насилия эксперты предлагают несколько критериев их классификации: возраст и пол жертв; мотивацию поведения преступника; характер насилия; механизм преступного поведения и др.

Обобщение проявлений цифрового насилия в срезе частоты и устойчивости позволяет выделить и проанализировать следующие его разновидности:

— **Цифровой бойкот (исключение)** — намеренное демонстративное исключение несовершеннолетней жертвы из чатов, совместных онлайн-бесед в ВКС или социальных сетях. По результатам проведенного нами опроса, более 70 % активных пользователей социальных сетей сталкивались с такой формой психологического давления. Несмотря на то что такого рода действия нередко сильно травмируют жертву, они не признаются правонарушением.

— **Киберсталкинг и доксинг (doxing)** — публикация в Сети конфиденциальной личной информации о потерпевшем. Как правило, речь идет о домашнем адресе, адресе электронной почты, номере телефона и др. Сбор информации осуществляется с целью преследования, запугивания или вымогательства.

²⁷ URL: <https://www.undrr.org/understanding-disaster-risk/terminology/hips/tl0026>.

²⁸ URL: https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/tackling_bullying_from_schoolyard_to_cyberspace_low_res_fa.pdf.

²⁹ URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762331/EPRS_BRI\(2024\)762331_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762331/EPRS_BRI(2024)762331_EN.pdf).

Судебная практика накопила достаточно примеров квалификации данных деяний по совокупности ст. 137 и 272 УК РФ. Но, несмотря на устойчивость такого подхода, суды нередко испытывают трудности при квалификации сбора и распространения личных сведений в Интернете. Во многом это связано с высокой анонимностью интернет-коммуникаций, а также с трудностями установления самого факта преступного сбора данных, когда эти данные свободно публикуются самим потерпевшим на открытых страницах и в аккаунтах, в новостной ленте и в сообщениях в публичных чатах и группах. В частности, на практике крайне трудно квалифицировать случаи сбора данных при помощи стalkerских приложений. Согласно данным «Лаборатории Касперского», «одним из самых популярных стalkerских приложений является Reptilicus, но при этом в целом в России было зарегистрировано более 180 стalkerских приложений, функциональность которых варьируется в зависимости от типа приложения и от того, распространяется ли оно на платной основе или нет. Чаще всего такие приложения распространяются под видом легитимного ПО, предназначенного для защиты от кражи устройства или родительского контроля. На самом же деле они устанавливаются на смартфоны пользователей без их ведома и позволяют осуществлять слежку за жертвой в скрытом режиме».

Стalkerские программы отличают следующие функции: сокрытие значка приложения; чтение SMS, MMS и журналов вызовов; получение списка контактов; отслеживание местоположения с помощью GPS; доступ к календарю; чтение сообщений из популярных мессенджеров и социальных сетей; просмотр фотографий и изображений из фотогалереи смартфона; создание скриншотов; съемка фотографий с фронтальной камеры (в режиме селфи)³⁰.

Установка подобных программ на компьютерное оборудование жертвы следует квалифицировать по ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ, но только при условии, что соответствующая компьютерная программа будет признана вредоносной.

В Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) под компьютерными программами по смыслу указанной статьи УК РФ в основном понимаются программы, известные как компьютерные вирусы (черви, троянские кони, кейлоггеры (клавиатурные шпионы), руткиты и др.)³¹.

Ни судебная практика, ни закон не дают исчерпывающего перечня признаков, позволяющих оценивать программу как вредоносную. В частности, нет критериев, ограничивающих стalkerское ПО от средств родительского контроля.

В постановлении Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» отмечается, что согласие потерпевшего на установку такого ПО исключает ответственность по ст. 273 УК РФ при условии, что вредоносная программа не будет использоваться для сбора информации. Но на практике это приводит к тому, что согласие на установку программы априори расценивается как признак правомерности сбора информации.

И о том, что такой подход судебной практики является распространенным, говорит статистика: по нашим данным, в 2/3 фиксируемых случаев слежение за жертвой осуществляется ее родственниками с ее одобрения и очень часто в дальнейшем приводит к реальному насилию.

Вызывает трудности и правовая оценка сбора информации о человеке на основе доступных интернет-метрик. В частности, Яндекс-метрика позволяет в свободном режиме отслеживать поведение пользователя: увидеть карты ссылок, кликов, скроллинга (как глубоко листаются страницы), аналитику форм (как пользователи заполняют их)³². Таким образом, у лица, работающего с метрикой, есть возможность отслеживать активность жертвы при условии, если

³⁰ URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/03/07183404/RU_The-State-of-Stalkerware_2022.pdf.

³¹ URL: <http://genproc.gov.ru> по состоянию на 15.04.2014.

³² URL: <https://skillbox.ru/media/marketing/yandexmetrika-glavnye-otchyety-i-funktsii-o-kotorykh-dolzhen-znat-dazhe-novichok/?ysclid=m2hgbox3pt2153340843#stk-1>.

у последней аккаунты и страницы являются открытыми.

Отследить конкретного человека в сети вполне легально позволяют такие программы, как Rambler's Top 100, HotLog, SpyLOG. При посещении большинства отечественных сайтов данные программы оставляют свои следы (HotLog, например, по умолчанию сохраняет их до 2070 г.), и по этим следам отслеживается пребывание онлайн. С их помощью можно выяснить, с какого сайта пришел посетитель, где физически находится оборудование, какой операционной системой пользуется человек, а также узнать, когда именно посетитель открыл данный сайт и по какому маршруту прошел по нему³³.

Именно на анализе оставленных программами следов и формируется цифровой образ человека, который в последующем используется в рекламных либо преступных целях.

Активно развивается и индустрия приложений, отслеживающих поведение человека в социальных сетях. Так, программа «Агент 307» позволяет определить, кто посещает страницу, посмотреть, кто ставит дизлайки, проанализировать свои диалоги и найти аккаунты людей, живущих поблизости.

Followers Plus в «Инстаграме»³⁴ позволяет определить, кто подписался либо отписался от аккаунта, найти заблокировавших страничку пользователей и начать их травлю.

Программа «Панда» открывает доступ к страницам тех, кто интересуется профилем конкретного лица, и позволяет в дальнейшем отслеживать их активность.

Приложение «ВКонтакте» «Мои гости» указывает на страницы тех, кто интересовался определенной информацией либо людьми: оно показывает статистику их посещений, лайков, репостов и комментариев. Эта программа бесплатна и может быть установлена на любом смартфоне и компьютере.

Распространение такого рода программ ставит вопрос о том, где проходит граница, отделяющая правомерный интерес к другому

человеку от преступного нарушения неприкосновенности частной жизни (ст. 138 УК РФ).

Сложности на практике вызывает и порядок сбора и использования персональных данных.

Как показал проведенный нами опрос, 90 % пользователей не знают, какой объем информации о них собирается в Интернете. Как правило, их согласие испрашивается на сбор конкретных данных, но фактически анализируется широкий спектр информации, относящийся, помимо прочего, к персональным данным. В отдельных случаях программы в рамках реализации своих задач прибегают к стороннему ПО, не уведомляя об этом пользователей.

Тревогу вызывает и статистика утечки данных.

Согласно отчету экспертно-аналитического центра (ЭАЦ) «ГК InfoWatch», количество утечек в мире за 2023 г. выросло более чем на 60 %, а объем скомпрометированных персональных данных — более чем в два раза.

На одну утечку в среднем пришлось 4,04 млн записей персональных данных. Только 38,7 % зарегистрированных в 2023 г. данных содержали сведения о количестве скомпрометированных записей персональных данных. В 2023 г. зарегистрировано 1 024 крупных утечек данных, каждая из которых включает не менее 1 млн записей персональных данных. Количество крупных атак выросло почти на 50 %³⁵.

К сожалению, существующих законодательных мер сдерживания утечки данных недостаточно для того, чтобы стимулировать бизнес и госучреждения к созданию надежной системы их хранения. Штрафы оказываются значительно меньше затрат на установку защиты.

Кроме того, вызывает вопросы правовая основа работы компаний, занимающихся анализом взломов информационных баз. В рамках своей деятельности они используют массивы украденных третьими лицами персональных данных. При этом они не являются субъектами обработки данных и не испрашивают согласия пользователей. Отсутствие четкой регламентации деятельности таких компаний нередко

³³ URL: https://www.igromania.ru/article/12578/Imenem_Bolshogo_Brata_kak_vysledit_cherez_onlayn_lyu_bogo_cheloveka.html?ysclid=m2hglrggd0788378274.

³⁴ Принадлежит компании Meta. Решением Тверского районного суда города Москвы от 21.03.2022 компания «Мета Платформс, Инк.» (Meta Platforms, Inc.) признана экстремистской организацией и ее деятельность запрещена на территории Российской Федерации.

³⁵ Исследование утечек информации в мире за 2022–2023 гг. // URL: <https://www.infowatch.ru/sites/default/files/analytics/files/issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf?ysclid=m2m0joq8r2523085657>.

приводит к тому, что они сами являются источниками получения информации о цифровом профиле пользователей Интернета.

В детальной проработке нуждаются и вопросы квалификации избыточного сбора и обработки информации, допуска пользователя к управлению своими данными и установления уголовной ответственности за незаконный сбор и использование персональных данных.

— **Кибертравля** — агрессивное целенаправленное воздействие на человека в Сети, которое может варьироваться от обидных шуток до террора. Нередко травля направлена на доведения человека до самоубийства, но на практике это доказать очень сложно в связи с тем, что в большинстве случаев способы цифрового воздействия на жертву не укладываются в узкие рамки обозначенных статьей 110 УК РФ способов: угрозы, жестокого обращения, систематического унижения человеческого достоинства.

Интернет-манипуляции могут носить не только прямой, но и косвенный характер. Они могут выражаться в скрытых формах запугивания, дискредитации, давления. Задача преступника в этих случаях — не столько унижить жертву, сколько взять под полный контроль ее поведение.

Традиционные способы давления на жертву сочетаются с новыми когнитивными методами воздействия.

Модель поведения жертвы задается действиями виновного и предполагает следующую последовательность: персонализация — все события интерпретируются человеком слишком лично; выборочное абстрагирование — оценка одной детали превращается в оценку всего события; произвольные умозаключения — умозаключения, не основанные на фактах, становятся определяющими для сознания; сверхгенерализация — обобщение строится на основании единичного или немногих случаев, произвольно выбранных преступником; преувеличение, катастрофизация — разрушительные последствия какого-либо события многократно преувеличиваются³⁶.

Усложнение форм цифрового насилия выводит на первый план вопрос о необходимости проработки признаков доведения до самоубийства с учетом использования новых форм когнитивного цифрового воздействия, прежде всего

через формирование методических указаний по расследованию и профилактике действий в Интернете, направленных на доведение до самоубийства.

— **Фрейпинг** — форма цифрового насилия, при которой агрессор получает доступ к сетевому аккаунту жертвы, от ее имени ведет дискуссии, оскорбляет, публикует материалы порочащего и оскорбительного характера.

Доступ к чужому аккаунту относится к разновидностям несанкционированного доступа к компьютерной информации и квалифицируется по ст. 272 УК РФ.

Если же фрейпинг является этапом совершения другого преступления (например, сексуального домогательства), он предполагает совокупность преступлений.

— **Хеппислепинг** — запись видеороликов, на которых агрессоры избивают жертву или издеваются над ней, а затем выкладывают их в Интернет.

Федеральный закон от 08.08.2024 № 218-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» дополнил 10 составов УК РФ (убийство, умышленное причинение тяжкого вреда здоровью, умышленное причинение средней тяжести вреда здоровью, умышленное причинение легкого вреда здоровью, побои, истязание, угрозу убийством или причинением тяжкого вреда здоровью, похищение человека, незаконное лишение свободы, использование рабского труда) квалифицирующим признаком — совершением умышленного преступления с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»).

По мнению авторов соответствующего законопроекта, треш-стримы не только угрожают жизни и здоровью отдельных лиц, но и посягают на общественную безопасность и общественный порядок, вводя данное преступное поведение в ранг допустимого и возможного для неограниченного круга лиц. Трансляции формируют ощущение, что данные действия можно повторять, что уже сейчас повлекло случаи подражательства известным треш-стримерам³⁷.

Вопросы, однако, вызывает сама конструкция квалифицированного состава. Формули-

³⁶ Барабаш В. В., Бордюгов Г. А., Котеленец Е. А. Образы России в мире. М., 2010.

³⁷ Паспорт проекта федерального закона № 506240-8 «О внесении изменений в Уголовный кодекс Российской Федерации» (в части усиления ответственности за совершение преступлений с публичной демон-

ровка «совершение преступления с публичной демонстрацией» не дает возможности определить хронологию деяний. Важно ли для квалификации, чтобы преступление транслировалось онлайн либо достаточно его записи с последующей демонстрацией в СМИ или Интернете? Что будет относиться к публичной демонстрации? Как следует квалифицировать убийство, записанное на видео, но так и не выложенное в Сеть? Как надлежит оценивать действия соучастников, если демонстрация преступления охватывалась умыслом только одного из них? Как следует рассматривать преступление, если умысел на его демонстрацию возник позднее?

К сожалению, практика пока не ответила на эти вопросы, но их решение принципиально важно в условиях активного развития как треш-стриминга, так и хеппислепинга.

— **Цифровая сексторция (сексторшен)** — форма шантажа, при которой лицо угрожает раскрыть компрометирующую информацию или опубликовать интимные материалы о человеке, если им не будут выполнены определенные требования. Как правило, эти требования обращены к малолетним и несовершеннолетним лицам и касаются публикации интимных фото либо демонстрации сексуальных манипуляций.

В настоящее время формируется преступный рынок цифровой сексторции. В социальных сетях создаются специальные закрытые группы, где выкладываются обнаженные фотографии жертв и организуются их групповой шантаж или травля.

Организованные группы преступников действуют по принципу разделения ролей: одни собирают информацию, другие разрабатывают программы для взлома, третьи ведут диалог с жертвами, четвертые организуют травлю. Уровнем ниже располагаются региональные группы. Они собирают компрометирующую информацию (интимный контент) или создают поводы сами (например, телеграм-канал «Рынок шкур» шантажирует потенциальных потерпевших публикациями с разоблачением якобы их прошлой

жизни; тенденциозные сайты могут представить законопослушных граждан как преступников в прошлом). Мелкие вымогатели работают по случайным, единичным целям, как правило, не применяют программные методы и не полагаются серьезной медийной поддержкой. Они довольствуются примитивным шантажом в социальных сетях, закрытых чатах, сексуальных стримах и т.п.³⁸

В каждом конкретном случае следует детально изучать механизм преступного поведения и оценивать степень организованности группы.

В случае если лица используют шантаж с целью получения от потерпевшего сексуальных услуг, данное деяние квалифицируется по ст. 133 «Понуждение к действиям сексуального характера», если требуют имущество либо деньги — по ст. 163 «Вымогательство» УК РФ. В зависимости от направленности умысла, деяния могут квалифицироваться и по иным статьям УК РФ (ст. 127.2, ст. 183, п. «в» ч. 2 ст. 230.1 и др.).

Иногда сексуальная сексторция выражается в форме спам-рассылки, убеждающей пользователя, что у недоброжелателей есть компрометирующие его съемки во время посещения порносайтов. Согласно отчету компании ESET, 11 % пользователей Сети были объектами таких «сексуальных вымогательств»³⁹.

В научной литературе и судебной практике до сих пор идут споры о том, как квалифицировать требование передачи имущества под угрозой распространения сведений, не соответствующих действительности. Дискуссия по данному вопросу связана с разъяснениями постановления Пленума Верховного Суда РФ от 17.12.2015 № 56 «О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации)», согласно которым «под сведениями, позорящими потерпевшего или его близких, следует понимать сведения, порочащие их честь, достоинство или подрывающие репутацию (например, данные о совершении правонарушения, аморального поступка)»⁴⁰.

страцией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»)) // СПС «КонсультантПлюс».

³⁸ Жмуров Д. В. Кибервиктимология вымогательств в цифровом пространстве // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. Т. 24. № 2. С. 85–98. URL: <https://doi.org/10.24866/1813-3274/2022-2/85-9>.

³⁹ Каждый десятый пользователь в России стал жертвой шантажа во время самоизоляции // URL: <https://hacker.ru/2020/06/01/covid-19-sextortion/>.

⁴⁰ Карпов К. Н. Квалификация вымогательства при угрозе распространения сведений о совершенном лицом правонарушении либо аморальном поступке // Современное право. 2018. № 5. С. 77–83.

Полагаем, что дилемма между обманом (мошенничеством) и угрозой (вымогательством) как определяющими уголовно-правовыми признаками должна быть разрешена в пользу угрозы. Как верно отмечает П. С. Яни, «угроза, по замыслу виновного, должна оказать воздействие на потерпевшего, который в результате передаст свое или находящееся в его ведении либо под его охраной имущество, передаст право на имущество (также не обязательно, чтобы субъектом такого права был сам потерпевший), совершит иные действия имущественного характера в пользу виновного»⁴¹.

Как показывает статистика, чаще всего сексуальный шантаж осуществляется в отношении лиц, практикующих сексинг как форму интернет-коммуникаций. По данным Pew Research Center, среди 25–44-летних американцев 56 % практикуют секстинг. В альтернативных исследованиях эта цифра превышает 80 %⁴².

Возможно несколько форм интернет-шантажа: угроза распространения интимных фотографий или видео с потерпевшим; шантаж перепиской, репостами, мемами; принадлежностью к какой-либо группе или сообществу; обвинением в растлении малолетних или сексуальных домогательствах.

Если порочащие потерпевшего сведения были добыты путем несанкционированного доступа к компьютерной информации либо установки вредоносных программ, данное деяние требует совокупности со ст. 272 или 273 УК РФ соответственно.

Если же интимные фотографии или сообщения лица, не достигшего возраста 16 лет, были получены в результате ведения с ним интимной переписки, есть основания для квалификации таких действий по ст. 135 «Развратные действия» при условии достижения виновным 18 лет.

— **Онлайн-груминг** — сексуальное домогательство по отношению к детям, реализуемое в сети «Интернет». Груминг имеет мани-

пулятивные черты, а несовершеннолетние, как правило, в силу возраста и уровня развития не могут в полной мере осознавать сексуальный характер и противоправное значение подобных коммуникаций⁴³.

По данным экспертов, анализ коммуникаций выявил три основные цели, которые преследовали взрослые при общении с несовершеннолетними:

1) совершить сексуальные действия в реальной жизни путем организации личной встречи (данная цель наблюдалась в 60,9 % случаев продолженных коммуникаций, в 2,4 % была реализована);

2) получить доступ к личным материалам интимного характера (фотографиям, видеоизображениям) несовершеннолетнего (75,6 % случаев продолженных коммуникаций; в 39,0 % случаев данная цель была реализована);

3) совершить сексуальные действия онлайн (19,5 % случаев продолженных коммуникаций; в 7,3 % случаев данная цель была реализована)⁴⁴.

Совершеннолетний преступник, как правило, сам находит жертву в социальных сетях, посылает ей запрос на дружбу под своим настоящим либо фиктивным аккаунтом. Постепенно виновный и потерпевший начинают переписываться, делиться новостями и переживаниями. Преступник пытается войти в доверие, завоевать уважение и привязанность потерпевшего. В дальнейшем он начинает вести разговоры на сексуальные темы, расспрашивать об интимной жизни, посылает фотографии обнаженного тела и просит фотографии в ответ. Если подросток соглашается, то в последующем ему предлагают перейти на видеообщение, где начинается его развращение⁴⁵.

Как правило, такие действия квалифицируются как развратные действия (ст. 135 УК РФ) при условии, если жертва не достигла возраста 16 лет, а виновный является совершеннолетним лицом. Если же малолетнему меньше 12 лет, ука-

⁴¹ Яни П. С. Вопросы квалификации вымогательства // Законность. 2015. № 11. С. 40–45.

⁴² How common is sexting? Over 80 percent of survey respondents report sexting within the past year // URL: <https://www.sciencedaily.com/releases/2015/08/150808172217.htm>.

⁴³ Медведева А. С., Дозорцева Е. Г. Характеристики онлайн-груминга как вида сексуальной эксплуатации несовершеннолетних (по результатам анализа переписок взрослых и детей в сети Интернет) // Психология и право. 2019. Т. 9. № 4. С. 161–173. DOI: 10.17759/psylaw.2019090412.

⁴⁴ Медведева А. С., Дозорцева Е. Г. Указ. соч.

⁴⁵ Семенцова И. А., Фоменко А. И. Актуальные вопросы предупреждения преступлений, совершаемых лицами с расстройством сексуального предпочтения (педофилией) посредством сети Интернет // Теория и практика общественного развития. 2015. № 10. С. 90.

званное деяние может быть квалифицировано по п. «б» ч. 4 ст. 132 УК РФ — как совершаемое в отношении беспомощной в силу возраста жертвы.

Сложнее дать квалификацию грумингу, если он осуществляется в отношении потерпевшего (потерпевшей), достигшего 16 лет, и предполагает дальнейшую демонстрацию интимных материалов.

Распространение интимных изображений лица, если оно совершено против его согласия и отсутствуют иные законные основания, подлежит квалификации по ст. 137 УК РФ. Между тем при уголовно-правовой оценке такого деяния необходимо решить вопрос о вменении незаконного оборота порнографической продукции. В правоприменительной практике обозначились три основных подхода к его квалификации⁴⁶.

В рамках первого указанное деяние предлагается квалифицировать только по ст. 137, без дополнительного вменения ст. 242 УК РФ. Как правило, суды ставят знак равенства между интимными и порнографическими материалами и не усматривают умысел виновного на причинение вреда общественной нравственности⁴⁷.

Второй подход судов подразумевает вменение ст. 242 наряду со ст. 137 УК РФ в силу отнесения распространенных материалов к порнографии. Например, М. О. была признана виновной в совершении преступлений, предусмотренных частью 1 ст. 137 и пунктом «б» ч. 3 ст. 242 УК РФ, поскольку отправила видео интимного характера с участием супруга и его любовницы нескольким знакомым последней, разместив его предварительно в фейковом аккаунте социальной сети. На фейковой странице было размещено также предложение сексуальных услуг. Видео было получено обвиняемой из общего с мужем облачного хранилища файлов. В определении суда кассационной инстанции уточняется, что, во-первых, действия интимного характера на видео — личная тайна потерпевшей и, во-вторых, «видео интимного характера» признано порнографическим материалом, а его размещение на фейковой странице

и отправка другим лицам — распространением и публичной демонстрацией с использованием сети «Интернет»⁴⁸.

В рамках третьего подхода предлагается оценивать деяние по ст. 242, без дополнительной квалификации по ст. 137 УК РФ. Таким образом, суды необоснованно сужают правовую оценку содеянного, не принимая во внимание тот факт, что демонстрация сексуального контента в первую очередь направлена на ущемление прав потерпевшего (потерпевшей).

Если виновный склоняет несовершеннолетнюю жертву к демонстрации сексуальных манипуляций и осуществляет ее фото- или видеосъемку, его действия квалифицируются по п. «г» ч. 2 ст. 242.2 и ст. 137 УК РФ. Если же он транслирует в переписке, открытых или закрытых группах направленные несовершеннолетним фото или видео, его действия оцениваются по п. «г» ч. 2 ст. 242.1 и ст. 137 УК РФ.

— **Порноместь** (Revenge porn) — публикация интимных видеороликов или фотографий с целью мести обычно бывшему партнеру или супругу.

Такого рода материал выкладывается в открытые и закрытые группы, распространяется в переписке или в виде спама.

Эти действия квалифицируются по совокупности ст. 137 и п. «б» ч. 3 ст. 242 УК РФ, если были выложены материалы совершеннолетней жертвы порнографического характера. Если же публикуются материалы интимного характера, не признанные порнографией, данное деяние квалифицируется по ст. 137 УК РФ.

Порноместь может быть основана на дипфейке: с помощью искусственного интеллекта можно создать изображение, аудио или видео, которое будет правдоподобно имитировать внешность или голос человека⁴⁹.

Применение дипфейков при совершении цифровых преступлений еще только предстоит детально изучить, но уже сейчас некоторые вопросы стоят особенно остро. В частности, неясно, как определить, кто на самом деле стал жертвой дипфейка, ведь видео изобраа-

⁴⁶ Алексеева Т. С. Интимные изображения человека как предмет нарушения неприкосновенности частной жизни // Уголовное право. 2023. № 4. С. 3–13.

⁴⁷ Кассационное определение Третьего кассационного суда общей юрисдикции от 05.04.2022 по делу № 77-1029/2022 // СПС «КонсультантПлюс».

⁴⁸ См.: Алексеева Т. С. Указ. соч.

⁴⁹ Делфино Р. А. Порнографические дипфейки: следующий трагический акт феномена «порно из мести» и необходимость принятия уголовного закона на федеральном уровне // Актуальные проблемы экономики и права. 2020. Т. 14. № 1. С. 105–141. DOI: <http://dx.doi.org/10.21202/1993-047X.14.2020.1.105-141>.

жает как минимум двух участников — того, чье тело было использовано, и того, чье лицо было добавлено? Например, программа FakeApp позволяет накладывать одно изображение на другое даже человеку, не имеющему специальных навыков. ПО анализирует и изменяет изображение лица одного человека, а затем прикрепляет его к телу другого.

Следуя буквальному толкованию ст. 137 УК РФ, это деяние сложно отнести к нарушению неприкосновенности частной жизни, поскольку с жизнью жертвы оно не связано.

Такие действия следует относить к производству и распространению порнографии и к способам развратных действий, если они носят порнографический характер.

Впрочем, практически невозможно дать правовую оценку распространению дипфейков, содержащих внешне интимную, а не порнографическую информацию, ведь само по себе оно представляет собой одну из форм цифрового шантажа и насилия над личностью.

— **Флейминг** (споры в онлайн-среде, которые намеренно разжигают агрессию). В настоящее время опасность этого вида цифрового насилия недооценивается в науке и судебной практике. В частности, не принимается во внимание тот факт, что в отдельных случаях флейминг может быть приготовлением к совершению преступлений (например, экстремизма) либо способом вовлечения в преступную и аморальную деятельность.

— **Зумбомбинг (zoom-bombing)** — захват видеоконференции и прерывание общения путем запуска видео (часто порнографического содержания) либо оскорбительных изображений.

Такого рода действия оцениваются судами как публичная демонстрация соответствующих материалов и в зависимости от характера самих материалов могут рассматриваться как распространение порнографии, оправдание терроризма и др.

— **Виртуальное изнасилование.** Возможность совершения подобного рода деяний стали серьезно обсуждать сравнительно недавно на фоне активного развития метавселенных и виртуального пространства.

В частности, в Великобритании расследуется случай группового изнасилования цифрового персонажа 16-летней девочки⁵⁰.

В США с обвинением в изнасиловании обратилась сотрудница правозащитной группы SumOfUs. Она заявила, что ее аватар на платформе виртуальной реальности Horizon World был изнасилован во время онлайн-игры⁵¹. Несколько пользователей попросили жертву отключить настройку безопасности, которая не позволяет аватарам приближаться друг к другу на расстояние менее 1,2 м, и изнасиловали ее персонаж.

Такого рода действия можно признать преступными только при установлении умысла виновного на совершение развратных действий в отношении лица, не достигшего 16 лет (ст. 135 УК РФ).

В остальных случаях признание данного деяния преступлением невозможно по ряду объективных обстоятельств: отсутствие правового определения метавселенной и виртуальной реальности, исключение правосубъектности аватаров и др.

Тем не менее очевидно, что с развитием технологий дополненной реальности и метавселенных важно будет разработать эффективные гарантии защиты прав человека в цифровом пространстве.

Выводы и заключения

Проведенный анализ цифрового насилия в отношении детей со всей очевидностью показал, что настоящая проблематика находится в начальной стадии своего изучения и проработки.

В качестве рекомендаций, направленных на выстраивание системы предупреждения цифрового насилия, предлагается рассмотреть следующие:

— формирование на уровне законодательства, следственной, прокурорской и судебной практики единого подхода как к самому определению цифрового насилия, так и к выделению его разновидностей;

— разработку единых критериев оценки допустимости сбора и применения персональной информации цифровыми сервисами и социальными сетями;

— анализ вопроса об установлении уголовной ответственности за следующие деяния: незаконное внесение, удаление или изменение

⁵⁰ URL: <https://rg.ru/2024/01/03/policiia-britanii-rassleduet-pervoe-iznasilovanie-v-virtualnoj-realnosti.html?sclid=m27hjkt2sj154294726>.

⁵¹ URL: <https://incrusia.ru/news/sexual-assault-metaverse/?ysclid=m2iui8dn13391710738>.

данных в автоматизированной системе обработки данных, обработку украденных персональных данных; кражу, незаконную передачу, распространение и сбыт и приобретение идентификационной информации о другом человеке;

— детальное изучение вопроса о правовых границах использования интернет-метрик и ПО, анализирующих поведение интернет-пользователей. Важно также четко определить критерии вредоносных программ в части оценки стalkerского ПО;

— расширение системы информирования граждан (и особенно несовершеннолетних)

о способах защиты в Интернете и алгоритмах блокировки деструктивного контента и агрессивных пользователей. Как показал проведенный опрос, только 12 % опрошенных заявили, что знают, куда и как жаловаться на факты цифрового насилия;

— привлечение детей к разработке решений по обеспечению их безопасности онлайн⁵². Программы по профилактике онлайн-насилия, направленные на обучение детей и их родителей, доказали свою эффективность, однако они не должны переносить всю ответственность на самих детей и их родителей.

СПИСОК ЛИТЕРАТУРЫ

Алексеева Т. С. Интимные изображения человека как предмет нарушения неприкосновенности частной жизни // Уголовное право. 2023. № 4. С. 3–13.

Артюшина О. В. Насильственная преступность и IT-технологии // Lex russica. 2019. № 9. С. 77–84.

Барабаш В. В., Бордюгов Г. А., Котеленец Е. А. Образы России в мире. М., 2010.

Гаухман Л. Д. Борьба с насильственными посягательствами. М., 1969.

Гаухман Л. Д. Проблемы уголовно-правовой борьбы с насильственными преступлениями в СССР / под ред. И. С. Ноя. Саратов, 1981.

Делфино Р. А. Порнографические дипфейки: следующий трагический акт феномена «порно из мести» и необходимость принятия уголовного закона на федеральном уровне // Актуальные проблемы экономики и права. 2020. Т. 14. № 1. С. 105–141.

Жмуров Д. В. Кибервиктимология вымогательств в цифровом пространстве // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. № 2. С. 85–98.

Жмуров Д. В. Жертвы кибербуллинга: состояние проблемы // Российский следователь. 2023. № 1. С. 45–50.

Карпов К. Н. Квалификация вымогательства при угрозе распространения сведений о совершенном лицом правонарушении либо аморальном поступке // Современное право. 2018. № 5. С. 77–83.

Медведева А. С., Дозорцева Е. Г. Характеристики онлайн-груминга как вида сексуальной эксплуатации несовершеннолетних (по результатам анализа переписок взрослых и детей в сети Интернет) // Психология и право. 2019. Т. 9. № 4. С. 161–173.

Меньшагин В. Д., Пионтковский А. А. Курс советского уголовного права. Особенная часть. Т. 1. М., 1955. Насильственная преступность / под ред. В. Н. Кудрявцева и А. В. Наумова. М., 1997.

Подгайный А. М. К вопросу о понятии и формах криминального насилия над личностью // «Черные дыры» в российском законодательстве. 2006. № 4. С. 429–431.

Пособие по противодействию гендерному кибернасилию / ООН (UNWomenTurkey) // URL: <https://eca.unwomen.org/sites/default/files/Field%20Office%20ECA/Attachments/>.

Семенцова И. А., Фоменко А. И. Актуальные вопросы предупреждения преступлений, совершаемых лицами с расстройством сексуального предпочтения (педофилией) посредством сети Интернет // Теория и практика общественного развития. 2015. № 10. С. 90–93.

Яни П. С. Вопросы квалификации вымогательства // Законность. 2015. № 11. С. 40–45.

Anderson C. A., Bushman B. J., Donnerstein E., Hummer T. A., Warburton W. SPSSI Research Summary on Media Violence // Analyses of Social Issues and Public Policy. 2015. Vol. 15. Issue 1. P. 4–19.

Chatzakou D., Kourtellis N., Blackburn J., De Cristofaro E., Stringhini G., Vakali A. Mean birds: detecting aggression and bullying on Twitter // Proceedings of the ACM on Web Science Conference. Troy, New York, USA, 2017. P. 13–22.

⁵² URL: https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/a_safer_digital_environment_for_children.pdf.

REFERENCES

- A Guide to Countering Gender Cyber-Violence (UNWomenTurkey). Available at: <https://eca.unwomen.org/sites/default/files/Field%20Office%20ECA/Attachments/>.
- Alekseeva TS. Intimate images of a person as a subject of violation of privacy. *Criminal Law*. 2023;4:3-13. (In Russ.).
- Anderson CA, Bushman BJ, Donnerstein E, Hummer TA, Warburton W. SPSSI Research Summary on Media Violence. *Analyses of Social Issues and Public Policy*. 2015;15(1):4-19.
- Artyushina OV. Violent crime and IT technologies. *Lex russica*. 2019;9:77-84. (In Russ.).
- Barabash VV, Bordyugov GA, Kotelenets EA. Images of Russia in the world. Moscow; 2010. (In Russ.).
- Chatzakou D, Kourtellis N, Blackburn J, De Cristofaro E, Stringhini G, Vakali A. Mean birds: detecting aggression and bullying on Twitter. *Proceedings of the ACM on Web Science Conference*. 2017;13–22. Troy, New York; USA
- Delfino RA. Pornographic deepfakes: the next tragic act of the phenomenon of «revenge porn» and the need to adopt a criminal law at the federal level. *Actual Problems of Economics And Law*. 2020;14(1):105-141. (In Russ.).
- Gaukman LD. Combating violent assaults. Moscow; 1969. (In Russ.).
- Gaukman LD. Problems of the criminal legal struggle against violent crimes in the USSR. Noah IS ed.). Saratov; 1981. (In Russ.).
- Karpov KN. Qualification of extortion in the threat of disseminating information about an offense committed by a person or an immoral act. *Modern Law*. 2018;5:77-83. (In Russ.).
- Kudryavtseva VN, Naumova AV (eds.). Violent Crime. Moscow; 1997. (In Russ.).
- Medvedeva AS, Dozortseva EG. Characteristics of online grooming as a type of sexual exploitation of minors (based on an analysis of correspondence between adults and children on the Internet). *Psychology and Law*. 2019;9(4):161-173. (In Russ.).
- Menshagin VD, Piontkovsky AA. Course of Soviet criminal law. Special part. Vol. 1. Moscow; 1955. (In Russ.).
- Podgayny AM. The concept and forms of criminal violence against a person. *Black Holes in Russian Legislation*. 2006;4:429-431. (In Russ.).
- Sementsova IA, Fomenko AI. Topical issues of preventing crimes committed by persons with a sexual preference disorder (pedophilia) via the Internet. *Theory and Practice of Social Development*. 2015;10:15. (In Russ.).
- Yani PS. Issues of extortion qualification. *Zakonnost*. 2015;11:40-45. (In Russ.).
- Zhmurov DV. Cybervictimology of extortion in the digital space. *Asia-Pacific Region: Economics, Politics, Law*. 2021;2:85-98. (In Russ.).
- Zhmurov DV. Victims of cyberbullying: the state of the problem. *Russian Investigator*. 2023;1:45-50. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Сидоренко Элина Леонидовна, доктор юридических наук, доцент, профессор кафедры уголовного права, уголовного процесса и криминалистики МГИМО МИД России, директор Центра цифровой экономики и финансовых инноваций ИМИ МГИМО МИД России
д. 76, Вернадского пр., г. Москва 119454, Российская Федерация
12011979@list.ru

INFORMATION ABOUT THE AUTHOR

Elina L. Sidorenko, Dr. Sci. (Law), Associate Professor, Department of Criminal Law, Criminal Procedure and Criminalistics, MGIMO University; Director of the Center for Digital Economics and Financial Innovation; IMI MGIMO University, Moscow, Russian Federation
12011979@list.ru

Материал поступил в редакцию 13 февраля 2024 г.
Статья получена после рецензирования 20 ноября 2024 г.
Принята к печати 22 ноября 2024 г.

Received 13.02.2024.
Revised 20.11.2024.
Accepted 22.11.2024.