Научная статья **Research article**

УДК 316.77
https://doi.org/10.26907/2079-5912.2025.4.4–10

ОРИГИНАЛЬНАЯ СТАТЬЯ

Социальные практики цифровой девиации и факторы кибервиктимизации

Бакулина Р.А.

Казанский (Приволжский) федеральный университет
420008, Россия, Республика Татарстан, г. Казань, ул. Кремлевская, д.18, корп. 1

Аннотация. Статья посвящена анализу социальных практик цифровой девиации и факторов кибервиктимизации пользователей социальных сетей на основе эмпирического исследования, проведённого среди жителей Республики Татарстан. Цель работы заключается в выявлении практик и форм рискованных цифровых практик, а также в описании способов реагирования пользователей на мошеннические и агрессивные проявления в сетевой среде. Методологическую основу исследования составили социологические подходы к изучению цифровых коммуникаций, медиатизации повседневности и трансформации нормативного поведения в условиях анонимности. Эмпирическая база представлена результатами онлайн-анкетирования жителей Республики Татарстан (n=1864). Полученные результаты свидетельствуют о высокой степени вовлечённости пользователей в цифровые коммуникации и широком распространении рискованных и девиантных практик, связанных с анонимностью, агрессивным взаимодействием и использованием инструментов сокрытия цифровой идентичности. Отмечается также значительная распространённость опыта кибервиктимизации и низкий уровень обращаемости за институциональной помощью. Сделан вывод о формировании устойчивых моделей цифровой девиации и необходимости разработки комплексных профилактических мер, ориентированных на повышение цифровой грамотности и укрепление региональной системы цифровой безопасности.

Ключевые слова: цифровая девиация, кибервиктимизация, онлайн-коммуникации, интернет-мошенничество, цифровая безопасность

Благодарности. Исследование выполнено за счет средств субсидии, выделенной Казанскому федеральному университету для выполнения проекта № FZSM-2023-0022 «Цифровая социализация и цифровая компетентность молодежи в условиях глобальных системных изменений: технологии регулирования, риски, сценарии» в рамках государственного задания

Для цитирования: Бакулина Р.А. Социальные практики цифровой девиации и факторы кибервиктимизации. *Казанский социально-гуманитарный вестник.* 2025; (4(71)):4–10.

Digital Deviant Practices and Factors Contributing to Cybervictimization

Bakulina R.A.

Kazan Federal University, Kazan, 420008 Russia

Abstract. The article examines social practices of digital deviance and factors of cyber victimization among social media users based on an empirical study conducted among residents of the Republic of Tatarstan. The aim of the study is to identify typical patterns of online behavior and forms of risky digital practices, as well as to describe users' responses to fraudulent and aggressive manifestations in the online environment. The methodological framework of the research is grounded in sociological approaches to the study of digital communications and the mediatization of everyday life. The empirical basis is represented by the results of an online survey among residents of the Republic of Tatarstan (n=1864). The findings indicate a high level of user involvement in digital communications and a widespread prevalence of risky and deviant practices associated with anonymity, aggressive interaction, and the use of tools to conceal digital identity. The study also reveals a significant prevalence of cyber victimization experiences and a low level of обращения for institutional assistance. The results suggest the formation of stable patterns of digital deviance and highlight the need to develop comprehensive preventive measures aimed at enhancing digital literacy and strengthening regional digital security systems.

Keywords: digital deviance, cyber victimization, online communication, internet fraud, digital security

Acknowledgements. The paper was published at the expense of the subsidy allocated to Kazan Federal University for the project № FZSM-2023-0022 «Digital socialisation and digital competence of young people in the conditions of global systemic changes: regulation technologies, risks, scenarios» within the framework of the state assignment

For citation: Bakulina R.A. Digital Deviant Practices and Factors Contributing to Cybervictimization. *The Kazan Social and Humanitarian Bulletin.* 2025; (4(71)):4–10 (In Russ.)

Введение

Современное развитие цифрового общества сопровождается интенсивным внедрением сетевых технологий в ключевые сферы социальной жизни, что трансформирует коммуникационные практики [1, 2]. Расширение участия пользователей в цифровых коммуникациях способствует появлению новых моделей поведения, включая отклоняющиеся или потенциально рискованные [3]. Как показывают эмпирические исследования цифровой повседневности, высокая степень онлайн-вовлечённости формирует устойчивые поведенческие сценарии, нормализующие интенсивное и зачастую нерефлексируемое присутствие в сетевом пространстве [4].

Цифровая среда формирует качественно иную социальную реальность, где ослабевают традиционные механизмы нормативного регулирования и социального контроля. В исследованиях, посвящённых цифровой культуре и виртуальным коммуникациям, аналогичная мысль раскрывается через анализ изменения отношения пользователей к допустимости нарушений и снижению устойчивости

к девиантным практикам в условиях высокой анонимности и размывания границ приватности [1, 2, 5, 6]. Отмечается, что именно объективные свойства цифровой среды — анонимность, невидимость и опосредованность взаимодействия — усиливают склонность к девиантным и деструктивным формам поведения [7].

Вопросы регулирования поведения в цифровой среде анализируются и в правовом дискурсе. И.Р. Бегишев подчёркивает необходимость адаптации правовых норм к динамичному характеру цифровых технологий [3]. Цифровизация порождает новые объекты правового регулирования, не вписывающиеся в традиционные правовые конструкции, одновременно усиливая трансформацию информационной правосубъектности и актуализируя потребность в совершенствовании механизмов регулирования цифровой деятельности [8].

Проблема цифровой девиации носит универсальный характер и проявляется в различных социальных и культурных контекстах. Развитие онлайн-коммуникаций сопровождается переосмыслением норм взаимодействия и ослаблением механизмов социального контроля, особенно в условиях анонимности [9]. Исследования деструктивных онлайн-практик, включая кибербуллинг, показывают, что сниженная персональная ответственность является ключевым фактором вовлечения пользователей в агрессивное и девиантное поведение [7].

Актуальность изучения цифровой девиации обусловлена ростом числа пользователей социальных сетей, повышением распространённости мошеннических практик и деструктивной коммуникации [10], ослаблением институциональных механизмов контроля и наличием правовых пробелов в регулировании цифрового взаимодействия.

В рамках работы цифровая девиация понимается как совокупность устойчивых форм отклоняющегося поведения в сети – от использования фейковых аккаунтов и анонимизирующих инструментов до агрессивных высказываний, манипулятивных практик и участия в мошеннических схемах. Кибервиктимизация в исследовании трактуется как причинение вреда пользователю вследствие его участия в онлайн-взаимодействиях, включающее экономический, психологический и репутационный ущерб. **Цель исследования** – выявление форм рискованных цифровых практик и способов реагирования пользователей на мошеннические и агрессивные проявления в сетевой среде.

Материалы и методика исследования

Методологическая база исследования основана на социологических подходах к анализу цифровых коммуникаций и девиантных онлайн-практик, включая концепции медиатизации, цифровой социализации и трансформации нормативного поведения в условиях анонимности.

Исследование проведено методом онлайн-анкетирования, направленного на выявление особенностей цифрового поведения, восприятия рисков и опыта кибервиктимизации. В опросе приняли участие 1864 респондента – жителей Республики Татарстан; выборка формировалась с применением квотирования по полу и возрасту в соответствии с региональными статистическими данными. Анкетирование проводилось в период с февраля по мая 2025 года и включало тематические блоки, отражающие особенности использования социальных сетей, рискованные и девиантные цифровые практики, опыт столкновения с онлайн-угрозами, реакции на кибервиктимизацию, восприятие социальных

рисков и готовность к девиантному поведению в условиях анонимности. Для обработки данных использовались методы описательной статистики, анализ групповых различий и интерпретативный контент-анализ открытых ответов.

Результаты

Исследование выявило, что современные социальные сети выступают ключевым элементом структуры цифровой коммуникации, определяя как интенсивность, так и качество взаимодействий пользователей. Практически полная вовлечённость населения в цифровую среду – 97,4% респондентов зарегистрированы минимум в одной социальной сети – формирует основу для широкого спектра как конструктивных, так и девиантных онлайн-практик. Наиболее популярными платформами являются WhatsApp * (82,3%), YouTube (71,5%) и Instagram* (54,3%), Telegram (80%), ВКонтакте (72%). Причём доминирование мессенджеров подчеркивает смещение цифровых коммуникаций в сторону более приватных каналов, где анонимность становится важным фактором пользовательского поведения. Социальные сети активно используются в различных сферах повседневности: для общения их применяют 89% пользователей, для поиска информации и самообразования – 70%, для рабочих и учебных задач – до 60%. Существенная часть межличностного взаимодействия переносится в онлайн: у большинства пользователей объем цифровой коммуникации составляет 50-70%, а среди молодёжи – до 100%. Эти данные свидетельствуют, что цифровые практики глубоко проникают в повседневные социальные связи, размывая границы между личной, образовательной и профессиональной сферами.

Одновременно с ростом онлайн-активности усиливаются рискованные и девиантные формы поведения. Так, 24,4% респондентов имеют фейковые или альтернативные аккаунты, что свидетельствует о распространённости стратегий сокрытия личности или параллельного ведения нескольких виртуальных ролей. Цифровая агрессия также является заметным компонентом онлайн-коммуникации: 18,8 % пользователей признают опыт размещения негативных или оскорбительных комментариев, причём среди молодежи этот показатель выше (20,4%). Значительная часть пользователей осознанно стремится усиливать анонимность: 29% опрошенных используют VPN-сервисы, 17,1% – скрытые функции мессенджеров, 17% – анонимные браузеры. Доступ к нежелательным или нелегальным ресурсам также распространён: 30-35% посещают такие сайты время от времени, а 10% – регулярно. Подобные показатели указывают на снижение барьеров в отношении рискованных цифровых практик и рост нормализации поведения, ранее воспринимавшегося как отклоняющееся.

Цифровые угрозы, прежде всего мошенничество, занимают значимое место в опыте пользователей: почти половина респондентов – 44,6% – сталкивались с экономическими мошенническими схемами, 25,3% – с навязанными псевдоуслугами, 20,1% – с обманом при онлайн-покупках, а 18% – с телефонными и банковскими мошенническими операциями. Фишинг (форма онлайн-мошенничества, направленная на незаконное получение персональных или финансовых данных пользователей путём имитации доверенных цифровых источников) является наиболее массовой формой цифрового мошенничества: 44% сталкивались с ним через мессенджеры, 38,1% – через электронную почту. Реальная кибервиктимизация оказалась весьма высо-

* Принадлежит компании Meta, признанной экстремистской организацией и запрещенной на территории Российской Федерации

кой: 19,1% респондентов становились жертвами цифровых мошенников. Однако реакция пользователей на угрозы крайне сдержанная — 88% не обращались в правоохранительные органы, мотивируя это неверием в эффективность защиты, незначительностью ущерба или эмоциональными барьерами. При этом 62,9% не рассказывали о случившемся окружающим, что влияет на формирование высокого уровня латентности цифровых преступлений и препятствует борьбе с ними.

Восприятие угроз среди пользователей отражает комплекс ключевых проблем цифровой среды: злоупотребление персональными данными, распространение манипулятивного и ложного контента, онлайн-агрессия, преследование, навязчивые финансовые схемы. По мнению респондентов, распространённость цифровой девиации обусловлена низким уровнем цифровой грамотности, высокой анонимностью онлайн-среды и сложностью выявления нарушителей. Значительное влияние анонимности подтверждается тем, что 70,5% пользователей допускают возможность девиантных действий при безнаказанности, а высокая латентность цифровых инцидентов отражается в том, что 88% пострадавших не обращаются в официальные структуры. Экономическая привлекательность мошеннических практик также воспринимается как значимый фактор, учитывая, что с ними сталкивались 45% респондентов.

Важным показателем является отношение пользователей к собственному поведению: при условии полной безнаказанности 78,7% допускают вероятность совершить мошенничество, 68,8% – публично оскорбить другого пользователя, а 63,7% – создать ложный образ ради выгоды. Эти данные ярко демонстрируют влияние анонимности на снижение нормативных ограничений и ослабление механизмов самоконтроля.

Дискуссионные вопросы

Полученные результаты согласуются с выводами российских и зарубежных исследований, согласно которым цифровая среда трансформирует социальные связи, ослабляя традиционные механизмы нормативного контроля и способствуя нормализации девиантных практик. Как показывают работы М. Кастельса и Ш. Тёркл, сетевой характер коммуникаций и анонимность усиливают склонность к рискованному и агрессивному поведению, что подтверждается и данными настоящего исследования. Особый интерес представляет изучение практики использования потенциально опасных программ, например, таких как VPN-сервисы. Как пишут в исследованиях по теме цифровых навыков киберзащиты, вероятно, этот момент связан с когнитивным искажением, когда преимущества от применения нивелируют возможные угрозы [11].

Важным выводом является зависимость форм цифровой девиации от архитектуры и функционала платформ: смещение коммуникаций в мессенджеры и закрытые каналы сопровождается ростом приватности и снижением внешнего контроля. В этом контексте перспективным направлением дальнейших исследований является анализ новых мессенджерных экосистем, включая отечественный мессенджер MAX.

Заключение

Проведённое исследование позволило уточнить структуру цифровой девиации как совокупности устойчивых поведенческих практик, формирующихся в условиях сетевого взаимодействия. Цифровая среда выступает не просто каналом коммуникации, а автономным социальным пространством, в котором трансформируются механизмы нормативного регулирования, перераспределяется

ответственность и переосмысливаются границы допустимого поведения. В этом контексте девиантные практики становятся частью повседневных цифровых сценариев, а не исключительными формами отклонений.

Ключевым выводом является понимание цифровой девиации как динамического процесса, напрямую связанного с архитектурой платформ, уровнем анонимности и характером пользовательского взаимодействия. Высокая латентность кибервиктимизации и ограниченное использование институциональных механизмов защиты указывают на структурную уязвимость пользователей и воспроизводство цифровых рисков. Это требует перехода от фрагментарных мер к комплексной стратегии, объединяющей регулирование, просвещение и развитие субъектной ответственности в цифровой среде, что открывает перспективы дальнейших междисциплинарных исследований.

Список литературы / References

1. Кастельс М. Информационная эпоха: экономика, общество и культура. М.: ГУ ВШЭ, 2020. 608 с.

Castells M. The Information Age: Economy, Society and Culture. Moscow: HSE Publishing House, 2020. 608 p. (In Russ.)

2. Кириллова Н.Б. Медиасреда и цифровая культура: социальные трансформации XXI века. М.: Аспект Пресс, 2019. 248 с.

Kirillova N.B. Media environment and digital culture: social transformations of the 21st century. Moscow: Aspekt Press, 2019. 248 p. (In Russ.)

3. Бегишев И.Р. Международно-правовые основы регулирования искусственного интеллекта и робототехники. *Международное публичное и частное право*. 2021; (1):37–40.

Begishev I.R. International legal foundations for the regulation of artificial intelligence and robotics. *International Public and Private Law*. 2021; (1):37–40. (In Russ.)

4. Ефлова М.Ю., Максимова О.А., Нагматуллина Л.К. Практики активности российской молодежи в цифровой среде. *Казанский социально-гуманитарный вестник*. 2023; (6 (63)):59–70.

Eflova M.Yu., Maksimova O.A., Nagmatullina L.K. Practices of Russian youth activity in the digital environment. *Kazan Social and Humanitarian Bulletin*. 2023; (6 (63)):59–70. (In Russ.)

5. Чистякова Ю.С. Социология цифрового поведения: проблемы и перспективы исследования. *Социологические исследования*. 2021; (9):45–55.

Chistyakova Yu.S. Sociology of digital behavior: problems and research prospects. *Sociological Studies*. 2021; (9):45–55. (In Russ.)

6. Castells M. The Rise of the Network Society. Oxford: Blackwell, 2010. 597 p.

7. Дадаева Т.М., Ларихина Т.В. Отношение молодежи к деструктивным практикам в цифровом пространстве. *Society and Security Insights*. 2022; 5(4):108–125.

Dadaeva T. M., Larikhina T. V. Youth attitudes toward destructive practices in the digital space. *Society and Security Insights*. 2022; 5(4):108–125. (In Russ.)

8. Чубукова С. Г. Информационная правосубъектность: цифровая трансформация. *Информационное право*. 2019; (3 (61)):12–18.

Chubukova S. G. Informational legal personality: digital transformation. *Information Law*. 2019; (3 (61)):12–18. (In Russ.)

9. Turkle S. Alone Together: Why We Expect More from Technology and Less from Each Other. New York: Basic Books, 2017. 361 p.

10. Дугин А.Г. Социология виртуального пространства. М.: Академический проект, 2021. 320 с.

Dugin A.G. Sociology of virtual space. Moscow: Akademicheskiy proekt, 2021. 320 p. (In Russ.)

11. Lipatova A., Eflova M. Assessment of Digital Safety Skills as a Component of Media Competence of Young People in the Sustainable Development Context. Finance, Economics, and Industry for Sustainable Development (ESG 2024): Proceedings of the 5th International Scientific Conference on Sustainable Development, St. Petersburg. Cham: Springer Nature Switzerland AG, 2025:317-324.

Информация об авторе

Бакулина Регина Айдаровна, ассистент, аспирант кафедры общей и этнической социологии, Институт социально-философских наук и массовых коммуникаций, Казанский (Приволжский) федеральный университет. Author ID 1320963; ORCID ID 0009-0000-5875-0582, E-mail: riginii9@gmail.com

Information about author

Bakulina Regina Aidarovna, assistant, postgraduate student in the in the Department of General and Ethnic Sociology at the Institute of Social and Philosophical Sciences and Mass Communications of Kazan Federal University. Author ID 1320963; ORCID ID 0009-0000-5875-0582, E-mail: riginii9@gmail.com

Поступила в редакцию 15.10.2025; принята к публикации 01.12.2025.
Received 15.10.2025; Accepted 01.12.2025.