



## Защита частной жизни в виртуальной реальности: ответственность за использование дипфейк-контента в метавселенной<sup>1</sup>

**Ольга Алексеевна  
КУЗНЕЦОВА,**

главный научный сотрудник,  
заведующий кафедрой уголовного  
права, уголовного процесса  
и криминалистики  
Юридического института  
Российского университета  
дружбы народов  
имени Патриса Лумумбы,  
доктор юридических наук, доцент  
[kuznetsova-ola@rudn.ru](mailto:kuznetsova-ola@rudn.ru)  
117198, Россия, г. Москва,  
ул. Миклухо-Маклая, д. 6



**Мурад Мамедович  
МАДЖУМАЕВ,**

ведущий научный сотрудник,  
старший преподаватель кафедры  
уголовного права, уголовного  
процесса и криминалистики  
Юридического института  
Российского университета  
дружбы народов имени  
Патриса Лумумбы,  
кандидат юридических наук  
[madzhumaev-mm@rudn.ru](mailto:madzhumaev-mm@rudn.ru)  
117198, Россия, г. Москва,  
ул. Миклухо-Маклая, д. 6

**Аннотация.** *Метавселенная, представляющая собой иммерсивную и постоянную виртуальную среду, в сочетании с неправомерным использованием технологий искусственного интеллекта для создания гиперреалистичных синтетических медиаматериалов (фото, видео, аудио), образует новую категорию угроз для общественных отношений в сфере обеспечения неприкосновенности частной жизни.*

*Действующие нормативно-правовые механизмы, предназначенные в основном для регулирования взаимодействия в физической реальности и более ранних итерациях цифровой среды, недостаточно адаптированы для эффективного противодействия вызовам, возникающим в связи с созданием, использованием и распространением так называемых дипфейков (deepfakes). Именно применение этих технологий для формирования виртуальных аватаров (образов) людей в метавселенной представляет собой особенно сложную задачу. Представлен возможный механизм установления юридической ответственности, основанный на формальном признании комплекса «виртуальные права личности». Этот комплекс включает в себя право на аутентичность и контроль над собственным аватаром, право на подтверждение авторства и защиту от незаконного присвоения виртуальной личности, а также право на обеспечение целостности виртуальной среды субъекта. Предлагаемый подход также предусматривает необходимость разграничения юридической ответственности между субъектами, непосредственно создающими синтетические медиаматериалы с использованием машинного обучения, теми, кто осуществляет их последующее использование и распространение, и провайдером платформ метавселенной, обеспечивающими инфраструктуру для такого взаимодействия.*

**Ключевые слова:** *метавселенная, метапреступление, виртуальная реальность, дополненная реальность, виртуальный аватар, автономность виртуальной личности, цифровой двойник, машинное обучение, дипфейк, частная жизнь*

DOI: 10.17803/2311-5998.2025.129.5.244-253

© Кузнецова О. А.,  
Маджумаев М. М., 2025

<sup>1</sup> Исследование выполнено за счет гранта Российского научного фонда № 25-28-01478, <https://rscf.ru/project/25-28-01478/>.

**Olga A. KUZNETSOVA,**

Chief Researcher, Head of the Department  
of Criminal Law, Criminal Procedure, and Criminalistics  
of the Law Institute of the Patrice Lumumba Russian  
University of Peoples' Friendship,  
Dr. Sci. (Law), Associate Professor  
**kuznetsova-ola@rudn.ru**  
6, ul. Miklukho-Maklaya, Moscow, Russia, 117198

**Murad M. MAJUMAEV,**

Leading Researcher, Senior Lecturer at the Department  
of Criminal Law, Criminal Procedure and Criminalistics  
of the Patrice Lumumba Russian University of Peoples' Friendship,  
Cand. Sci. (Law)  
**madzhumaev-mm@rudn.ru**  
6, ul. Miklukho-Maklaya, Moscow, Russia, 117198

### **Protection of Privacy in Virtual Reality: Liability for the Use of Deepfake Content in the Metaverse**

**Abstract.** *The metaverse, as an immersive and persistent virtual environment, forms a new category of threat to public relations regarding privacy, when combined with the misuse of artificial intelligence technologies to create hyper-realistic synthetic media (photo, video, audio).*

*Existing legal frameworks, predominantly designed to regulate interaction in physical reality and earlier iterations of the digital environment, are not sufficiently adapted to effectively counteract the challenges posed by the creation, use and dissemination of so-called deepfakes. The application of these technologies to the formation of virtual avatars (images) of people in the metaverse presents a particularly complex regulatory challenge.*

*Presented is a possible mechanism for establishing legal liability based on the formal recognition of a set of "virtual personality rights". This complex includes the right to authenticity and control over one's own avatar, the right to confirm authorship and protection from misappropriation of virtual identity, as well as the right to ensure the integrity of the subject's virtual environment. The proposed approach also envisages the need to distinguish the legal responsibility between the actors who directly create synthetic media materials using machine learning, those who carry out their subsequent use and distribution, and the providers of metaverse platforms that deliver the infrastructure for such interaction.*

**Keywords:** *metaverse, metacrime, virtual reality, augmented reality, virtual avatar, autonomy of virtual personality, digital twin, machine learning, deepfake, privacy*



Современные тенденции развития общественных отношений сопряжены со стремительным распространением передовых вычислительных систем и цифровых (виртуальных) инфраструктур, способных в беспрецедентных масштабах перестроить существующие социально-экономические процессы. На фоне столь ускоренной научно-технической эволюции юриспруденция не может занимать позицию дисциплинарного изоляционизма. Необходима динамичная реконструкция устоявшихся нормативных рамок в целях обеспечения эффективного усвоения и практического применения инновационных достижений технических наук. Упущение таких интеграционных мер может представлять серьезную опасность: право окажется в непоправимом отрыве от складывающихся реалий и технологических парадигм, на которых строится взаимодействие внутри общества. Аналогичным образом сама траектория развития научно-технических инноваций требует соответствующего правового регулирования.

Показательным в этом отношении является метавселенная, представляющая собой формирующуюся систему взаимосвязанных виртуальных пространств, которая способна переосмыслить формы социального взаимодействия. Статистические показатели указывают на солидный оборот глобального рынка метавселенной, который в 2023 г. оценивался в 94,1 млрд долларов США при ежемесячной активной пользовательской базе в 400 млн человек, а к 2032 г. должен вырасти до 2 346,2 млрд долларов США<sup>2</sup>.

В то же время результаты проведенного исследования свидетельствуют о росте количества дипфейк-контента: в первом триместре 2025 г. в Российской Федерации был выявлен 61 такой уникальный контент и 2 300 копий, что на 65 % больше, чем за весь 2024 г., и в 2,6 раза больше, чем в 2023 г.<sup>3</sup> Все это лишний раз подтверждает необходимость тщательного изучения возможных форм социальных отношений в этих иммерсивных цифровых реальностях, в особенности с учетом использования изображений людей в метавселенной.

Метавселенная является гипотетической, следующей стадией развития сети Интернет, так называемой Web 3.0 или пространственной паутиной, которая характеризуется слиянием физической и цифровой реальностей, обеспечивая плавные переходы и взаимодействие между различными виртуальными пространствами<sup>4</sup>. Она представляет собой постоянную взаимосвязанную сеть общих трехмерных виртуальных пространств<sup>5</sup>. В этих пространствах пользователи, обычно представляемые фотографиями или другими графическими изображениями (аватарами), используемыми в учетной записи для их персонализации, могут синхронно взаимодействовать с окружающей средой, друг с другом

<sup>2</sup> Pangarkar T. Metaverse Statistics 2025 by New Technology in Virtual Space // Market.us Scoop. 2025. URL: <https://scoop.market.us/metaverse-statistics/> (дата обращения: 28.03.2025).

<sup>3</sup> Wave of deepfake fraud: how technology is changing the threat landscape // Global Fact-Checking Network (GFCN). 2025. URL: <https://globalfactchecking.com/wave-of-deepfake-fraud-how-technology-is-changing-the-threat-landscape/> (дата обращения: 09.04.2025).

<sup>4</sup> Kiaer J. Conversing in the Metaverse: The Embodied Future of Online Communication. Great Britain : Bloomsbury Publishing Plc, 2024. P. 6—12.

<sup>5</sup> Kiaer J. Op. cit. P. 6.

и программными агентами в режиме полного погружения<sup>6</sup>. Эти аватары служат цифровыми суррогатами, позволяя пользователям выразить свою индивидуальность, взаимодействовать с другими пользователями и ориентироваться в виртуальном мире. Уровень детализации и настройки аватаров на различных платформах метавселенной может варьироваться от стилизованных изображений до фотореалистичных.

Постоянство (устойчивость) метавселенной означает, что виртуальное пространство и цифровые активы в нем существуют непрерывно, независимо от того, активны (присутствуют) ли в нем отдельные пользователи<sup>7</sup>. В отличие от многих «традиционных» виртуальных пространств, таких как онлайн-игры или симуляторы, которые часто основаны на сессиях и прекращают свое существование (функционирование), как только пользователь отключается от сети, здесь «жизнь» продолжается и развивается независимо от присутствия или отсутствия (бездействия) отдельного пользователя.

Синхронность, с другой стороны, предполагает взаимодействие в реальном времени и совместный пользовательский опыт в метавселенной<sup>8</sup>.

Воплощенное цифровое присутствие является другой определяющей характеристикой метавселенной, относящейся к представлению пользователей через аватары в виртуальной среде, обеспечивая ощущение «присутствия». Чувство воплощенного присутствия усиливают такие технологии, как виртуальная реальность (VR), дополненная реальность (AR), смешанная реальность (MR), расширенная реальность (XR) и тактильные эффекты (haptics), которые обеспечивают визуальный, слуховой и тактильный опыт, способствующий ощущению «реального» пребывания в цифровом пространстве<sup>9</sup>. Так, гарнитуры VR позволяют полностью погрузить пользователя в виртуальную среду, при AR накладываются цифровые элементы на реальный мир, а MR объединяет обе реальности, позволяя взаимодействовать между виртуальными и физическими объектами.

По мере расширения деятельности индивидов в таких виртуальных пространствах формируется качественно новая форма криминальной активности, которую можно обозначить как метапреступление. Под ним следует понимать «любое преступление, объективная сторона которого частично или полностью совершается в виртуальной среде метавселенной»<sup>10</sup>.

Открывая новые перспективы, этот технологический рубеж одновременно порождает и новые правовые вызовы, прежде всего связанные с защитой частной жизни.

<sup>6</sup> *Mystakidis S.* Metaverse // Encyclopedia. 2022. Vol. 2. № 1. P. 491—493.

<sup>7</sup> *Mystakidis S.* Op. cit. P. 486.

<sup>8</sup> *Mystakidis S.* Op. cit. P. 488—489.

<sup>9</sup> *Murala D. K., Panda S. K.* The role of immersive reality (AR/VR/MR/XR) in metaverse. In *Metaverse and Immersive Technologies* (eds. A. Chandrashekhkar, S. H. Saheb, S. K. Panda, S. Balamurugan and S.-L. Peng). 2023. P. 159—189 ; *Pacchierotti C.* et al. Guest Editorial Haptics in the Metaverse: Haptic Feedback for Virtual, Augmented, Mixed, and eXtended Realities // *IEEE Transactions on Haptics*. 2024. Vol. 17. № 2. P. 122—128.

<sup>10</sup> *Seo S., Seok B., Lee C.* Digital forensic investigation framework for the metaverse // *Journal of Supercomputing*. 2023. Vol. 79. № 9. P. 9467—9468.



Обеспечение полного погружения (ощущения присутствия) является ключевой особенностью технологии виртуальной реальности и предполагает сбор, обработку и использование личной или семейной информации о пользователе. В основном эти данные требуются для создания реалистичной виртуальной среды, отслеживания взаимодействия с пользователем и персонализации опыта. Диапазон данных, собираемых в виртуальных средах, широк и многогранен и охватывает различные категории.

Собираются метаданные о пользователях, включая их профили, данные об использовании и аналитику, которые применяются для улучшения приложений с помощью A/B-тестирования и рекомендаций VR-контента<sup>11</sup>. Эта категория также может включать социально-демографическую информацию, предпочтения пользователей, интересы, время, проведенное в «среде», и паттерны взаимодействия, которые потенциально могут быть использованы для целевого развития и рекламы<sup>12</sup>. Даже IP-адреса могут собираться для целей модерации, например, для введения запретов на их основе<sup>13</sup>.

Помимо этого, осуществляется сбор физиологических данных о пользователях, причем виртуальные платформы и приложения потенциально могут собирать такие физические параметры, как рост и вес, для отслеживания физической формы<sup>14</sup>. Биометрические данные, в частности взгляд (изображение радужной оболочки глаза человека) и реакция лица, могут использоваться для организации рекламы и определения восприятия пользователями новых функций<sup>15</sup>.

При этом существует потенциальный риск использования таких данных, составляющих частную жизнь человека, без его согласия для регистрации аватара в метавселенной. В частности, распространены технологии, основанные на алгоритмах искусственного интеллекта (машинного обучения) для создания дипфейк-контента с использованием генеративных состязательных сетей (GAN) и диффузионных моделей. Они представляют собой возможность создания высокореалистичных искусственных (синтетических) цифровых материалов, способных модифицировать визуальный и аудиоконтент, что размывает границы между реальностью и «фабрикацией»<sup>16</sup>.

<sup>11</sup> *Abhinaya S. B. et al.* "What are they gonna do with my data?": Privacy Expectations, Concerns, and Behaviors in Virtual Reality // *Proceedings on Privacy Enhancing Technologies*. 2025. № 1. P. 62.

<sup>12</sup> *Chakraborty D. et al.* Use of metaverse in socializing: Application of the big five personality traits framework // *Psychology & Marketing*. 2023. Vol. 40. P. 10.

<sup>13</sup> *Chawki M., Basu S., Choi K. S.* Redefining boundaries in the Metaverse: navigating the challenges of virtual harm and user safety // *Laws*. 2024. Vol. 13. № 3. P. 33.

<sup>14</sup> *Lee J., Yoon H. K., Kim D.* Design of Metaverse-Based Physical Fitness Service for the Enhancement of Exercise Capability for Youth // *Mobile Information Systems*. 2023. № 1. P. 7272781.

<sup>15</sup> *Manna R., Singh A., Apte M.* Demystifying metaverse data from user-technology interaction // *Applied Marketing Analytics*. 2024. Vol. 9. № 4. P. 357—374.

<sup>16</sup> *Van der Sloot B.* Regulating the synthetic society: Generative AI, legal questions, and societal challenges. Great Britain : Bloomsbury Publishing Plc, 2024. P. 45—46.

Генеративные состязательные сети используют систему из двух нейронных сетей: генератора, который должен создавать искусственный (поддельный) контент, и дискриминатора, который пытается отличить настоящий контент от сгенерированного<sup>17</sup>. В ходе последовательного состязательного процесса генератор совершенствуется в создании синтетического контента, который может достаточно убедительно ввести в заблуждение дискриминатор, в результате чего получаются достаточно реалистичные подделки<sup>18</sup>. То есть генеративные состязательные сети используются для создания реалистичных фото-, видеоматериалов с заменой лица, голоса, в которых сходство одного человека плавно накладывается на фигуру (голос) другого, сохраняя убедительную мимику и движения.

Диффузионные модели работают путем преобразования простых распределений данных, таких как гауссовский шум, в сложные данные, которые выглядят очень похожими на реальные изображения или видео<sup>19</sup>. Используя технологию диффузии, пользователи могут манипулировать существующим медиаконтентом, например, частично изменять черты лица или полностью заменять лица людей, либо создавать совершенно новый образ несуществующих людей или объектов на основе текстовых описаний, как синтез сценариев, в которых люди говорят или делают то, чего они на самом деле никогда не говорили и не делали<sup>20</sup>.

Использование глубокого обучения для создания поддельных биометрических данных (информации, характеризующей физиологические и биологические особенности человека) представляет собой повышенную общественную опасность и нарушает неприкосновенность частной жизни. В метавселенной после получения биометрических данных пользователя его аватар, цифровые активы, социальные связи и цифровая (метавиртуальная) жизнь будут скомпрометированы самым деструктивным образом, чем в современной сети Интернет (киберсреде), поскольку большинство биометрических данных невозможно сбросить.

Действующие правовые механизмы (за исключением тех, которые направлены на регулирование цифровой (кибер) среды, отличающейся от метасреды, метавселенной), предназначенные в первую очередь для регулирования общественных отношений, возникающих в реальном (физическом) мире, не способны в полной мере противостоять уникальным вызовам, возникающим в результате дипфейков в иммерсивных виртуальных средах.

На сегодняшний день уже не раз предпринимались попытки уголовно-правового регулирования отдельных общественных отношений, возникающих в связи с совершением преступлений с использованием дипфейк-контента. В Государственную Думу внесена инициатива о введении уголовной ответственности за использование дипфейк-контента при совершении преступлений, предусмотренных ст. 128<sup>1</sup>, 158, 159, 159<sup>6</sup>, 165 УК РФ, с использованием изображения или голоса (в том числе поддельного или искусственно созданного) потерпевшего или иного лица, а также с использованием биометрических персональных данных

<sup>17</sup> Van der Sloot B. Op. cit. P. 45.

<sup>18</sup> Van der Sloot B. Op. cit. P. 45.

<sup>19</sup> Croitoru F. A. et al. Diffusion models in vision: A survey // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023. Vol. 45. № 9. P. 10851.

<sup>20</sup> Croitoru F. A. et al. Op. cit. P. 10851.



потерпевшего или иного лица<sup>21</sup>. Другой законодательной инициативой была предпринята попытка отнести использование технологий искусственного интеллекта при совершении преступления в целом к обстоятельствам, отягчающим наказание в связи с их повышенной общественной опасностью<sup>22</sup>.

Отсутствие нормативного обеспечения в метавселенной может создать условия, в которых злоумышленники смогут воспользоваться этими пробелами, что в итоге приведет к недостаточной защите интересов цифровой идентичности от противоправных действий и затруднит их уголовное преследование за ущерб, причиненный в результате использования дипфейков. Поэтому необходим принципиально новый комплексный подход к правовому регулированию метавселенной. Этот подход должен основываться на признании возникающих прав, характерных для виртуальной среды, и установлении обязанностей, которые должны быть надлежащим образом выверены в рамках разнообразных экосистем метавселенной.

В этой связи представляется целесообразным предложить идею признания целостности и автономности виртуальной личности, т.е. признания, что цифровое представление человека в метавселенной, включая выбранный им аватар и связанные с ним биометрические и поведенческие данные, является продолжением его личности в реальной (физической) действительности. Здесь признается важность виртуального присутствия человека, все более погружающегося в цифровой мир, для его самовыражения и взаимодействия с другими членами общества<sup>23</sup>. При этом для обеспечения защиты такой виртуальной идентичности необходимо реализовать ряд основных (мета)прав.

Во-первых, это право на аутентичность и контроль аватара<sup>24</sup>, которое подразумевает исключительную прерогативу индивида определять форму и характеристики своего основного виртуального образа в метавселенной. Это право является основополагающим для развития чувства собственности и контроля над своим виртуальным «я». Несанкционированное создание или размещение практически аналогичного аватара, особенно если он используется в контексте, который может быть обоснованно воспринят как представление человека или его мнения, будет являться нарушением этого права. Технологии дипфейк значительно повышают угрозу этому праву, позволяя неправомерно имитировать аватар человека путем манипулирования биометрическими и поведенческими данными, на основе которых формируются движения, мимика и голосовые сигналы аватара.

<sup>21</sup> Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности)» // URL: [https://sozd.duma.gov.ru/bill/718538-8#bh\\_histras](https://sozd.duma.gov.ru/bill/718538-8#bh_histras) (дата обращения: 11.04.2025).

<sup>22</sup> Законопроект № 885494-8. В архиве. «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации» // URL: <https://sozd.duma.gov.ru/bill/885494-8> (дата обращения: 11.04.2025).

<sup>23</sup> Безгодова С. А., Микляева А. В. Цифровые трансформации психологии человека : учебное пособие / под ред. А. В. Микляевой. СПб. : Издательство РГПУ имени А. И. Герцена, 2023. С. 5.

<sup>24</sup> Cheong B. C. Avatars in the metaverse: potential legal issues and remedies // *International Cybersecurity Law Review*. 2022. Vol. 3. № 2. P. 467—494.

Это право вписывается в общую тенденцию признания важности виртуальной идентичности как фундаментального компонента человеческого существования в цифровую эпоху. В то же время пользователи должны иметь возможность управлять и контролировать свои виртуальные образы. Появление технологий искусственного манипулирования медиаконтентом напрямую обуславливает необходимость правовой защиты от несанкционированного использования своего виртуального образа.

Следующее право — на утверждение авторства и предотвращение незаконного присвоения виртуальной личности<sup>25</sup> — предполагает, что любые виртуальные действия, заявления или выступления, приписываемые аватару человека, действительно являются его собственными. Создание и распространение поддельного контента, который ложно приписывает действия или высказывания аватару, тем самым искажая намерения или поведение человека в метавселенной, должно рассматриваться как нарушение этого права. Таким образом, признается возможность значительного репутационного ущерба и психических страданий, которые могут быть вызваны такими цифровыми искажениями.

Кроме того, следует признать, что право на целостность виртуальной среды<sup>26</sup>, окружающей человека, определяет его заинтересованность в том, чтобы это пространство было свободно от вредоносного поддельного контента, который непосредственно направлен на его аватар или выдает себя за него, представляя собой преследование, клевету или причинение иного вреда. Иммерсивный характер среды виртуальной реальности может значительно усилить последствия таких нарушений по сравнению с «традиционными» онлайн-платформами. Это право подчеркивает необходимость создания безопасной и надежной виртуальной среды, в которой люди могут взаимодействовать, не опасаясь криминального подражания или целенаправленного преследования. Проактивные меры по предотвращению создания и распространения таких вредоносных имитаций крайне важны, поскольку их последствия в иммерсивных средах могут быть весьма серьезными.

Ответственность за потенциальные посягательства на частную жизнь в метавселенной должна быть дифференцирована в отношении тех, кто создал и (или) использовал дипфейк-контент, или вовлеченных в процесс субъектов:

Вменяемые физические лица (авторы дипфейк-контента), намеренно создающие синтетический материал с использованием глубокого обучения с целью причинения вреда третьим лицам в метавселенной, должны нести ответственность на общих условиях. Эта ответственность должна распространяться как на создание, так и на первоначальное распространение такого материала.

Вменяемые физические лица, которые сознательно распространяют вредоносный дипфейк-контент, созданный другими в метавселенной, также должны нести ответственность. Степень ответственности может варьироваться в зависимости от их участия в совершении преступления.

Также можно рассмотреть вопрос об ответственности провайдеров платформ метавселенной за непринятие необходимых мер для предотвращения создания и

<sup>25</sup> Cheong B. C. Op. cit. P. 477—478.

<sup>26</sup> Cheong B. C. Op. cit. P. 475—477.



распространения вредоносного дипфейк-контента на своих платформах. К таким мерам могут относиться разработка и внедрение технологий для обнаружения дипфейк-контента, создание четких руководящих принципов сообщества, запрещающих создание, использование и распространение дипфейк-контента, а также предоставление пользователям механизмов для сообщения и получения компенсации за причиненный вред.

Принципы виртуальной аутентичности, алгоритмической подотчетности и распределенной ответственности образуют устойчивую основу для формирования нового подхода к решению вопросов, связанных с созданием, использованием и распространением фальшивого, поддельного контента в метавселенной.

При таком подходе, когда устанавливаются четкие права, связанные с целостностью и автономией виртуальной личности, на провайдеров платформ возлагается ответственность за проактивное обнаружение, аутентификацию и модерацию контента, а также устанавливается ответственность для участников оборота дипфейк-контента в зависимости от их намерений и действий (бездействия), представляет собой комплексную стратегию для построения доверия и аутентичности в виртуальной среде метавселенной.

Невозможно переоценить важность технологической совместимости и стандартизированной аутентификации, поскольку эти меры имеют решающее значение для практической реализации и обеспечения соблюдения любых правовых рамок. Наконец, постоянная потребность в междисциплинарных исследованиях и разработке адаптивных правовых механизмов обеспечит эффективное регулирование быстро развивающейся технологической среды метавселенной.

Принятие такого многоуровневого и принципиального подхода позволит реализовать видение метавселенной как пространства доверия, подлинности и ответственного виртуального взаимодействия.

## БИБЛИОГРАФИЯ

1. *Безгодова С. А., Микляева А. В.* Цифровые трансформации психологии человека : учебное пособие / под ред. А. В. Микляевой. — СПб. : Издательство РГПУ имени А. И. Герцена, 2023.
2. *Abhinaya S. B. et al.* “What are they gonna do with my data?”: Privacy Expectations, Concerns, and Behaviors in Virtual Reality // *Proceedings on Privacy Enhancing Technologies*. — 2025. — № 1.
3. *Chakraborty D. et al.* Use of metaverse in socializing: Application of the big five personality traits framework // *Psychology & Marketing*. — 2023. — Vol. 40.
4. *Chawki M., Basu S., Choi K. S.* Redefining boundaries in the Metaverse: navigating the challenges of virtual harm and user safety // *Laws*. — 2024. — Vol. 13. — № 3.
5. *Cheong B. C.* Avatars in the metaverse: potential legal issues and remedies // *International Cybersecurity Law Review*. — 2022. — Vol. 3. — № 2. — P. 467—494.
6. *Croitoru F. A. et al.* Diffusion models in vision: A survey // *IEEE Transactions on Pattern Analysis and Machine Intelligence*. — 2023. — Vol. 45. — № 9.

7. *Kiaer J.* Conversing in the Metaverse: The Embodied Future of Online Communication. — Great Britain : Bloomsbury Publishing Plc, 2024. — P. 6—12.
8. *Lee J., Yoon H. K., Kim D.* Design of Metaverse-Based Physical Fitness Service for the Enhancement of Exercise Capability for Youth // *Mobile Information Systems*. — 2023. — № 1.
9. *Manna R., Singh A., Apte M.* Demystifying metaverse data from user-technology interaction // *Applied Marketing Analytics*. — 2024. — Vol. 9. — № 4. — P. 357—374.
10. *Murala D. K., Panda S. K.* The role of immersive reality (AR/VR/MR/XR) in metaverse. In *Metaverse and Immersive Technologies* (eds. A. Chandrashekhara, S. H. Saheb, S. K. Panda, S. Balamurugan and S.-L. Peng). — 2023. — P. 159—189.
11. *Mystakidis S.* Metaverse // *Encyclopedia*. — 2022. — Vol. 2. — № 1. — P. 491—493.
12. *Pacchierotti C. et al.* Guest Editorial Haptics in the Metaverse: Haptic Feedback for Virtual, Augmented, Mixed, and eXtended Realities // *IEEE Transactions on Haptics*. — 2024. — Vol. 17. — № 2. — P. 122—128.
13. *Pangarkar T.* Metaverse Statistics 2025 By New Technology in Virtual Space // *Market.us Scoop*. — 2025. — URL: <https://scoop.market.us/metaverse-statistics/> (дата обращения: 28.03.2025).
14. *Seo S., Seok B., Lee C.* Digital forensic investigation framework for the metaverse // *Journal of Supercomputing*. — 2023. — Vol. 79. — № 9. — P. 9467—9468.
15. *Van der Sloot B.* Regulating the synthetic society: Generative AI, legal questions, and societal challenges. — Great Britain : Bloomsbury Publishing Plc, 2024. — P. 45—46.
16. Wave of deepfake fraud: how technology is changing the threat landscape // *Global Fact-Checking Network (GFCN)*. — 2025. — URL: <https://globalfactchecking.com/wave-of-deepfake-fraud-how-technology-is-changing-the-threat-landscape/> (дата обращения: 09.04.2025).