**Научная статья**
**https://doi.org/10.34853/NH.2026.13.11.003**



**УДК 316; 122/129**

**Зейналов Гусейн Гардаш Оглы**
доктор философских наук, профессор, профессор кафедры права и философии,
Мордовский государственный педагогический университет имени М.Е. Евсевьева,
e-mail: zggo@mail.ru.
**Виноградова Ирина Борисовна**
кандидат философских наук, доцент кафедры права и философии,
Мордовский государственный педагогический университет имени М.Е. Евсевьева,
e-mail: virene82@mail.ru.
**Еремкин Никита Вячеславович**
аспирант кафедры права и философии,
Мордовский государственный педагогический университет имени М.Е. Евсевьева,
e-mail: nickita.eremkin@yandex.ru
**Huseyn G. Zeynalov**
Doctor of Philosophy, Professor, Professor of the Department of Law and Philosophy, Mordovian State Pedagogical University named after M.E. Evseviev,
e-mail: zggo@mail.ru.
**Irina B. Vinogradova**
Candidate of Philosophical Sciences, Associate Professor of the Department of Law and Philosophy,
Mordovian State Pedagogical University named after M.E. Evseviev,
e-mail: virene82@mail.ru.
**Nikita V. Eremkin**
Postgraduate student of the Department of Law and Philosophy,
Mordovian State Pedagogical University named after M.E. Evseviev,
e-mail: nickita.eremkin@yandex.ru

# ПРОБЛЕМЫ БЕЗОПАСНОСТИ СМЕШАННОЙ ОБЪЕКТИВНО-ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

# SECURITY PROBLEMS OF MIXED OBJECTIVE-VIRTUAL REALITY

***Аннотация.*** *В статье проблема безопасности рассматривается в контексте новой смешанной социокультурной реальности объективно-виртуального характера. Отмечается, что она сочетает в себе цифровые и реальные настройки мира. В рамках социального бытия современного человека в новой реальности преобладает технологическое составляющее. Новая гибридная реальность превращается в технологическую платформу и требует формирования новой модели безопасности гибридного типа. Характерной чертой этой модели становятся технологизация безопасности на общекультурном уровне. В контексте осмысления новой модели безопасности проводится анализ кибербезопасности. Она сочетает в себе физические и виртуальные сегменты. Выделяются такие направления кибербезопасности как угроза конфиденциальности информации, угроза целостности системы и угроза доступности, что затрагивает физическую составляющую смешанной реальности. Так как основное социокультурное бытие человека проходит в рамках виртуальной реальности и совершается в информационном формате, то информационная составляющая безопасного бытия культуры в смешанной объективно-виртуальной реальности обретает практически абсолютный характер. Учитывая угрозы, которые связаны с применением технологий смешанной реальности, авторы предлагают комплексный подход при решении проблем безопасности. По мнению авторов, развитие технологий смешанной объективно-виртуальной реальности носит стремительный характер. Соответственно, наряду с технологическими мерами, возникают и проблемы на уровне правовых основ обеспечения безопасности. Правовые вопросы оказываются непроработанными до конца. Регулирование правовых вопросов часто содержит в себе этические аспекты индивидуального характера, связанные с непосредственным взаимодействием пользователя с подобной технологией.*

***Ключевые слова:*** *смешанная объективно-виртуальная реальность, технологизация безопасности, гибридная модель безопасности, информационные угрозы, этические и правовые аспекты безопасности*

***Abstract.*** *The article considers the security problem in the context of a new mixed socio-cultural reality of an objective-virtual nature. It is noted that it combines digital and real settings of the world. Within the framework of the social existence of a modern person in the new reality, the technological component prevails. The new hybrid reality is turning*

*into a technological platform and requires the formation of a new hybrid security model. A characteristic feature of this model is the technologization of security at the general cultural level. In the context of understanding the new security model, the analysis of cybersecurity is carried out. It combines physical and virtual segments. Such areas of cybersecurity as a threat to information confidentiality, a threat to system integrity and a threat to accessibility are distinguished, which affect the physical component of mixed reality. Since the main socio-cultural existence of a person takes place within the framework of virtual reality and is carried out in an information format, the information component of the safe existence of culture in a mixed objective-virtual reality acquires an almost absolute character. Considering the threats associated with the use of mixed reality technologies, the authors propose an integrated approach to solving security problems. According to the authors, the development of mixed objective-virtual reality technologies is rapid. Accordingly, along with technological measures, problems arise at the level of legal foundations for ensuring security. Legal issues are not fully worked out. The regulation of legal issues often contains ethical aspects of an individual nature related to the direct interaction of the user with such technology.*

***Keywords:*** *mixed objective-virtual reality, security technologization, hybrid security model, information threats, ethical and legal aspects of security.*

Бытие современного человека больше всего проходит в пространстве смешанной (гибридной) объективно-виртуальной реальности (СОВР). Смешанная реальность складывается в результате применения технологий виртуальной реальности (VR), расширенной (или дополненной) реальности (AR) и смешанной реальности (MR). Поэтому она – зона постоянной нестабильности и неопределенности, изменчивости и опасности. В нашем понимании, смешанная объективно-виртуальная реальность является в широком смысле общим названием той искусственной реальности, которая возникает как результат наложения или сосуществования элементов предметного мира и технологий VR, AR, MR реальностей [2]. Благодаря этим технологиям цифровые объекты могут быть введены в реальный физический мир человека и/или наоборот. Вследствие чего возникает новое расширенное культурное пространство бытия человека [5], где в основном проистекает его деятельность в сфере экономики, культуры, политики и т.д. В первую очередь, благодаря технологиям смешанной объективно-виртуальной реальности автоматизируются и оптимизируются многие социальные, производственные и культурные процессы. Вся эта деятельность отличается от классических моделей деятельности тем, что имеет информационно-виртуальный формат исполнения.

В новой реальности человеку все больше приходится иметь отношение с информационными продуктами. В этом есть ряд преимуществ, также имеются опасности. Отсюда и вытекает актуализация информационной составляющей безопасного бытия культуры. Первостепенные проблемы безопасности связаны с применением информационно-компьютерных технологий и развитостью технологической культуры на личностном уровне [1]. В таком случае, новая гибридная (смешанная) реальность превращается в технологическую платформу и требует формирования модели безопасности гибридного типа, сочетающей в себе физическо-предметные и виртуально-информационные сегменты.

Новая модель безопасности разрабатывается на протяжении последних десятилетий с учетом технических возможностей информационно-компьютерных технологий. Отечественный социолог В.Н. Кузнецов считает, что «Безопасность становится обязательной предпосылкой целесообразного развития и сохранения базовых ценностей и традиций народов, нормальных отношений личности и государства, способности эффективно предотвращать и преодолевать угрозы внешней среды» [4, с.143].

Как было отмечено, смешанная объективно-виртуальная реальность (MR) по своей природе несет в себе ряд проблем в плане безопасности технологического характера, требующего внимания. Важнейшей из них для нашей эпохи становится кибербезопасность. Кибербезопасность включает в себя различные направления, по которым необходимо проводить работу для предоставления необходимого уровня защиты. Мы можем выделить три угрозы, которые наиболее актуальны для обеспечения безопасности в смешанной объективно-виртуальной реальности:

- *угроза конфиденциальности*: при использовании технологий СОВР необходимо учитывать вероятность на возможные риски относительно целостности персональных данных и биометрии (при её наличии в системе). Так, даже электронная подпись организации необходимая для документооборота как внутри, так и для внешних сделок, может подвергаться риску. Если подобного рода информация попадёт в руки злоумышленников, она может быть использована для мошенничества и конкурентного манипулирования или для совершения других преступных действий;
- *угроза целостности*: подразумевается, что обрабатываемая и подгружаемая информация с помощью технологий СОВР может стать целью для внедрения вредоносных данных, а также изменения контента. Примером такой угрозы можно назвать феномен DeepFake, развившийся благодаря обучению ИИ-технологий, который представляет собой создание копии личности человека (видео-, фото- и аудио- составляющая) с целью получения мошеннической и преступной выгоды, а также манипулирования и запугивания пользователя. Подобные угрозы могут ввести в заблуждение, а также нарушают целостность действующей системы;

- *угроза доступности*: затрагивается физическая составляющая СОВР, поскольку интеграция происходит за счет каких-либо конкретных технологий (устройства ввода, очки виртуальной реальности и пр.). Такого рода устройства могут быть уязвимы для хакерских атак, что впоследствии может привести к получению злоумышленниками доступа к данным и удалённого контроля над устройством.

Как мы заметили, кибербезопасность в контексте СОВР является неотъемлемой составляющей социальной безопасности, поскольку при использовании подобных технологий в финансовой сфере (виртуальная валюта, мобильные платежи, цифровые карты) есть вероятность использования этих технологий в качестве канала для извлечения информации преступниками в киберпространстве.

Стоит также подчеркнуть опасность феномена Deepfake, наиболее важного, на наш взгляд, среди остальных уязвимостей СОВР. Deepfake (англ. «глубокий обман») представляет собой технологию по созданию правдоподобного контента, который на самом деле не соотносится с реальностью (например, изображения, видео с определенными людьми). Развитие нейросетей и ИИ-технологий значительно упростило деятельность человека, но вместе с тем это повлекло за собой множество потенциальных угроз. Так, основная проблема использования Deepfake в контексте безопасности в рамках СОВР заключается в том, что злоумышленник имеет немало возможностей навредить системе: подменить лица людей в реальном времени, распространить дезинформацию, а также нарушить конфиденциальность [7].

Следующей немаловажной проблемой безопасности является проблема идентификации и аутентификации в системах смешанной объективно-виртуальной реальности. Ранее уже упоминалось использование биометрических материалов. В контексте данной темы все угрозы и риски, связанные с СОВР взаимосвязаны между собой, а потому требуют столь детального анализа [3]. Так, технологии по идентификации и аутентификации направлены на устранение или снижение риска возникновения угрозы. Они требуют надежных методов работы, поскольку их функция строится на подтверждении личности пользователей и их действий в виртуальной среде. Необходимо контролировать основные аспекты, включая биометрию, распознавание голосов и лиц.

В качестве метода аутентификации в настоящее время большой известностью и практичностью пользуется именно биометрия из-за своей удобности и относительной надежности. В биометрические данные обычно принято относить отпечатки пальцев, распознавание лиц и сетчатки глаза. Однако, несмотря на распространённую практику использования биометрии (например, подтверждение личности при оплате на кассе – внедрённая Сбером функция «оплата улыбкой» пришедшая в 2023 году в качестве альтернативы Google Pay и Apple Pay), существует отдельный серьёзный вид угрозы в этом направлении.

Подделка биометрических данных как угроза безопасности в СОВР существует достаточно давно. За этим явлением закрепился термин «спуфинг» (англ. «spoofing» – подмена). Данный факт стал глобальной угрозой для бизнеса и других элементов социальной системы. Спуфинг, как явление, может наносить серьезный урон предпринимателям и государственным органам. Зачастую спуфинг можно спутать с DeepFake, но во втором случае отмечается, что это относительно новый вид угроз, поскольку развитие ИИ-технологий пришлось на последние пять лет, а риски, касаемые биометрии, существуют намного дольше [6]. Однако и то, и другое может нести одинаковую опасность для безопасности данных личности. Так, в России участились случаи спуфинг-атак через мессенджер Telegram. Схема действия спуфинга в данном случае следующая – мошенники создают поддельные аккаунты, например, руководителей организации или её сотрудников для возможности получить доступ к конфиденциальным данным и провести несанкционированные денежные переводы [3].

В качестве решения проблемы угрозы спуфинг-атак, которым подвержены большинство биометрических систем, можно внедрять и использовать дополнительные меры защиты, однако это требует дополнительных технологий и квалифицированных кадров для поддержания устойчивости и надежности систем.

Также важной проблемой на пути обеспечения безопасности СОВР являются этические и правовые аспекты безопасности. Поскольку существует неопределенность в нормативной базе регулирования действия СОВР, необходима качественная проработка всех аспектов. Ввиду того, что смешанная объективно-виртуальная реальность на уровне технологий развивается стремительно, а правовая основа, которая должна регулировать её использование, зачастую до конца не проработана. Специалисты в данной области не успевают совершенствовать правовую систему из-за ускоренного развития технологических составляющих. Отсутствие законодательно установленных норм, регулирующих действия в рамках современных технологий СОВР, также усложняет условия обеспечения их безопасность, что является косвенной причиной вероятных проблем в защите системы индивидуальных и коллективных данных.

По-прежнему одной из проблем также остается согласие самих пользователей на применение технологий смешанной объективно-виртуальной реальности для обеспечения безопасности. Взаимодействие с подобного рода технологией содержит в себе во многом вопросы этического аспекта. Поскольку зачастую люди, использующие технологий СОВР, не до конца понимают, на что они дают своё согласие при принятии правил использования. При определенных ситуациях возможно возникновение обстоятельств, когда человек может под давлением согласиться с условиями, которые бы не принял самостоятельно. Такие ситуации могут вызывать этические и правовые споры

по использованию элементов СОВР в целом.

Обращая внимание на угрозы, которые связаны с непосредственным взаимодействием пользователей с такими технологиями, необходимо внедрять и использовать комплексный подход, который будет включать в себя как правовые, этические составляющие, так и технологические меры. В данном случае следует пересмотреть возможные рекомендации, которые, в целом, могут повысить безопасность современных технологий СОВР во многих аспектах.

Итак, с развитием СОВР классическую модель безопасности можно считать устаревшей. Технологизация объективно-виртуального бытия превращает ее в ведущую глобальную проблему общекультурного характера. Требуются радикальные перестановки в системе безопасности. Наиболее очевидным является пересмотр ее социально-философских основ с учетом двойственности ее онтологической природы: высоко-технологичности и информационно-виртуальности, а также решение сопутствующих ее динамике правовых и этических вопросов. Проведенный анализ не дает готовых решений, но обозначает векторы исследований, в рамках которых кибербезопасность выступает основным условием существования современного общества.

**Список литературы**


1. Зейналов Г.Г. Смешанная объективно-виртуальная реальность как технологическая платформа развития современного образования // Alma mater (Вестник высшей школы) : научно-методический журнал. 2019. № 10. С. 33–37.
2. Зейналов Г.Г., Захитова О.Г. Проблема безопасности в пространстве смешанной объективно-виртуальной реальности // Безопасность в условиях глобализации мира : Материалы Национальной научной конференции, посвященной 75-летию со дня рождения первого президента Калмыцкого государственного университета, профессора Германа Манджиевича Борликова. Редколлегия: Б.К. Салаев, В.А Эвиев [и др.]. Элиста, 2019. С. 31–34.
3. Иванова А.В. Технологии виртуальной и дополненной реальности: возможности и препятствия применения // Стратегические решения и риск-менеджмент. 2018. №3 (108). URL: https://cyberleninka.ru/article/n/tehnologii-virtualnoy-i-dopolnennoy-realnosti-vozmozhnosti-i-prepyatstviya-primeneniya (дата обращения: 09.06.2025).
4. Кузнецов В.Н. Социология безопасности : учебное пособие для студентов высших учебных заведений, обучающихся по специальности 040200 «Социология»; Московский гос. ун-т им. М. В. Ломоносова, Социологический фак. Москва : Книжный дом Университет, 2009. 422 с.
5. Маклюэн Г.М. Понимание медиа: внешние расширения человека / Пер. с англ. В. Николаева; Закл. ст. М. Вавилова. М.: Жуковский: Какон-пресс-Ц; Кучково поле, 2003. 464 с.
6. Спуфинг и дипфейки: бизнес под прицелом. Исследование MTS AI и Б1. URL: https://mts.ai/ru/tehnologii/research-on-the-impact-of-spoofing/(дата обращения: 09.06.2025).
7. Солдатова Г.У., Вишнева А.Е. Особенности развития когнитивной сферы у детей с разной онлайн-активностью: есть ли золотая середина? // Консультативная психология и психотерапия. 2019. Т. 27. № 3. С. 97–118.


**References**


1. Zeynalov G.G. Mixed objective-virtual reality as a technological platform for development of modern education // Alma mater (Higher School Bulletin): scientific and methodological journal. 2019. No. 10. pp. 33–37.
2. Zeynalov G.G., Zakhitova O.G. The problem of security in the space of mixed objective-virtual reality // Security in the context of a globalizing world: Proceedings of the National Scientific Conference dedicated to the 75th anniversary of the birth of the first president of Kalmyk State University, professor German Mandzhievich Borlikov. Editorial board: B.K. Salaev, V.A. Eviev [et al.]. Elista, 2019. pp. 31–34.
3. Ivanova A.V. Virtual and augmented reality technologies: opportunities and obstacles to application // Strategic decisions and risk management. 2018. No. 3 (108). URL: https://cyberleninka.ru/article/n/tehnologii-virtualnoy-i-dopolnennoy-realnosti-vozmozhnosti-i-prepatstviya-primeneniya (accessed: 06/09/2025).
4. Kuznetsov V.N. Sociology of Security: a textbook for students of higher educational institutions studying in the specialty 040200 “Sociology”; Moscow State University named after M.V. Lomonosov, Faculty of Sociology. Moscow: University Book House, 2009. 422 p.
5. McLuhan H.M. Understanding Media: Human External Extensions / Translated from English by V. Nikolaev; Concluding Article by M. Vavilov. Moscow: Zhukovsky: Kakon-press-Ts; Kuchkovo fuild, 2003. 464 p.
6. Spoofing and deepfakes: Business under fire. MTS AI and B1 Research. URL: https://mts.ai/ru/tehnologii/research-on-the-impact-of-spoofing/ (accessed: 09.06.2025).
7. Soldatova G.U., Vishneva A.E. Features of the development of the cognitive sphere in children with different online activity: is there a golden mean? // Counseling Psychology and Psychotherapy. 2019. Vol. 27. No. 3. P. 97–118.