

ТРИБУНА МОЛОДОГО УЧЕНОГО

TRIBUNE FOR YOUNG SCIENTISTS

Original article
УДК 349:004
DOI 10.33184/pravgos-2025.3.14

Научная статья

ДОЛУНЦ Вартан Сурикович
Московский государственный юридический
университет имени О.Е. Кутафина (МГЮА),
Москва, Россия,
vartan.dolunts@gmail.com

DOLUNTS Vartan Surikovich
Kutafin Moscow State Law University (MSAL),
Moscow, Russia

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ КАК ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ: СУЩНОСТЬ, УГРОЗЫ И МЕХАНИЗМЫ ЗАЩИТЫ

VIRTUAL REALITY AS AN OBJECT OF LEGAL REGULATION: THE ESSENCE, THREATS AND
PROTECTION MECHANISMS

Аннотация. В связи с развитием технологий виртуальной реальности актуальной задачей является разработка механизмов, направленных на защиту пользователей от потенциальных информационных угроз. В условиях трансграничности отношений в виртуальной реальности, технологической зависимости России от зарубежных стран, низкого уровня знаний у граждан в сфере информационной безопасности указанная задача становится особенно важной. Цель: выявление особенностей правового регулирования и разработка механизмов защиты пользователей виртуальной реальности с учетом специфики данной технологии и актуальных вызовов. В исследовании применялись методы системного анализа – для комплексного осмысления правовой природы виртуальной реальности, сравнительно-правового анализа – для сопоставления отечественного и зарубежного законодательства и правоприменительной практики, синтеза – для обобщения полученных теоретических и эмпирических данных с целью формирования авторской концепции правового регулирования, правового моделирования – для разработки предложений по совершенствованию действующего законодательства и формированию эффективных механизмов защиты пользователей виртуальной реальности. Результаты: предложена авторская концепция соотношения понятий «виртуальная реальность», «виртуальный мир» и «виртуальная среда», в соответствии с которой понятие «виртуальная реальность»

Abstract. Due to the development of virtual reality technologies, it is an urgent task to develop measures aimed at protecting users from potential information threats. In the context of cross-border relations in virtual reality, Russia's technological dependence on foreign countries, and the low level of knowledge among citizens in the field of information security, this task becomes especially important. Purpose: to identify the specifics of legal regulation and develop mechanisms for protecting virtual reality users, taking into account the specific features of this technology and current challenges. The study uses methods of system analysis to comprehensively understand the legal nature of virtual reality; comparative legal analysis is used to compare national and foreign legislation, and law enforcement practice; synthesis is used to summarize the theoretical and empirical data obtained in order to form the author's concept of legal regulation; legal modeling is used to develop proposals for improving current legislation and form effective mechanisms for protecting virtual reality users. Results: the article proposes the author's concept of the relationship between the concepts of "virtual reality", "virtual world" and "virtual environment", according to which the concept of "virtual reality" is specific in relation to the concepts of "virtual environment"

является видовым по отношению к понятиям «виртуальная среда» и «виртуальный мир». Такой подход позволяет распространить существующие нормы, действующие в других виртуальных средах, на виртуальную реальность. В целях обеспечения защиты данных о пользователях предлагаются изменения в законодательство, регулирующие оборот биометрических персональных данных, для защиты неидентифицированных пользователей на уровне идентифицированных, а также введение специальной формы согласия на обработку персональных данных. Отмечается необходимость внесения изменений в КоАП РФ ввиду особой опасности кибербуллинга и иных правонарушений в виртуальной реальности. Предложены административные меры противодействия информационным угрозам: введение ГОСТов, систем лицензирования, протоколов быстрого реагирования, идентификации пользователей и общей базы данных нарушителей. Подчеркивается необходимость активного привлечения создателей, разработчиков и пользователей виртуальной реальности к формированию будущего регулирования, создания «регуляторных песочниц» и повышения уровня знаний сотрудников правоохранительных органов и пользователей в области информационной безопасности.

Ключевые слова: виртуальная реальность, виртуальная среда, виртуальный мир, кибербуллинг, компьютерные правонарушения, персональные данные, идентификация

Для цитирования: Долунц В.С. Виртуальная реальность как объект правового регулирования: сущность, угрозы и механизмы защиты / В.С. Долунц. – DOI 10.33184/pravgos-2025.3.14 // Правовое государство: теория и практика. – 2025. – № 3. – С. 119–128.

and “virtual world”. This approach makes it possible to extend existing norms applicable in other virtual environments to virtual reality. In order to ensure protection of user data, the article proposes amendments to the legislation regulating the turnover of biometric personal data with the aim of protecting unidentified users at the level of identified ones, as well as the introduction of a special form of consent to the processing of personal data. The article notes the need to amend the Administrative Code of the Russian Federation due to the particular danger of cyberbullying and other offenses in virtual reality. Administrative measures to counter information threats are proposed: the introduction of state standards, licensing systems, rapid response protocols, user identification, and a common database of violators. The article highlights the need to actively involve creators, developers, and users of virtual reality in shaping future regulation, creating “regulatory sandboxes”, and improving the knowledge of law enforcement officials and users in the field of information security.

Keywords: virtual reality, virtual environment, virtual world, cyberbullying, computer offences, personal data, identification

For citation: Dolunts V.S. Virtual Reality as an Object of Legal Regulation: The Essence, Threats and Protection Mechanisms. *Pravovoe gosudarstvo: teoriya i praktika* = *The Rule-of-Law State: Theory and Practice*, 2025, no. 3, pp. 119–128. (In Russian). DOI 10.33184/pravgos-2025.3.14.

ВВЕДЕНИЕ

Технологии виртуальной реальности (VR) стали неотъемлемой частью современных инноваций. Их использование в промышленности, медицине и образовании сократило потенциальные риски на производстве, позволило создать эффективные инструменты для моделирования различных ситуаций, открыло новые возможности для обучения.

Перспективность технологий виртуальной реальности отмечается и в науке. Так, по мнению китайских исследователей, иммерсивная VR поможет сформировать новую образовательную систему будущего [1, с. 1901]. А.В. Минбалеев и Е.В. Титова отмечают пер-

спективу проведения в виртуальной среде спортивных мероприятий [2, с. 137].

Особенно активно технологии виртуальной реальности используются в развлекательной сфере: разрабатываются компьютерные игры, совместимые с технологиями виртуальной реальности, выпускается все больше контента, специализированного под данные технологии. Однако вместе с пользой новые технологии, ввиду их уникальности, вызывают все больше вопросов, проблем и, к сожалению, нередко угроз. Одной из таких угроз являются правонарушения в виртуальной реальности. Безусловно, многие действия, такие как спам, кибербуллинг, вирусные атаки, уже признаны законодатель-

ством многих стран, в том числе Российской Федерации, правонарушениями.

Особенности, присущие виртуальной реальности, требуют специального изучения и формирования концепции возможного правового регулирования в контексте компьютерных правонарушений. Реализация обозначенной цели влечет необходимость решения следующих задач: 1) посредством методов анализа и сравнения установить сущность понятия «виртуальная реальность»; 2) с помощью анализа действующего законодательства, судебной практики, а также юридической доктрины обозначить имеющиеся проблемы противодействия компьютерным правонарушениям; 3) выявить особенности правонарушений в виртуальной реальности и посредством сравнительно-правового анализа предложить возможные изменения российского законодательства.

ПОНЯТИЕ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Термин «виртуальная реальность» сегодня активно используется в российском информационном поле. По общему определению, виртуальная реальность – это «моделируемая с помощью компьютерного оборудования и программного обеспечения трехмерная среда, позволяющая пользователям посредством воздействия на органы чувств исследовать и взаимодействовать с имитирующей реальностью виртуальной средой»¹.

Некоторые определения VR содержатся в документах технологического регулирования. Так, в соответствии с ГОСТ Р 57721-2017 «виртуальная реальность – это высокоразвитая форма виртуальной среды, обладающая высокой степенью достоверности визуализации, имитирующая как воздействие на изучаемый объект, так и реакции на это воздействие»²,

а в соответствии с ГОСТ Р ИСО/МЭК 18038-2023 под виртуальной реальностью понимаются «интерактивные функциональные возможности, созданные компьютером и доступные в искусственно созданной и эмулированной среде»³. Указанные документы требуют анализа.

В ГОСТ Р ИСО/МЭК 18038-2023 термин «виртуальная реальность» тесно связывается с термином «виртуальный мир» – «набор, состоящий из одного или нескольких файлов виртуальной реальности и другого мультимедийного контента, который после обработки браузером с поддержкой технологии VR предоставляет пользователю интерактивные функциональные возможности, спроектированные разработчиком». Приведенное определение сложно назвать бесспорным. Во-первых, «виртуальная реальность» и «виртуальный мир» – схожие понятия, обладающие аналогичными признаками и свойствами: оба существуют вне зависимости от наблюдателя, сгенерированы с помощью программного кода, интерактивны и т. д. Во-вторых, понятия «виртуальная реальность» и «технологии виртуальной реальности», по нашему мнению, следует разграничивать. Технологии виртуальной реальности вбирают в себя программный код, аппаратуру, контент и т. д., то есть являются конвергенцией технологий, с помощью которых пользователь получает доступ к виртуальной реальности. Сама же виртуальная реальность не создает другую реальность или мир, а им и является. Вместе с тем отождествлять данные понятия тоже не стоит. Представляется, что «виртуальный мир» – более широкое понятие, оно включает в себя в том числе компьютерные игры, социальные сети и иные отличные от материального мира реальности.

Определение термина «виртуальная среда» дано в ГОСТ Р 57721-2017: «виртуальная реальность является одной из форм виртуальной среды, представляющей из себя форму имитационного моделирования, использующую средства визуализации для формирования наглядных копий моделируемых систем (объектов, процессов, явлений)». Иными словами, виртуальная реальность – одна из, но

1 Demystifying the Virtual Reality Landscape [Электронный ресурс]. URL: <https://www.intel.com/content/www/us/en/tech-tips-and-tricks/virtual-reality-vs-augmented-reality.html> (дата обращения: 06.10.2024) ; Virtual reality [Электронный ресурс]. URL: <https://www.techtarget.com/whatis/definition/virtual-reality> (дата обращения: 06.10.2024) ; What are the Security and Privacy Risks of VR and AR [Электронный ресурс]. URL: <https://www.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr> (дата обращения: 06.10.2024).

2 ГОСТ Р 57721-2017 «Информационно-коммуникационные технологии в образовании. Эксперимент виртуальный. Общие положения» // Доступ из справ.-правовой системы «КонсультантПлюс».

3 ГОСТ Р ИСО/МЭК 18038-2023 «Информационные технологии. Компьютерная графика, обработка изображений и представление данных об окружающей среде. Представление сенсоров в смешанной и дополненной реальности» // Доступ из справ.-правовой системы «КонсультантПлюс».

не единственная форма виртуальной среды. Такое разделение в целом поддерживается исследовательским сообществом. Так, проводя дифференциацию между виртуальной реальностью и виртуальной средой, Джим Бласкович отмечает, что как только виртуальная среда становится такой, что человек воспринимает себя существующим в ней, то в таком случае речь уже идет об иммерсивной виртуальной среде, то есть о виртуальной реальности [3, с. 129]. Таким образом, аналогично «виртуальному миру» «виртуальная среда» – более широкое понятие по отношению к «виртуальной реальности» и может включать в себя иные виртуальные среды.

Это свидетельствует о том, что понятия «виртуальная среда» и «виртуальный мир» являются синонимами. В дальнейшем эти термины будут использоваться как равнозначные.

Проведенный анализ позволяет сделать заключение, что виртуальная реальность представляет собой иммерсивный трехмерный виртуальный мир (виртуальную среду), создаваемый с помощью специальных компьютерных средств, в рамках которого пользователь имеет возможность взаимодействовать с другими участниками такой реальности, а также с интегрированной в нее вычислительной средой. Взаимодействие обеспечивается посредством специальных устройств, воздействующих на органы чувств. Особенности технологий виртуальной реальности могут помочь ей стать перспективной площадкой для различного вида социальной и публичной деятельности с имитацией личного присутствия пользователя [4, с. 116], например, организации учебного процесса, оборота цифровых активов, имитации трудовых отношений и т. д. Все это свидетельствует о возможности появления в виртуальной реальности различных общественных отношений, которые, по верному замечанию И.А. Филиповой, ставят новые задачи перед правовой системой, поскольку технологии продолжают формировать и изменять общество [5, с. 9].

ПРАВОНАРУШЕНИЯ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Одной из задач правового регулирования виртуальной реальности становится противо-

действие правонарушениям в данной среде. Виртуальная реальность, будучи средой взаимодействия пользователей между собой и с вычислительными системами, подвержена риску совершения компьютерных правонарушений. Все известные и потенциальные компьютерные атаки, такие как неправомерный доступ, распространение вредоносного программного обеспечения, DDoS-атаки, могут быть совершены в виртуальной реальности.

Одновременно с этим, как отмечалось ранее, виртуальная реальность является одной из форм виртуальной среды, к которой относятся социальные сети, сеть Интернет в целом, уже получившие свое регулирование в рамках российского закона, в том числе в части правонарушений. С учетом проведенного анализа соотношения понятий «виртуальная среда (мир)» и «виртуальная реальность», в соответствии с которым виртуальная реальность – одна из форм виртуальной среды (мира), положения действующих нормативно-правовых актов, применяемых по отношению к виртуальным средам, по нашему мнению, могут и должны в условиях отсутствия специального регулирования применяться к виртуальной реальности. Подобного подхода придерживаются, например, в США, где, как и в Российской Федерации, нет специальных норм, регулирующих виртуальную реальность, однако существуют нормы, которым разработчики и пользователи виртуальной реальности должны следовать. Это законы штатов и федеральные законы, касающиеся хозяйственной деятельности. К ним относятся нормы об азартных играх, денежных переводах, ценных бумагах, недобросовестной и вводящей в заблуждение торговой практике, кибербезопасности, антимонопольном регулировании, авторском праве, хранимых сообщениях, а также Четвертая поправка, определяющая защиту от неправомерного обыска и конфискации имущества [6, с. 52].

Тем не менее, несмотря на принимаемые меры, проблема компьютерных правонарушений сегодня все еще остро стоит на повестке дня во всем мире. В соответствии со сведениями, представленными В. Колокольцевым в рамках его выступления в Совете Федерации 14 мая 2024 г., ущерб от компьютерных преступлений, краж и мошенничеств в 2023 г.

составил 156 млрд рублей⁴. Ситуация осложняется низкой раскрываемостью компьютерных правонарушений. Согласно статистике, приведенной пресс-центром МВД России, раскрываемость киберпреступлений в 2023 г. составила 29,9 %, в том числе совершенных с использованием сети Интернет – 28,8 %⁵. Аналогичная ситуация складывается и с административными правонарушениями в сфере информации, например, в области персональных данных⁶. Такая низкая раскрываемость обусловлена несколькими факторами.

В первую очередь, идентифицировать правонарушителя нередко проблематично. Законодательством Российской Федерации не предусмотрена обязанность пользователя подтверждать свои данные, указанные в сети Интернет. Единственный случай такой необходимости предусмотрен постановлением Правительства РФ от 20 октября 2021 г. № 1801 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети "Интернет" организатором сервиса обмена мгновенными сообщениями», в соответствии с которым организатор сервиса обмена мгновенными сообщениями обязан не допускать передачу электронных сообщений пользователям сервиса обмена мгновенными сообщениями без прохождения процедуры идентификации⁷, осуществляющейся исключительно по номеру телефона. Однако несмотря на предусмотренную Федеральным законом от 7 июля 2023 г. № 126-ФЗ «О связи» обязанность мобильных операторов по оформлению SIM-карт исключительно на граждан, предъявивших паспорт, все еще остается

огромное количество нелегальных номеров, используемых злоумышленниками. Безусловно, современные технологии позволяют идентифицировать правонарушителей с помощью device-level либо browser-level идентификаторов, но по-прежнему существует ряд обстоятельств, препятствующих их дальнейшему привлечению к ответственности.

Первое и самое главное обстоятельство – трансграничность компьютерных правонарушений. Нередко злоумышленники находятся в тысячах километрах от своей жертвы. Покупка зарубежного номера без каких-либо документов сегодня не составляет труда.

Во-вторых, низкий уровень раскрываемости компьютерных правонарушений связан со скептическим отношением сотрудников правоохранительных органов к подобного рода правонарушениям, нередко с отсутствием у них специальных навыков расследования таких деяний, а также с низким уровнем знаний граждан в области информационной безопасности.

Указанное не игнорируется мировым сообществом в лице не только государств, но и международных организаций и частных компаний, которые ведут сотрудничество на различных уровнях. В частности, 27 июля 2021 г. Генеральной прокуратурой РФ был представлен российский вариант проекта Конвенции ООН «О противодействии использованию информационно-коммуникационных технологий в преступных целях». Активно идет сотрудничество на уровне ШОС, ОДКБ, БРИКС и других международных организаций и структур. Частные компании, в том числе российские, предпринимают меры технологического и правового характера, направленные на противодействие компьютерным угрозам.

Изложенное свидетельствует о наличии положительной динамики в области противодействия компьютерным правонарушениям. В то же время параллельно с ростом способов защиты от компьютерных угроз совершенствуются и способы их совершения, что также связано с развитием информационных технологий, таких как искусственный интеллект, блокчейн и виртуальная реальность. По верному замечанию Р.И. Дремлюги, «попытки контроля интернет-пространства привлекли к разработке средств, обходящих такой контроль» [7, с. 46].

4 Ущерб от действий IT-преступников в РФ в прошлом году составил 156 млрд рублей [Электронный ресурс]. URL: <https://www.interfax.ru/business/960384> (дата обращения: 06.10.2024).

5 МВД России публикует статистические данные о состоянии преступности в Российской Федерации за восемь месяцев 2023 года [Электронный ресурс]. URL: <https://mvdmedia.ru/news/official/mvd-rossii-publikuet-statisticheskie-dannye-o-sostoyanii-prestupnosti-v-rossiyskoy-federatsii-za-vos/> (дата обращения: 06.10.2024).

6 Российские компании стали скрывать утечки данных на фоне введения оборотных штрафов [Электронный ресурс]. URL: <https://telesputnik.ru/materials/trends/news/rossiyskie-kompanii-stali-skryvat-utechki-dannyh-na-fone-vvedeniya-oborotnyh-shtrafov> (дата обращения: 06.10.2024).

7 Собрание законодательства РФ. 2021. № 43, ст. 7291.

НОВЫЕ ВЫЗОВЫ: ОСОБЕННОСТИ И ПРОФИЛАКТИКА ПРАВОНАРУШЕНИЙ В ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Виртуальная реальность, будучи средой с высокой степенью интерактивности и иммерсивности, формирует новую правовую и техническую плоскость для совершения правонарушений. Ее особенности обуславливают необходимость выработки специальных мер регулирования.

Интеграция пользователя в виртуальную реальность возможна только посредством использования специальных устройств – очков виртуальной реальности или VR-шлемов, перчаток, трекеров, жилетов и т. д., которые собирают огромные объемы данных о пользователях виртуальной реальности: о передвижениях, местоположении, предпочтениях, походке, движении глаз, реакции на те или иные события и другие данные, связанные с органами чувств. Некоторые из указанных сведений являются нетипичными, их сбор и комплексный характер не всегда с одобрением воспринимаются пользователями, а некоторые, в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»⁸ и письмами Минцифры России от 17 июля 2020 г. № ОП-П24-070-19433 и Роскомнадзора от 10 февраля 2020 г. № 08АП-6782, относятся к биометрическим данным. Подобный характер указанных сведений делает их одной из приоритетных целей для злоумышленников.

Вместе с тем стоит учитывать, что согласно ст. 11 Федерального закона «О персональных данных», несмотря на то что указанные сведения относятся к биометрическим персональным данным, особый порядок их обработки устанавливается только если эти «данные используются оператором для установления личности субъекта персональных данных». Иными словами, если пользователь в виртуальной реальности не авторизован под своей учетной записью и, соответственно, не идентифицирован или целью сбора таких данных не является идентификация, особый порядок обработки не применяется. Изложенное подтверждается судебной практикой. Так, например, согласно апелляционному определению Санкт-Петербургского городского суда от

⁸ Собрание законодательства РФ. 2006. № 31 (ч. I), ст. 3451.

15 ноября 2016 г. № 33-22976/2016 по делу № 2-2932/2015 «изображение лица, размещенное на косметической продукции, не является биометрическими персональными данными, поскольку не может идентифицировать... личность»⁹. Такой подход, по нашему мнению, не может применяться по отношению к виртуальной реальности ввиду чувствительности и совокупности собираемых о пользователях сведений, особенно с учетом объема утечек персональных данных за последнее время.

Безусловно, большинство платформ в виртуальной реальности требуют авторизации пользователей и, как следствие, его идентификации. Данный вопрос нуждается в проработке.

Прежде всего, обработка биометрических персональных данных осуществляется с письменного согласия субъекта. Согласие может быть получено в электронной форме, однако в соответствии с распоряжением Правительства РФ от 30 июня 2018 г. № 1322-р требуется указания паспортных данных субъекта¹⁰. Передача таких сведений может стать стимулом для оттока пользователей из данных платформ и, как следствие, вызовет кризис на рынке устройств виртуальной реальности. Кроме того, даже в случае предоставления пользователем его персональных данных оператору у последнего нет гарантий их достоверности. По нашему мнению, проблема может быть решена, например, путем введения специальной формы согласия субъекта на обработку его персональных данных со стороны операторов в виртуальной реальности, включающего в себя Ф. И. О., адрес электронной почты и номер телефона для подтверждения его личности. Дополнительно для обеспечения защиты персональных данных неидентифицированных пользователей целесообразно установить для операторов обязанность по обеспечению защищенности таких сведений на уровне, аналогичном тому, который применяется в случаях происхождения идентификации.

⁹ Доступ из справ.-правовой системы «КонсультантПлюс».

¹⁰ Об утверждении формы согласия на размещение и обработку персональных данных в единой системе идентификации и аутентификации и биометрических персональных данных в единой биометрической системе, в том числе на передачу векторов единой биометрической системы : распоряжение Правительства РФ от 30.06.2018 № 1322-р // Собрание законодательства РФ. 2018. № 28, ст. 4268.

Дополнительно стоит обратить внимание на Федеральный закон от 29 декабря 2022 г. № 572-ФЗ, в соответствии с которым вся собранная государственными и коммерческими системами биометрия (к ней в соответствии с данным законом относятся изображение лица или голос) должна быть передана в Единую биометрическую систему. В дальнейшем такие данные подлежат зашифровке и отдельно от других персональных данных, таких как Ф. И. О., адрес и т. д., хранению¹¹. Представляется, что по мере внедрения технологий виртуальной реальности в отечественный рынок требования указанного закона могут быть распространены и на отношения в виртуальной реальности.

Меры тем не менее могут распространяться не только на производителей и разработчиков, но и на самих пользователей. К примеру, еще одним потенциальным решением вопросов, связанных с обработкой персональных данных в виртуальной реальности, может стать обязательная техническая реализация невозможности подтверждения согласия на обработку персональных данных пользователя без его прочтения. Причем получение согласия не должно сводиться исключительно к нажатию кнопки «Согласен». Учитывая возможную сложность и объемность таких согласий, решением может стать выделение жирным шрифтом перечня собираемых о пользователях персональных данных, целей, лиц, имеющих право их обрабатывать, возможность отказа от согласия и т. д.

Еще одной угрозой, требующей отдельного внимания в рамках VR, является кибербуллинг – «проявление физического или психологического насилия по отношению к другим людям в цифровом пространстве». Несмотря на имеющийся в обществе скептицизм к травле в интернете, исходя из данных, приведенных компанией VK, «57 % пользователей сталкивались с кибербуллингом»¹². В случае

¹¹ Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации : Федеральный закон от 29.12.2022 № 572-ФЗ // Собрание законодательства РФ. 2023. № 1 (ч. I), ст. 19.

¹² Проект компании VK #неткибербуллингу [Электронный ресурс]. URL: <https://kiberbulling.net/> (дата обращения: 06.10.2024).

с виртуальной реальностью ситуация еще более сложная. Было отмечено, что пользователь при использовании аппаратуры виртуальной реальности попадает в виртуальный мир, цель которого – создать иллюзию его реальности. В таких условиях пользователь как будто испытывает все чувства наяву и, соответственно, более подвержен риску преследований, угроз, демонстрации обнаженных частей тела и прочим способам негативного воздействия на его сознание. Несмотря на наличие норм в российском законодательстве, предусматривающих ответственность за травлю в сети Интернет, их сложно назвать действенными. Так, ст. 5.61 КоАП РФ предусматривает штраф от 3 до 5 тыс. рублей за унижение чести и достоинства другого лица. За такое оскорбление в «социальной сети, зарегистрированной в качестве средства массовой информации» ответственность возрастает до 10 тыс. рублей. Представляется, что эта сумма недостаточна и требует увеличения. Лицо, осуществляющее травлю в цифровом пространстве, чувствует себя более безнаказанным сразу по нескольким причинам: анонимность, отсутствие «живого» контакта с жертвой, территориальные ограничения и др.

Весьма показательна в этой связи позиция российского законодателя в рамках уголовного регулирования. В августе 2024 г. ст. 63 УК РФ была дополнена пунктом «т», согласно которому совершение умышленного преступления с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет), рассматривается в качестве обстоятельства, отягчающего наказание. Считаем, что такой же подход должен найти отражение и в ст. 4.3 КоАП РФ, которая должна быть дополнена пунктом 7, предусматривающим аналогичное положение.

Не менее важную и связанную с предыдущими особенностями проблему поднимают Марк Лемли и Юджин Волох. Они указывают на так называемую «проблему Бангладеша», которая заключается в скептическом отношении правоохранительных органов к заявлениям пользователей о правонарушениях, совершенных в виртуальной реальности. Скептицизм обусловлен нетипичностью подобных правонарушений для правоохра-

нительной системы, а также трансграничностью, которая также поднимает вопросы определения государственной юрисдикции и экстрадиции [8, с. 1134]. Конечно, большинство правонарушений в виртуальной реальности совершаются посредством использования примитивных средств атаки, а злоумышленники могут быть достаточно быстро узнаны. В то же время расследование в отношении них не приводит к эффективным последствиям ввиду расстояния. М.А. Федотов в этой связи пишет: «чтобы государство смогло выработать правовые нормы, способные работать в Сети, оно должно сначала найти себя в киберпространстве и определить, где здесь проходят границы его суверенитета и юрисдикции» [9, с. 168].

Указанные проблемы не являются единственными для виртуальной реальности. Однако наиболее важен тот факт, что технологии виртуальной реальности, несмотря на свою текущую популярность, тем не менее пока не получили большого распространения в России. Это связано с высокой стоимостью оборудования, отсутствием конкурентоспособных отечественных платформ и устройств и т. д. В таких условиях защита пользователей от потенциальных угроз выпадает из поля зрения законодательных и регулирующих органов. Представляется, что для развития отечественного производства, защиты российских пользователей требуется создание особых условий для российских производителей устройств, которые, однако, обязательно должны соответствовать определенным техническим требованиям, в том числе связанным с обеспечением информационной безопасности. Эти требования могут быть закреплены не только в нормах законодательного характера, но и, например, в документах технического регулирования.

Не менее действенным средством может оказаться внедрение системы лицензирования виртуальных платформ, что позволит государству установить требования к безопасности и управлению данными пользователей, предотвращать распространение противоправного контента. Такие требования могут включать необходимость разработки и внедрения со стороны операторов платформ виртуальной реальности протоколов быстро-

го реагирования на жалобы пользователей на правонарушения. Указанные протоколы должны включать удаление противоправного контента и блокировку пользователей. За нарушения требований лицензирования может быть предусмотрена система штрафов для лиц, ответственных за их соблюдение.

Ключевым элементом противодействия информационным угрозам в виртуальной реальности может стать внедрение процедуры идентификации пользователей. Подобная мера будет способствовать усложнению действий злоумышленников и облегчит привлечение их к ответственности. Однако идентификация должна быть соразмерной и основываться на принципах разумной достаточности и направленности на достижение конкретных целей, без избыточного сбора личных данных. Для пользователей, чья деятельность в виртуальной реальности ограничивается развлекательными целями, идентификация не должна предполагать раскрытие полного объема личной информации.

Достаточно действенным способом, учитывая, что виртуальная реальность подразумевает глобальную систему взаимодействия пользователей, может стать ведение общей базы данных о лицах, совершивших правонарушения в виртуальной реальности. Такие данные могут распространяться среди операторов платформ для ограничения доступа правонарушителей.

ЗАКЛЮЧЕНИЕ

Виртуальная реальность, будучи социально нейтральной технологией, способна оказывать как положительное, так и негативное воздействие на общество. Сложность и, как следствие, законодательная неурегулированность данной сферы становится стимулом для появления потенциальных угроз не только для рядовых пользователей, но и для информационного сообщества в целом.

Проведенный анализ показал наличие вопросов, требующих разрешения в сфере информационной безопасности виртуальной реальности, что потребует комплексного подхода, соединяющего в себе меры не только правового, но и технического и образова-

тельного характера. Концепции минимизации потенциальных угроз, помимо предложенных мер, могут также включать в себя установление определенных правил и обязательств для компаний-разработчиков, а также для правоохранительных органов и самих пользователей. Например, введение со стороны разработчиков обязательного ознакомительного курса по информационной безопасности для пользователей виртуальной реальности.

Установление же правового режима требует тщательного предварительного анализа виртуальной реальности. Проблематика в данном случае, как отмечает В.В. Архипов, «дополняется вопросом о соотношении виртуального и реального, то есть о пределах применения норм реального права к виртуальным отношениям» [10, с. 4]. В таких обстоятельствах в первую очередь требуется четко определить правовую природу виртуальной реальности. Ведь, по верному замечанию И.Л. Бачило, «формирование языка науки является одним из ключевых при формировании информационного законодательства» [11]. Также требуется решить уже существующие проблемы в рамках противодействия информационным угрозам и в дальнейшем сформировать модель регулирования виртуальной реальности. Проведенный нами анализ может способствовать решению обозначенных вопросов.

Вместе с тем введение жестких мер может стать болезненным для рынка VR-устройств и фатальным для производителей, особенно учитывая, что основные производители VR-устройств и виртуальных платформ – зарубежные компании. Тем не менее в условиях отсутствия полноценной законодательной защиты пользователей от компьютерных правонарушений именно создатели VR-устройств и виртуальных платформ становятся единственным рубежом защиты пользователей от злоумышленников.

Решение обозначенных и иных проблем требует совместных усилий как со стороны государства, так и со стороны производителей, разработчиков и пользователей. Представляется, что метод сорегулирования может стать фундаментом для дальнейшего развития технологий виртуальной реальности и их регулирования. Подобное сотрудничество может заключаться в создании «регуляторных песочниц», в рамках которых производители и разработчики смогут опробовать те или иные меры защиты информации, в привлечении граждан для их тестирования, введении минимальной или нулевой налоговой ставки и т. д. Все изложенное, по нашему мнению, позволит в равной степени учесть интересы государства, производителей, разработчиков и пользователей виртуальной реальности.

СПИСОК ИСТОЧНИКОВ

1. Jie Huang. Analysis of the Future Prospects for the Metaverse / Jie Huang, Pingjin Sun, Weijie Zhang. // *Advances in Economics. Business and Management Research*. – 2022. – Vol. 211. – P. 1899–1904.
2. Минбалеев А.В. Правовые проблемы и риски проведения спортивных мероприятий в метавселенной / А.В. Минбалеев, Е.В. Титова // *Человек. Спорт. Медицина*. – 2023. – № S1. – С. 136–142.
3. Blascovich J. Social Influence within Immersive Virtual Environments / J. Blascovich // *The Social Life of Avatars. Computer Supported Cooperative Work*. Springer. – London, 2002. – P. 127–145.
4. Холодная Е.В. О правовой концепции метавселенных / Е.В. Холодная // *Lex Russica*. – 2024. – № 77 (3). – С. 116–128.
5. Филипова И.А. Создание метавселенной: последствия для экономики, общества и права / И.А. Филипова // *Журнал цифровых технологий и права*. – 2023. – Т. 1, № 1. – С. 7–32.

REFERENCES

1. Jie Huang, Pingjin Sun, Weijie Zhang. Analysis of the Future Prospects for the Metaverse. *Advances in Economics. Business and Management Research*, 2022, vol. 211, pp. 1899–1904.
2. Minbaleev A.V., Titova E.V. Legal Issues and Risks of Holding Sports Events in the Metaverse. *Human. Sport. Medicine*, 2023, no. S1, pp. 136–142. (In Russian).
3. Blascovich J. Social Influence within Immersive Virtual Environments. *The Social Life of Avatars. Computer Supported Cooperative Work*. Springer. London, 2002, pp. 127–145.
4. Kholodnaya E.V. On the Legal Concept of Metaverses. *Lex Russica*, 2024, no. 77 (3), pp. 116–128. (In Russian).
5. Filipova I.A. Creating the Metaverse: Consequences for Economy, Society, and Law. *Journal of Digital Technologies and Law*, 2023, vol. 1, no. 1, pp. 7–32. (In Russian).

6. Евсиков К.С. Метавселенные как новый объект регулирования для информационного права / К.С. Евсиков // Труды по интеллектуальной собственности (Works on Intellectual Property). – 2023. – Т. 44, № 1. – С. 47–57.

7. Дремлюга Р.И. Виртуальная реальность: общие проблемы правового регулирования / Р.И. Дремлюга // Актуальные проблемы российского права. – 2020. – Т. 15, № 9. – С. 39–49.

8. Lemley M. Law, Virtual Reality, and Augmented Reality / M. Lemley, E. Volokh // University of Pennsylvania Law Review. – 2018. – Vol. 166, № 5. – P. 1051–1138.

9. Федотов М.А. Конституционные ответы на вызовы киберпространства / М.А. Федотов // Lex Russica. – 2016. – № 3. – С. 164–182.

10. Архипов В.В. Персонажи (аватары) в многопользовательских компьютерных играх: вопросы правовой квалификации в свете междисциплинарных исследований / В.В. Архипов // Закон. – 2022. – № 3. – С. 58–74.

11. Бачило И.Л. Институциональный подход к решению проблем понятийного аппарата в информационном законодательстве / И.Л. Бачило // Понятийный аппарат в информационном праве : монография / отв. ред.: И.Л. Бачило, Т.А. Полякова, В.Б. Наумов. – Москва : ИГП РАН – Издательство «Канон+» РООИ «Реабилитация», 2017. – 264 с.

6. Evsikov K.S. Metaverses as a New Object of Regulation for Information Law. *Trudi po Intellectualnoy Sobstvennosti (Works on Intellectual Property)*, 2023, vol. 44, no. 1, pp. 47–57. (In Russian).

7. Dremlyuga R.I. Virtual Reality: Common Problems of Legal Regulation. *Actual Problems of Russian Law*, 2020, vol. 15, no. 9, pp. 39–49. (In Russian).

8. Lemley M., Volokh E. Law, Virtual Reality, and Augmented Reality. *University of Pennsylvania Law Review*, 2018, vol. 166, no. 5, pp. 1051–1138.

9. Fedotov M.A. Constitutional Answers for the Challenges of Cyberspace. *Lex Russica*, 2016, no. 3, pp. 164–182. (In Russian).

10. Arkhipov V.V. Characters (Avatars) in Multiplayer Computer Games: Issues of Legal Qualification in Light of Interdisciplinary Research. *Law*, 2022, no. 3, pp. 58–74. (In Russian).

11. Bachilo I.L. Institutional Approach to Solving Problems of the Conceptual Apparatus in Information Legislation. In Bachilo I.L., Polyakova T.A., Naumov V.B. (eds.). *Conceptual Apparatus in Information Law*. Moscow, Canon + Rehabilitation Publ., 2017. 264 p.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Долунц Вартан Сурикович – аспирант кафедры информационного права и цифровых технологий.

INFORMATION ABOUT THE AUTHOR

Dolunts Vartan Surikovich – Postgraduate Student of the Chair of Information Law and Digital Technologies.

Статья поступила в редакцию 01.06.2025; одобрена после рецензирования 07.07.2025; принята к публикации 07.07.2025. The article was submitted 01.06.2025; approved after reviewing 07.07.2025; accepted for publication 07.07.2025.