

Научная статья

УДК 343.9

DOI 10.33184/vest-law-bsu-2026.31.19

Иванова Елена Вячеславовна

ФГКОУ ВО «Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева», ГОУ ВО МО
«Государственный социально-гуманитарный университет», Москва, Россия,
ivanova-elena-7@yandex.ru, <https://orcid.org/0000-0003-2589-7726>

Никитина Ирина Эдуардовна

ФГКОУ ВО «Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева», ФГБОУ ВО
«Национальный исследовательский университет «МЭИ», Москва, Россия,
irinanikitina23@rambler.ru

ОНЛАЙН-ПРЕСТУПЛЕНИЯ В ЦИФРОВЫХ ИМИТИРОВАННЫХ МИРАХ: ТЕНДЕНЦИИ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

Аннотация. Задачей мирового сообщества на современном этапе является нахождение оптимального баланса в использовании «метавселенной»: её активно внедряют, с ней экспериментируют, подчеркивая её актуальность и потенциальное влияние в глобальном масштабе. Широкое распространение таких технологий – не просто тенденция, а глобальное движение, формирующее будущее человеческого взаимодействия и развития.

Тем не менее, достигнутый технический прогресс вызывает серьёзные опасения, связанные с неправомерными деяниями в виртуальной среде и особенностями их расследований в реальном мире.

Отдельного внимания заслуживают преступления в цифровых имитированных пространствах (англ. «metaverse crimes»), что требует нового взгляда на институциональные и функциональные аспекты отечественной правовой системы с учётом специфики их совершения.

Цель: выявление основных тенденций совершения онлайн-преступлений в цифровых имитированных мирах и выработка мер противодействия.

Методы: эмпирические методы сравнения, описания, интерпретации; теоретические методы формальной и диалектической логики; частнонаучные методы: юридико-догматический и другие.

Результаты: исследование позволило выявить двойственные прогнозы относительно «метавселенной». С одной стороны, «метавселенная» революционизирует социальные структуры, уменьшая физические препятствия и создавая гиперпространственно-временную иррациональную реальность, где пользователи

могут участвовать в социальных взаимодействиях, профессиональной деятельности и развлекательных мероприятиях, не будучи ограниченными временем и физическим расстоянием. Несмотря на то, что технологии могут способствовать значимому и продуктивному обмену, они также несут в себе потенциальные риски, как-то: социальное разделение, неравенство или вмешательство в частную жизнь.

В качестве основного условия дальнейшего развития «метавселенной» авторы называют нахождение оптимального баланса между обеспечением безопасности и невмешательством в частную жизнь.

Ключевые слова: метавселенная, цифровые имитированные пространства, преступления, Интерпол, Европол, террористическая деятельность, обеспечение безопасности, права человека

Для цитирования: Иванова Е.В., Никитина И.Э. Онлайн-преступления в цифровых имитированных мирах: тенденции и меры противодействия / Е.В. Иванова, И.Э. Никитина. – DOI 10.33184/vest-law-bsu-2026.31.19 // Вестник Института права Башкирского государственного университета. – 2026. – № 3. – С. 249–265.

Original article

Ivanova Elena Vyacheslavovna

Sukharev Moscow Academy of the Investigative Committee of the Russian Federation, State University of Social Sciences and Humanities, Moscow, Russia, ivanova-elena-7@yandex.ru, <https://orcid.org/0000-0003-2589-7726>

Nikitina Irina Eduardovna

Sukharev Moscow Academy of the Investigative Committee of the Russian Federation, National Research University "MEI", Moscow, Russia, irinanikitina23@rambler.ru

ONLINE CRIMES IN DIGITAL SIMULATED WORLDS: TRENDS AND COUNTERMEASURES

Abstract: At the present stage, the world community task is to find the optimal balance in the "metaverse" use: it is actively implemented, experimented with, emphasizing its relevance and potential impact on a global scale. The widespread adoption of such technologies is not just a trend, but a global movement shaping the future of human interaction and development. However, technological advances have raised serious concerns about virtual environment and the features of their real-world investigations. Special attention should be paid to crimes in digital simulated spaces ("metaverse crimes"), which requires a new look at the institutional and functional aspects of the domestic legal system, taking into account the specifics of their commission. Purpose: to identify the main trends in online crime in digitally simulated worlds and to develop countermeasures. Methods: empirical methods of comparison, description, interpretation; theoretical methods of formal and dialectical logic; private scientific methods: legal-dogmatic and others. Results: the study

revealed ambivalent predictions about the “metaverse”. On the one hand, the “metaverse” revolutionizes social structures by reducing physical obstacles and creating a hyperspace-time irrational reality where users can participate in social interactions, professional activities and recreational activities without being limited by time and physical distance. While technology can facilitate meaningful and productive exchange, it also carries potential risks such as social division, inequality, or interference with privacy. The authors cite finding the optimal balance between ensuring security and non-interference in private life as the main condition for the further development of the “metaverse”.

Keywords: metaverse, digital simulated spaces, crimes, Interpol, Europol, terrorist activities, security, human rights

For citation: Ivanova E.V., Nikitina I.E. Online Crimes in Digital Simulated Worlds: Trends and Countermeasures. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University*, 2026, no. 3, pp. 249–265. (In Russian). DOI 10.33184/vest-law-bsu-2026.31.19

Введение. От Японии до США, от Южной Кореи до Сингапура и Индонезии наблюдается растущий интерес к «метавселенной»: её активно внедряют, с ней экспериментируют, подчеркивая её актуальность и потенциальное влияние в глобальном масштабе. Широкое распространение таких технологий – не просто тенденция, а глобальное движение, формирующее будущее человеческого взаимодействия и развития. Государства разрабатывают стратегии по расширению возможностей её использования, например, стратегия Дубая по развитию «метавселенной» в ОАЭ (Dubai Metaverse Strategy)¹.

Часть стран идёт по пути расширения опыта использования технологий цифрового взаимодействия онлайн. Например, Египет запустил первый хака-тон² в «метавселенной».

Термин «метавселенная» относится к образному, имитированному миру, который включает две части: «мета» («за пределами») и «вселенная» («за пределами мира»). Этот термин впервые был использован в научно-фантастическом романе Нила Стивенсона 1992 г. «Снежная катастрофа», в котором люди, как аватары, взаимодействуют друг с другом и программным обеспечением в виртуальном трёхмерном пространстве, подобном реальному миру [1, 2].

В настоящее время «метавселенная», в основном, детерминируется как виртуальная реальность (VR), но всё чаще определяется с точки зрения дополненной реальности (AR) или расширенной / смешанной реальности (XR)³.

¹ Стратегия Дубая в сфере метавселенных (Dubai Metaverse Strategy) направлена на превращение эмирата в один из 10 ведущих мировых центров экономики метавселенных, привлечение 1000 специализированных компаний и создание более 40 000 виртуальных рабочих мест к 2030 г. Инициатива делает упор на внедрение дополненной реальности, цифровых двойников и развитие законодательной базы для секторов туризма, госуслуг и недвижимости.

² Это командное соревнование (Metaverse hackathon), включающее в себя серию соревновательных и интерактивных мероприятий, реализуемых в гибридной форме, которая сочетает онлайн-мероприятия и интерактивные действия, способствующие построению и развитию «метавселенной» при помощи создания приложений и использования различных технологических решений, а также создание первого египетского города в виртуальном мире под названием «Метатот» (Metatot).

Статистические исследования показывают, что рынок «метавселенной», оцениваемый в 39 миллиардов долларов в 2021 г., вырос до 47 миллиардов

³ Метавселенная состоит из нескольких основных элементов, которые, по сути, составляют этот новый виртуальный мир, а именно:

1. Платформы метавселенной: Виртуальные платформы являются важным компонентом технологии метавселенной, поскольку они считаются пространством, через которое пользователи получают и осуществляют виртуальную деятельность, такую как работа, обучение, игры, покупки и т. д. Недавно появились несколько виртуальных платформ, таких как The Sandbox, Decentraland, Roblox и Nakamoto. Эксперты считают, что эти платформы будут представлять собой новое развитие сайтов социальных сетей. В свете этого многие крупные технологические компании по всему миру начали создавать свои виртуальные миры, такие как Meta и другие.

2. Невзаимозаменяемые токены (NFT) – это цифровые активы с определённой идентификационной информацией, хранящейся и документируемой с помощью технологии блокчейн. Они могут представлять собой аватары, костюмы и предметы в видеоиграх, домах, виртуальных мирах или других местах. Эти цифровые коды считаются важной составляющей метавселенной, поскольку именно они те основные элементы, на которых строятся иммерсивные впечатления пользователей. Аватары, представляющие цифровых двойников пользователей, являются самой продаваемой категорией NFT, достигнув объёма продаж более 16 миллиардов долларов в 2021 г., что составляет 46 % от объёма продаж рынка невзаимозаменяемых токенов.

3. Цифровые валюты: цифровые валюты играют важную роль в метавселенной, поскольку они считаются цифровыми единицами стоимости, посредством которых совершаются все финансовые транзакции. Каждый мир метавселенной содержит определённую валюту, которая используется в нём. Например, SAND – это валюта мира «Песочница», а MANA – валюта «Децентрализованной страны». Владельцы этих валют могут оплачивать любые услуги или товары в этих мирах. Каждая валюта метавселенной имеет определённую стоимость, которая может время от времени меняться, как и у других цифровых валют. Валюты метавселенной продемонстрировали значительный рост за последний период, совпавший с тем, как мировые технологические гиганты стремятся пробиться в этот мир и вкладывают в него миллиарды инвестиций.

4. Виртуальная и дополненная реальность: метавселенная опирается на различные технологии. Это позволяет пользователям виртуально взаимодействовать в её среде. Технологии виртуальной реальности (VR) и дополненной реальности (AR) считаются одними из наиболее важных технологий, на которых основана метавселенная. Эти две технологии обеспечивают пользователям эффект полного погружения в трёхмерные виртуальные среды благодаря аппаратному и программному обеспечению, создавая у пользователя ощущение присутствия в реальном мире.

Например, платформы метавселенной, использующие технологии виртуальной реальности, предоставляют пользователям эффект полного погружения, «обманывая человеческий разум» и имитируя значительное количество чувств. Это достигается с помощью наушников, сенсорных перчаток и т. п. В свете этого эксперты рассматривают технологии виртуальной и дополненной реальности как неотъемлемую часть технологий метавселенной.

5. Блокчейн – это гигантская база данных, через которую транзакции и данные записываются и документируются децентрализованным образом, обеспечивая безопасность, скорость и эффективность использования. Эта технология считается одной из ключевых технологий, основанных на метавселенной. Все платформы в основном полагаются на блокчейн для безопасного и неизменяемого хранения данных. Эта технология также играет важную роль в документировании невзаимозаменяемых токенов в метавселенной. Эксперты ожидают, что будущая метавселенная будет состоять из открытых, взаимосвязанных и децентрализованных виртуальных миров, каждый из которых будет иметь локальную функциональную экономику, основанную на блокчейне.

6. Искусственный интеллект: Искусственный интеллект – это цифровая модель, способная решать сложные задачи и выполнять когнитивные функции, такие как обучение, решение проблем, рассуждение, восприятие и т. д.

долларов в 2022 г. и далее до 56,6 миллиардов долларов в 2023 г., и в конечном итоге достигнет ошеломляющих 679 миллиардов долларов к 2030 г. [3].

Представленные экономические показатели демонстрируют потенциал «метавселенной» и её возможное влияние на мировую экономику, обоснованно предполагая многообещающие перспективы. Эксперты прогнозируют, что «метавселенная» станет платформой для коммерческих предложений с ожидаемой прибылью на сумму до 13 триллионов долларов к 2030 г. [4, 5].

Сегодня крупные технологические компании начали извлекать выгоду от использования искусственного интеллекта, создавая свои имитированные миры, а также разрабатывая и проектируя токены (NFT) с его помощью. Например, генеральный директор Meta Марк Цукерберг объявил о привлечении экспертов по искусственному интеллекту для разработки инструмента под названием Builder Bot, который позволяет пользователям в виртуальном мире изменять окружающую обстановку с помощью голосовых команд. Следует отметить, что искусственный интеллект может создавать аватары для пользователей, которые очень на них похожи, что делает среду «метавселенной» более реалистичной [3].

Исследования показывают, что «метавселенная» влияет на социальную динамику и сплочённость сообщества, создавая новые возможности для значимого участия в его деятельности, изменяя социально-пространственные отношения и предоставляя альтернативы физическому социальному взаимодействию.

Технологии, применяемые в имитированных мирах, также способствуют развитию инклюзивности, создавая новые социально-технологические группы. Несмотря на то, что технологии могут способствовать значимому и продуктивному обмену, они также несут в себе потенциальные риски, как-то: социальное разделение, неравенство или вмешательство в частную жизнь.

Ожидается, что продолжающаяся эволюция «метавселенной» произведёт революцию в социальных структурах, интегрируя действительность в цифровую среду, переопределяя динамику человеческого взаимодействия и формирование сообществ и предлагая альтернативные социальные возможности во многих областях, выходящих за пределы реального мира [6].

Технологии виртуальной и дополненной реальности, составляющие основу «метавселенной», могут стимулировать нейробиологические и когнитивные процессы, сопоставимые с теми, которые наблюдаются в реальном мире [7]. Это потенциально может способствовать более значимому и продуктивному взаимодействию в онлайн-сообществах.

«Метавселенная» революционизирует социальные структуры, уменьшая физические препятствия и создавая гиперпространственно-временную иррациональную реальность, где пользователи могут участвовать в социальных взаимодействиях, профессиональной деятельности и развлекательных мероприятиях, не будучи ограниченными временем и физическим расстоянием [8, с. 121–126; 9, с. 319–352]. Вместе с тем, полагаем, что термин «метавселенная», отсылающий к концепции цифрового пространства, разрабатываемого компанией «Meta», не отражает его сущности. Цифровую среду, имитирующую

реальность, со своими правилами и особенностями более точно передаёт, на наш взгляд, понятие «имитированный цифровой мир», который мы будем употреблять далее. С имитированными цифровыми мирами тесно связаны понятия «цифровая личность»⁴, «цифровой образ»⁵ («digital identity»), «цифровой профиль (гражданина)»⁶ и др.

Преступления в цифровых имитированных мирах. Тем не менее, достигнутый технический прогресс вызывает серьёзные опасения, связанные с неправомерными деяниями в виртуальной среде и особенностями их расследований в реальном мире.

Отдельного внимания заслуживают преступления в цифровых имитированных пространствах (англ. «metaverse crimes»), в том числе кража цифрового образа (неправомерный доступ, риски токенизации), дипфейки (угрозы с фальсифицированным материалом, обезличивание или имперсонализация, распространение заведомо ложных сведений), нарушение права на неприкосновенность частной жизни в цифровом пространстве (отслеживание, агрессивное преследование, кибербуллинг), фишинг (кража учётных данных, неправомерный сбор персональных данных), кибермошенничество (схемы в сфере технической поддержки, инвестиций, обезличивания или имперсонализации), виртуально-физические атаки, атаки с эффектом погружения в виртуальную реальность, виктимизация-суперреализм, неправомерное использование биометрических данных, деяния с использованием или против аватаров, виртуального имущества и активов (шантаж, вандализм, события, приводящие к сбоям), цифровые преступления сексуального характера (эксплуатация, насилие, харасмент), нарушения прав на интеллектуальную собственность. Такие преступления могут, на наш взгляд, именоваться онлайн-преступлениями, поскольку происходят в 3D онлайн-имитированных мирах.

Большие языковые модели по типу «DeepSeek», «ChatGPT», «Microsoft Copilot» с использованием методов джейлбрейк могут также быть использованными в преступных целях, в частности для написания основ кодов на языке программирования «C++» для клавиатурных шпионов (англ. «keylogger»), программ-вымогателей с последующей ручной корректировкой [10, с. 52–53].

В 2024 г. полиция Великобритании начала расследование первого случая нападения в виртуальной реальности на несовершеннолетнего, когда его аватар подвергся сексуальному насилию [11]. Это далеко не первый случай сексуального насилия в цифровых имитированных мирах. Появляются свидетельства того, что феномен, известный как культура «геймергейт», включающий в себя преследование женщин в онлайн-игровых средах, будет сохраняться в «ме-

⁴ Цифровой личностью предлагается считать индивида, который обладает правами, связанными с цифровыми технологиями и реализуемыми в цифровом пространстве.

⁵ Цифровой образ – система данных о человеке, участвующих в операциях в цифровом пространстве.

⁶ Совокупность актуальных, достоверных данных и иных сведений о физических и юридических лицах, формируемых в целях их предоставления субъектам в определённом порядке и посредством соответствующей инфраструктуры.

тавселенной» и не сможет быть эффективно разрешён лишь одними технологическими средствами [12].

Европол обоснованно считает, что цифровые имитированные миры могут стать центральным пространством для отмывания цифровых денег. Преступные группы, занимающиеся незаконным отмыванием денег, имеют возможности покупать и продавать виртуальные активы в «метавселенных» благодаря анонимности создания аватаров и потенциальному злоупотреблению валютой (metaverse coin)⁷.

Террористы в ближайшем времени научатся широко использовать новые технологические возможности для пропаганды, вербовки и обучения «потенциальных жертв» в цифровых пространствах. Благодаря более совершенным технологиям и связанным с ними генерируемыми данными террористам стало легче находить «уязвимых людей» и адаптировать свои психологические приёмы к их восприятию действительности, что позволяет им более эффективно вести пропаганду и вербовать людей [13, с. 171–181].

Отсутствие каких-либо механизмов контроля в имитированном мире угрожает кибербезопасности, тем более что осуществление мониторинга огромного количества пользователей одновременно будет сложным, даже практически неосуществимым процессом. Вышеуказанное позволяет заключить, что технологии цифровых имитированных пространств могут способствовать распространению киберпреступности в мире, причём с течением времени всё в большей степени.

Несмотря на то, что практика расследования и противодействия противоправным деяниям в цифровых имитированных пространствах в настоящее время только нарабатывается, потребуются определённые коррективы в процесс обнаружения, фиксации и сохранения доказательств, однозначно поставив задачи криминалистике. Это связано с быстрыми технологическими изменениями, в результате которых мир движется к полной зависимости от «метавселенной».

Интерпол и цифровой имитированный мир: подходы и перспективы. Интерпол полагает, что наиболее серьёзными проблемами, с которыми столкнутся правоохранительные органы применительно к цифровым имитированным мирам, станут требования к технологиям и инфраструктуре: для эффективного использования «метавселенной» нужны значительные средства, включая затраты на оборудование для виртуальной реальности, мощные сетевые серверы и обучение персонала. Конфиденциальность персональных данных, их защита, а также обеспечение этичного использования личных данных в цифровом имитированном мире являются теми проблемами, над которыми уже сейчас необходимо работать, особенно в тех случаях, когда виртуальная среда

⁷ Europol (2022), Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg [Электронный ресурс] // URL: <https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf> (дата обращения: 14.07.2026).

«пересекается» с реальном миром, например, в случаях утечки персональных данных или подмены цифровой личности.

Интерпол разрабатывает и распространяет практические пособия по цифровым доказательствам, такие как «Global Guidelines for Digital Forensic Laboratories» (Глобальное руководство по цифровизации судебно-экспертных лабораторий) и «Guidelines for First Insights in Digital Forensics» (Руководство для начинающих по цифровизации в криминалистике). В них отражены принципы работы по обнаружению, изъятию, идентификации и обработке цифровых доказательств, обеспечивая их целостность для приемлемости в судебных разбирательствах. Организация проводит форумы, такие как совещание экспертной группы Интерпола по цифровизации в криминалистике (ежегодное собрание), участие в котором открыто для специалистов и руководителей правоохранительных органов, государственных учреждений, компаний по цифровым технологиям и университетских учреждений.

В октябре 2022 г. Интерполом создана «группа экспертов по метавселенной» для разработки рекомендаций по борьбе с потенциальным неправомерным использованием цифровых имитированных пространств преступными элементами.

Кроме того, Интерпол запустил виртуальную версию своей штаб-квартиры в Лионе (Франция) с использованием технологий цифрового пространства, позволяющей зарегистрированным пользователям исследовать её без каких-либо географических или физических ограничений.

Интерпол по мере развития технологий предлагает сотрудникам правоохранительных органов стран-членов организации взаимодействовать со своими коллегами при помощи обмена фотографическими снимками (символикой) и участия в совещаниях и учебных курсах, посвящённых возможностям цифровых пространств. По существу, Интерпол использует «метавселенную» в качестве инструмента правоохранительной деятельности.

Параллельно с этим в январе 2024 г. Интерпол выпустил официальный доклад – белая книга о «метавселенной» «Сценарии использования, преступность, судебная экспертиза, расследование и управление» (Use Cases, Crime, Forensics, Investigation and Governance).

Противодействие онлайн-преступлениям. При расследовании онлайн-преступлений неизбежно возникнут правовые коллизии, поскольку действующее уголовное законодательство не предусматривает особенности некоторых противоправных деяний, совершаемых в цифровых имитированных мирах (например, нападение на цифрового двойника личности). Также присутствуют разночтения в определении временных и пространственных критериев совершаемых правонарушений.

Наличествуем мнение, что для конкретных видов преступлений, таких как противоправные действия сексуального характера против аватаров, следует разработать отдельные санкции, поскольку существующее национальное законодательство может быть недостаточно эффективным в отношении таких деяний [14].

«Метавселенная» создала новую концепцию места преступления, в которой действия одного человека могут иметь последствия в нескольких местах в один и тот же момент времени в отличие от временного измерения в реальности, которое варьируется от состояния к состоянию с временными промежутками, в результате чего характеристики объективной стороны будут различаться [15].

Многие исследователи полагают, что международная признанная система принципов, поощряющая сотрудничество между государствами, будет способствовать эффективности борьбы с онлайн-преступлениями и поддержанию демократического управления в «метавселенной» [16]. Государствам настоятельно рекомендуется модернизировать национальные системы уголовного правосудия специально под запросы «метавселенной», а мировое сообщество должно уделять этому вопросу приоритетное внимание [17].

Ещё одна точка зрения связана с тем, что для борьбы с онлайн-преступлениями необходимы отдельные законы, такие как «уголовное право метавселенной». Разработка общих правил и конкретных положений может эффективно противодействовать неправомерной деятельности в «метавселенной» [14].

Существует мнение, что модель уголовного кодекса «метавселенной» обеспечит регулирование правонарушений, имеющих отношение к электронным юрисдикциям, тем самым сдерживая онлайн-преступность [18].

Другая часть исследователей предлагает установление стандартов и единообразных подходов к онлайн-преступлениям. Так, для снижения уровня преступности в «метавселенной» крайне важно провести оценку рисков финансовой безопасности, проанализировать существующие стратегии борьбы с киберпреступностью и исследовать потенциал поведенческого анализа и регулирования [19, с. 4, 37–49].

Отдельные авторы считают, что участие общественности в обсуждениях правовых норм по противодействию преступной деятельности в цифровых имитированных онлайн-пространствах позволит соблюсти интересы разных индустрий государства и пользователей. Кроме того, крайне важно собирать и учитывать предложения соответствующих отраслевых магнатов, пользователей и экспертных групп [20].

Ещё одно мнение связано с тем, что имитированные миры имеют ограниченный потенциал для возникновения новых видов преступной деятельности и что науки уголовно-правового профиля столкнутся с трудностями при изучении и анализе аномального поведения в таких пространствах. Некоторые добавляют, что разработка эффективных инициатив по укреплению правомерного поведения в имитированном пространстве потребует множество исследований и инвестиций [21].

В целом, эффективное противодействие преступности в цифровых имитированных мирах будет зависеть от нескольких факторов, таких как:

– международной унификации уголовно-правовой борьбы с такими деяниями, что полностью согласуется с общечеловеческим подходом, который

афористично преподнёс Л.Н. Толстой: «Если плохие люди объединяются, хорошие люди должны это сделать обязательно» [22, с. 989];

- создание специализированной системы уголовного правосудия для цифровых имитированных пространств;

- разработка единых технологических стандартов с криптографической защитой.

Перспективы использования технологий имитированных пространств в правоохранительной деятельности. Ожидания от использования технологий имитированных миров в правоохранительной деятельности видятся в следующем:

- интеграция с искусственным интеллектом для создания более динамичных и оперативных сценариев обучения и содействия действиям полиции в имитированном мире;

- расширение операций: правоохранительные органы смогут расширить масштабы своих операций в имитированных мирах, что приведёт к более разнообразным вариантам использования этой технологии.

Ключевой посыл заключается в том, чтобы адаптировать эти технологии для нужд правосудия и помощи правоохранительным органам, учитывая, что технологии имитированных миров расширяют их возможности, предоставляя инновационные инструменты для дополненной реальности, виртуальной реальности и расширенной реальности.

Наиболее перспективное направление, в котором следует использовать технологии имитированных миров, – это платформа для подготовки сотрудников правоохранительных органов, расширения сотрудничества между ними путём проведения онлайн-совещаний, поддержки в осмотре мест преступлений в цифровых пространствах, оказания технической поддержки, предоставления государственных услуг, получения отчётов и жалоб.

Защитники «метавселенной» (advocates) утверждают, что в обозримом будущем она станет неотъемлемым аспектом повседневной жизни, поскольку люди будут использовать онлайн-3D-виртуальные среды для работы, образования, социального взаимодействия, развлечений и даже для получения жизненно важных услуг, таких как банковские услуги и здравоохранение. Так же будут использоваться смартфоны для доступа к цифровой сфере.

Естественно, амбициозное видение будущего имитированных миров, продвигаемое в основном крупными технологическими компаниями, опирается на несколько технологических прорывов в таких областях как дополненная реальность, виртуальная реальность, смешанная реальность (MR), пограничные вычисления, искусственный интеллект (AI), 5G, блокчейн, невзаимозаменяемые токены (Non-Fungible Tokens (NFT)) и другие децентрализованные приложения. Это развитие будет влиять на рост онлайн-преступлений, подчёркивая необходимость глобального сотрудничества в борьбе с преступлениями в имитированных мирах и разработке международных договоров, специфичных для цифровых пространств.

Технологии предотвращения онлайн-преступлений. Значительная роль в предотвращении онлайн-преступлений в имитированных мирах отдаётся различным технологическим решениям, которые можно внедрить для снижения риска киберпреступлений, включая аутентификацию, шифрование и мониторинг [23]. Ещё один способ, которым пользователь может обеспечить свою безопасность, – это постоянно обновлять программное обеспечение.

Аутентификация – это процесс проверки личности пользователя. В цифровом имитированном пространстве аутентификация может использоваться для предотвращения несанкционированного доступа к учётным записям пользователей и цифровым активам. Одним из эффективных методов аутентификации является двухфакторная аутентификация (2FA), которая требует от пользователей предоставления двух форм идентификации, таких как пароль (то, что вы знаете) и код, отправленный на их мобильное устройство [24], или токен (то, чем вы владеете), или может потребовать сканирования пользователя – отпечатка пальца или лица в случае входа с мобильных устройств (биометрия).

Шифрование – это процесс преобразования данных в код для предотвращения несанкционированного доступа.

Шифрование может использоваться для защиты пользовательских данных, транзакций с цифровыми активами и другой конфиденциальной информации в имитированном мире. Администраторы имитированных миров могут внедрять шифрование, используя защищённые протоколы связи, такие как протокол транспортного уровня (TLS) и протокол защищённых сокетов (SSL) [25, с. 2126–2129].

Мониторинг – это процесс наблюдения за активностью пользователей в целях обнаружения подозрительного поведения. В имитированном пространстве мониторинг может использоваться для обнаружения кибербуллинга, фишинговых атак и других видов онлайн-преступлений.

Администраторы имитированных миров могут отслеживать активность пользователей, анализируя пользовательские данные и внедряя автоматизированные инструменты мониторинга.

Меры реагирования на онлайн-преступления. Меры реагирования – это те меры, которые могут быть предприняты в ответ на онлайн-преступления в имитированных мирах. Они включают расследование, судебное следствие и восстановление прав пострадавшей стороны.

Расследование представляет собой процесс сбора доказательств и информации для идентификации лица, совершившего онлайн-преступление. В имитированных мирах расследование усложняется из-за их анонимного характера. Однако администраторы имитированных пространств могут внедрять инструменты для отслеживания активности пользователей и расследования онлайн-преступлений [26, с. 1–5].

Преследование – это процесс предъявления обвинений лицу, совершившему онлайн-преступление. В имитированных цифровых пространствах преследование может быть сложным из-за юрисдикционных вопросов и сложности идентификации лиц, совершивших преступление. Однако администраторы

виртуальных миров могут сотрудничать с правоохранительными органами для возбуждения дел против киберпреступников [27, с. 1–9].

Восстановление – процесс возвращения жертвы онлайн-преступления в состояние, предшествующее инциденту. В имитированных пространствах это может включать в себя восстановление украденных или уничтоженных цифровых активов, а также предоставление консультационных услуг жертвам кибербуллинга и внедрение более надёжных мер безопасности для предотвращения подобных инцидентов в будущем.

Заключение. Таким образом, онлайн-преступность в имитированных мирах представляет собой проблему, требующую серьёзного внимания со стороны всех заинтересованных сторон. Разрабатывая чёткие правила, внедряя эффективные превентивные меры и создавая новые технологии и стратегии, можно создать такие условия, чтобы имитированные цифровые пространства оставались безопасной и защищённой средой для всех пользователей.

Список источников

1. Innocente C., Nonis F., Ruggieri R., Ulrich L., Vezzetti E. A Metaverse Platform for Preserving and Promoting Intangible Cultural Heritage // *Applied Sciences* (Basel, Switzerland). – 2024. – № 14 (8), 3426. DOI: 10.3390/app14083426.
2. Khalifa E. Potential Threats: Extremism and Terrorism in the Metaverse // *Forecasting Cyber Crimes in the Age of the Metaverse*. – 2024. – P. 171–181.
3. Teodorov A.-V. Cybercrimes in the Metaverse: Challenges and Solutions // *International Conference on Cybersecurity and Cybercrime*. – 2023. – P. 209–215. DOI: 10.19107/CYBERCON.2023.28.
4. El-Kady R.M. Handling E-evidence in Egyptian and Comparative Legislation: A Comparative Analytical Study // *Arab Journal of Forensic Sciences & Forensic Medicine*. – 2023. – № 6 (1). – P. 37–68. DOI: 10.26735/WGZY6322.
5. Citi GPS. Metaverse and Money, Decrypting the Future [Электронный ресурс] // URL: https://icg.citi.com/icghome/what-we-think/citigps/insights/metaverse-and-money_20220330 (дата обращения: 14.07.2026).
6. Büyükbaykal A., Sönmezer Z. The Relationship Between Metaverse and Social Life // *International Journal of Cultural and Social Studies*. – 2022. – № 8 (1). – P. 139–148.
7. Riva G., Wiederhold B., Mantovani F. Searching for the Metaverse: Neuroscience of Physical and Digital Communities // *Cyberpsychology, Behavior, and Social Networking*. – 2024. – № 27 (1). – P. 9–18. DOI: 10.1089/cyber.2023.0040.
8. Wu C., Li Y. The Metaverse: Exploring the Convergence of Technologies and Social Dynamics // *2023 IEEE 43rd International Conference on Distributed Computing Systems Workshops (ICDCSW)*. – 2023. – P. 121–126. DOI: 10.1109/ICDCSW60045.2023.00019.

9. Wang Y., Su Z., Zhang N., Liu D., Xing R., Luan T., Shen X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy // *IEEE Communications Surveys and Tutorials*. – 2023. – № 25 (1). – P. 319–352. DOI: 10.1109/COMST.2022.3202047.
10. Цыплакова А.Д. Противодействие киберпреступлениям в отдельных странах Глобального Юга: дис. ... канд. юрид. наук / А.Д. Цыплакова. – М., 2025. – 368 с.
11. Camber R. British police probe VIRTUAL rape in metaverse: Young girl's digital persona is sexually attacked by a gang of adult men in immersive video game'-sparking the first investigation of its kind and questions about the extent current laws apply in the online world [Электронный ресурс] // *Daily Mail: сайт*. URL: <https://www.dailymail.com/news/article-12917329/Police-launch-investigation-kind-virtual-rape-metaverse.html> (дата обращения: 14.07.2026).
12. Zhou Y., Tiwari M., Bernot A., Lin K. Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality // *Asian Journal of Criminology*. – 2024. – № 19 (3). – P. 419–439. DOI: 10.1007/s11417-024-09436-y.
13. Oladokun Bolaji David, Ebieri Diana Orubebe, Yusuf Ajani, Yinka Martins Omoniyi, Edidiong Nyong Ben. Cyber Threats and Safeguarding Strategies in Metaverse Libraries: A Systematic Review // *Southern African Journal of Security*. – 2024. – 15 p. DOI: 10.25159/3005-4222/17806.
14. Lee D.I. A Study on the Countermeasures of Avatar Sex Crime. *Forum of Public Safety and Culture* // *Forum of Public Safety and Culture* 19. – 2022. – P. 155–170. DOI: 10.52902/kjsc.2022.19.155.
15. Jibril M. The Legal Challenges of Metaverse Technology from the Criminal Point of View (Cairo: Dar Al-Ahram for Legal Publications).
16. Qin H.X., Wang Y., Hui P. Identity, Crimes, and Law Enforcement in the Metaverse // *Humanities and Social Sciences Communications* 12. – 2025. – № 194. <https://doi.org/10.1057/s41599-024-04266-w/>.
17. Bovenzi G. MetaCrimes: Criminal accountability for conducts in the Metaverse // *Companion Proceedings of the ACM Web Conference*. – 2023. – P. 565–567. <https://doi.org/DOI: 10.1145/3543873.3587535>.
18. Kostenko O., Zhuravlov D., Dniprov O., Korotiuk O. METAVERSE: MODEL CRIMINAL CODE // *Baltic Journal of Economic Studies*. – 2023. – Vol. 9, № 4. – P. 134–147. <https://doi.org/DOI: 10.30525/2256-0742/2023-9-4-134-147>.
19. Wu J., Lin K., Lin D., Zheng Z., Huang H., Zheng Z. Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities // *IEEE Open Journal of the Computer Society*. – 2023. – Vol. 4. – P. 37–49. DOI: 10.1109/OJCS.2023.3245801.
20. Lee J., Min H. Review of legal protection measures against security threats related to Metaverse // *Korean Journal of Public Safety and Criminal Justice*. – 2022. – Vol. 31, № 3. – P. 321–344.

21. Petrigna L., Musumeci G. The Metaverse: A New Challenge for the Healthcare System: A Scoping Review // *Journal of Functional Morphology and Kinesiology*. – 2022. – № 7 (3), 63. DOI: 10.3390/jfkmk7030063.
22. Приводится по: Лунеев В.В. Курс мировой и российской криминологии: учебник: в 2 т. Т. 1. Общая часть / В.В. Лунеев. – М.: Юрайт, 2011. – 1003 с.
23. R. K. Sharma and S. S. Tyagi. Security issues in virtual worlds // 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India. – 2017. – P. 1212–1215. DOI: 10.1109/ICCMC.2017.8074659.
24. N. G. Carr, M. F. M. Yassin. Two-factor authentication in virtual worlds // 2014 International Conference on Information Science, Electronics and Electrical Engineering (ISEEE), Sapporo, Japan. – 2014. – P. 1843–1846. DOI: 10.1109/InfoSEEE.2014.6947985.
25. Y. Sun, L. Zhao, J. Zhao and Y. Shen. Design and implementation of security encryption in virtual world // 2011 International Conference on Electric Information and Control Engineering, Wuhan, China. – 2011. – P. 2126–2129. DOI: 10.1109/ICEICE.2011. 5777899.
26. S. R. Patil, S. R. Suralkar. Detection of cyberbullying in virtual world // 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India. – 2017. – P. 1–5. DOI: 10.1109/ICCUBEA.2017.8329707.
27. J. C. Yang, J. C. Chen, C. H. Wu. Detection of unauthorized virtual money transactions in online games // *Journal of Network and Computer Applications*. – 2010. – Vol. 33, № 1. – P. 1–9.

References

1. Innocente C., Nonis F., Ruggieri R. et al. A Metaverse Platform for Preserving and Promoting Intangible Cultural Heritage. *Applied Sciences (Basel, Switzerland)*, 2024, no. 14 (8), 3426. DOI: 10.3390/app14083426. (In English).
2. Khalifa E. Potential Threats: Extremism and Terrorism in the Metaverse. Forecasting Cyber Crimes in the Age of the Metaverse, 2024, pp. 171–181. (In English).
3. Teodorov A.-V. Cybercrimes in the Metaverse: Challenges and Solutions. *Materials of the International Conference on Cybersecurity and Cybercrime*. 2023, vol. 10, pp. 209–215. DOI: 10.19107/CYBERCON.2023.28. (In English).
4. El-Kady R.M. Handling E-evidence in Egyptian and Comparative Legislation: A Comparative Analytical Study. *Arab Journal of Forensic Sciences & Forensic Medicine*, 2023, no. 6 (1), pp. 37–68. DOI: 10.26735/WGZY6322. (In English).
5. Ghose R., Bantanidis S., Burke J. et al. Citi GPS. Metaverse and Money, Decrypting the Future. *Technology & Innovation*, 2022. Available at: https://icg.citi.com/icghome/what-we-think/citigps/insights/metaverse-and-money_20220330. (In English).
6. Büyükbaykal A., Sönmezer Z. The Relationship Between Metaverse and Social Life. *International Journal of Cultural and Social Studies*, 2022, no. 8 (1), pp. 139–148. (In English).

7. Riva G., Wiederhold B., Mantovani F. Searching for the Metaverse: Neuroscience of Physical and Digital Communities. *Cyberpsychology, Behavior, and Social Networking*, 2024, no. 27 (1), pp. 9–18. DOI: 10.1089/cyber.2023.0040. (In English).
8. Wu C., Li Y. The Metaverse: Exploring the Convergence of Technologies and Social Dynamics. *Materials of the 43rd International Conference on Distributed Computing Systems Workshops (ICDCSW), Hong Kong, July, 18-21, 2023*. IEEE, 2023, pp. 121–126. DOI: 10.1109/ICDCSW60045.2023.00019. (In English).
9. Wang Y., Su Z., Zhang N. et al. A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys and Tutorials*, 2023, no. 25 (1), pp. 319–352. DOI: 10.1109/COMST.2022.3202047. (In English).
10. Tsyplakova A.D. Countering Cybercrimes in Certain Countries of the Global South. *Cand. Diss. Moscow*, 2025, 368 p. (In Russian).
11. Camber R. British Police Probe VIRTUAL Rape in Metaverse: Young Girl's Digital Persona Is Sexually Attacked by a Gang of Adult Men in Immersive Video Game'-Sparking the First Investigation of Its Kind and Questions about the Extent Current Laws Apply in the Online World. Available at: <https://www.dailymail.com/news/article-12917329/Police-launch-investigation-kind-virtual-rape-metaverse.html>. (In English).
12. Zhou Y., Tiwari M., Bernot A. et al. Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*, 2024, no. 19 (3), pp. 419–439. DOI: 10.1007/s11417-024-09436-y. (In English).
13. Oladokun B. D., Orubebe E. D., Ajani Yu. Et al. Cyber Threats and Safeguarding Strategies in Metaverse Libraries: A Systematic Review. *Southern African Journal of Security*, 2024. 15 p. DOI: 10.25159/3005-4222/17806. (In English).
14. Lee D.I. A Study on the Countermeasures of Avatar Sex Crime. *Forum of Public Safety and Culture*, 2022, pp. 155–170. DOI: 10.52902/kjsc.2022.19.155. (In English).
15. Jibril M. The Legal Challenges of Metaverse Technology from the Criminal Point of View. Cairo, Dar Al-Ahram for Legal Publ. (In English).
16. Qin H.X., Wang Y., Hui P. Identity, Crimes, and Law Enforcement in the Metaverse. *Humanities and Social Sciences Communications*, 2025, no. 194. <https://doi.org/10.1057/s41599-024-04266-w/>. (In English).
17. Bovenzi G. Meta Crimes: Criminal Accountability for Conducts in the Metaverse. *Companion Proceedings of the ACM Web Conference, Austin, 30 April 2023 – 4 May, 2023*. ACM, 2023, pp. 565–567. <https://doi.org/DOI:10.1145/3543873.3587535>. (In English).
18. Kostenko O., Zhuravlov D., Dniprov O. et al. Metaverse: Model Criminal Code. *Baltic Journal of Economic Studies*, 2023, vol. 9, no. 4, pp. 134–147. <https://doi.org/10.30525/2256-0742/2023-9-4-134-147>. (In English).
19. Wu J., Lin K., Lin D. et al. Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities. *IEEE Open Journal of the Computer Society*, 2023, vol. 4, pp. 37–49. DOI: 10.1109/OJCS.2023.3245801. (In English).

20. Lee J., Min H. Review of Legal Protection Measures against Security Threats Related to Metaverse. *Korean Journal of Public Safety and Criminal Justice*, 2022, vol. 31, no. 3, pp. 321–344. (In English).
21. Petrigna L., Musumeci G. The Metaverse: A New Challenge for the Healthcare System: A Scoping Review. *Journal of Functional Morphology and Kinesiology*, 2022, no. 7 (3), 63. DOI: 10.3390/jfmk7030063. (In English).
22. Luneev V.V. Course of World and Russian Criminology: Textbook. Moscow, Yurayt, 2011. 1003 p. (In Russian).
23. Sharma R. K., Tyagi S. S. Security Issues in Virtual Worlds. *Materials of International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2017*. India, 2017, pp. 1212–1215. DOI: 10.1109/ICCMC.2017.8074659. (In English).
24. Carr N.G., Yassin M. F.M. Two-Factor Authentication in Virtual Worlds. *Materials of International Conference on Information Science, Electronics and Electrical Engineering, Sapporo, Japan, 26–28, April, 2014*. Japan, 2014, pp. 1843–1846. DOI: 10.1109/InfoSEEE.2014.6947985. (In English).
25. Sun Y., Zhao L., Zhao J. et al. Design and Implementation of Security Encryption in Virtual World. *Materials of International Conference on Electric Information and Control Engineering, Wuhan, China, 2011*. China, 2011, pp. 2126–2129. DOI: 10.1109/ICEICE.2011. 5777899. (In English).
26. Patil S.R., Suralkar S.R. Detection of Cyberbullying in Virtual World. *Materials of International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017*. India, 2017, pp. 1–5. DOI: 10.1109/ICCUBEA.2017.8329707. (In English).
27. Yang J.C., Chen J.C., Wu C.H. Detection of Unauthorized Virtual Money Transactions in Online Games. *Journal of Network and Computer Applications*, 2010, vol. 33, no.1, pp. 1–9. (In English).

Информация об авторах

Иванова Елена Вячеславовна – доктор юридических наук, доцент, декан факультета подготовки криминалистов ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации им. А.Я. Сухарева», профессор кафедры судебной экспертизы и уголовно-правовых дисциплин ГОУ ВО МО «Государственный социально-гуманитарный университет»

Information about the Authors

Ivanova Elena Vyacheslavovna –Doctor of Law, Associate Professor, Dean of the Faculty of Forensic Science Training, A.Ya. Sukharev Moscow Academy of the Investigative Committee of the Russian Federation; Professor of the Department of Forensic Expertise and Criminal Law Disciplines, State Social and Humanitarian University of Moscow Region;

Никитина Ирина Эдуардовна – доктор юридических наук, доцент кафедры информационных технологий и организации расследований киберпреступлений факультета криминалистики Московской академии следственного комитета им. А.Я. Сухарева; профессор кафедры философии, социологии и политологии им. Г.С. Арефьевой Федерального государственного бюджетного образовательного учреждения высшего образования «Национальный исследовательский университет «МЭИ»

Nikitina Irina Eduardovna – Doctor of Law, Associate Professor of the Department of Information Technologies and Cybercrime Investigation, Faculty of Criminalistics, A.Ya. Sukharev Moscow Academy of the Investigative Committee; Professor of the Department of Philosophy, Sociology, and Political Science named after G.S. Arfyeva, National Research University “MPEI”

Статья поступила в редакцию 15.07.2026 г.; одобрена после рецензирования 06.08.2026 г.; принята к публикации 07.08.2026 г.

The article was submitted 15.07.2026; approved after reviewing 06.08.2026; accepted for publication 07.08.2026.