УДК 343, 349 DOI: 10.31249/iajpravo/2026.01.09

# МАДЖУМАЕВ М.М.[1] УГОЛОВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА В ТРАНСГРАНИЧНЫХ МЕТАВСЕЛЕННЫХ[2]

***Аннотация***. Статья посвящена проблеме действия уголовного закона в трансграничных метавселенных. Установлено, что традиционные принципы (территориальности, гражданства) и существующие разъяснения Верховного Суда РФ неэффективны в атерриториальной цифровой среде. Это создает юрисдикционный вакуум, угрожает цифровому суверенитету и ведет к доминированию lex informatica (частноправового регулирования платформ). В статье критически оцениваются существующие подходы и предлагаются новые решения. Среди них внедрение доктрины эффекта (по месту наступления существенных последствий), механизм «приземления» IT-операторов, юрисдикция дистрибуции (контроль над магазинами приложений) и концепция суверенизации цифровой личности (государственно-верифицированный аватар) для обеспечения уголовно-правовой защиты прав граждан.

***Ключевые слова***: метавселенная; действие уголовного закона в пространстве; коллизии юрисдикции; цифровой суверенитет; децентрализация; юрисдикция дистрибуции; суверенизация цифровой личности; аватар; цифровой двойник человека; деанонимизация.

## MADZHUMAYEV M.M. Criminal legal maintenance of state sovereignty in cross-border metaverse

[1] © *Маджумаев Мурад Мамедович*, ведущий научный сотрудник, старший преподаватель кафедры уголовного права, уголовного процесса и криминалистики Юридического института Российского университета дружбы народов им. Патриса Лумумбы, кандидат юридических наук.

[2] Исследование выполнено за счет гранта Российского научного фонда № 25-28-01478, https://rscf.ru/project/25-28-01478/

***Abstract.*** The paper addresses the challenge of the application of criminal law in cross-border metaverses. Conventional principles (territoriality, citizenship) and existing interpretations from the Supreme Court of the Russian Federation are found to be ineffective in the aterritorial digital environment. This creates a jurisdictional vacuum, threatens digital sovereignty, and leads to the dominance of lex informatica (private law regulation of platforms). The article critically assesses existing approaches and proposes new solutions. Among them is the introduction of the effect doctrine (based on the place where the essential consequences occur), a grounding mechanism for IT operators, distribution jurisdiction (control over app stores), and the concept of digital persona sovereignty (state-verified avatar) to ensure criminal law protection of citizens' rights.

***Keywords***: metaverse; spatial application of criminal law; conflicts of jurisdiction; digital sovereignty; decentralization; distribution jurisdiction; digital persona sovereignty; avatar; human digital twin; deanonymization.

***Для цитирования***: Маджумаев М.М. Уголовно-правовое обеспечение безопасности государственного суверенитета в трансграничных метавселенных // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2026. – № 1. – С. 142–157. – DOI: 10.31249/iajpravo/2026.01.09

## Введение
## Коллизионный потенциал атерриториальных пространств и проблема цифрового суверенитета

Ускоренная цифровизация и внедрение сложных вычислительных систем в ткань общественных отношений требуют от правовой науки переоценки консервативных доктринальных подходов и перехода к проактивному формированию адаптивной нормативной среды. Неспособность существующих юридических институтов адекватно и своевременно реагировать на экспоненциальный рост технологических инноваций создает опасный вакуум регулирования, чреватый не только дестабилизацией социально-экономических процессов, но и эрозией фундаментальных основ правопорядка, включая государственный суверенитет. В таких вопросах право не может занимать позицию дисциплинарного изоляционизма. Аналогичным образом сама траектория развития научно-

технических инноваций требует соответствующего правового регулирования.

Стремительное развитие иммерсивных технологий и формирование глобальных, устойчивых и интерактивных виртуальных сред, объединенных концепцией «метавселенной»[1], знаменует собой не только технологическую, но и фундаментальную правовую революцию. Метавселенная, т.е. иммерсивное, синхронное и интероперабельное цифровое пространство[2] создает новую сферу для социально значимого взаимодействия. Эти трехмерные пространства параллельной реальности функционируют независимо от присутствия в них конкретных пользователей, которые представлены аватарами (цифровыми двойниками).

В то время как общественные отношения в объективной реальности физического мира (и некоторые цифровые взаимоотношения) регулируются принципами государственного суверенитета и территориальной юрисдикции, метавселенные функционируют как бесшовное, нетерриториальное (или надтерриториальное) пространство. Именно такая трансформация инициирует фундаментальный кризис существующих принципов действия уголовного (и не только) закона в пространстве, которые исторически и концептуально основаны на незыблемости физической географии и государственного суверенитета, проистекающего из контроля над ней.

Правопорядок, являясь главной функцией государства, сталкивается с беспрецедентной сложностью реализации в средах, которые по своей архитектуре атерриториальны, децентрализованы, зачастую анонимизированы и находятся под операционным управлением частных, преимущественно иностранных (транснациональных), корпораций. Классическая вестфальская модель, основанная на жесткой корреляции суверенитета и физической территории[3], демонстрирует свою функциональную исчерпанность.

[1] Benaben F., Congès A., Fertier A. A Prospective Vision of the Evolution of Immersive Technologies: Towards a Definition of Metaverse // Technovation. – 2025. – Vol. 140. – P. 103–154. – URL: https://doi.org/10.1016/j.technovation.2024.103154 (дата обращения 24.11.2025).

[2] Murala D.K., Panda S.K. Metaverse: A Study on Immersive Technologies // Metaverse and Immersive Technologies: An Introduction to Industrial, Business and Social Applications. – 2023. – P. 1–41. – URL: https://doi.org/10.1002/9781394177165.ch1 (дата обращения 24.11.2025).

[3] Hu H. Revisiting Territorial Sovereignty: Origins, Legitimacy, and Modern Implications // San Diego International Law Journal. – 2024. – Vol. 26. – P. 1. – URL: https://digital.sandiego.edu/ilj/vol26/iss1/2/ (дата обращения 24.11.2025).

Возникающий де-юре юрисдикционный вакуум де-факто неминуемо заполняется квазиюрисдикцией операторов платформ, устанавливающих собственные правила компьютерным кодом в виде различных компьютерных программ или компьютерных протоколов, в совокупности называемых lex informatica.

## Пределы применимости территориальной юрисдикции в атерриториальных пространствах метавселенных

Принцип территориальности (ст. 11 УК РФ), являющийся краеугольным камнем российского уголовного права, устанавливает юрисдикцию государства над преступлениями, совершенными на его территории. Однако в метавселенной само понятие locus delicti (места совершения преступления) становится неопределенным. Требуется разрешение коллизии относительно территориальной юрисдикции применительно к совершенному деянию в таких средах:

а) по месту нахождения пользователя-субъекта общественно опасного деяния. Для этого требуется его физическая локализация, что крайне затруднительно в условиях анонимности и использования программно-аппаратных средств туннелирования, шифрования и подмены IP-адреса[1] при доступе к информационным ресурсам, информационно-телекоммуникационным сетям (VPN);

б) по месту нахождения пользователя-жертвы. Аналогичная проблема идентификации и локализации;

в) по месту нахождения серверов, на которых размещена метавселенная (его платформы). Серверы могут быть распределены по разным государствам, использовать облачную инфраструктуру, а сама платформа может быть децентрализованной (например, на базе блокчейна), не имея единого центра управления;

г) в самом виртуальном пространстве. Оно не имеет географических координат и не является суверенной территорией какого-либо государства.

[1] A survey on edge computing (EC) security challenges: Classification, threats, and mitigation strategies / A.M. Sheikh, M.R. Islam, M.H. Habaebi, S.A. Zabidi, A.R. Bin Najeeb, A. Kabbani, // Future Internet. – 2025. – Vol. 17, N 4. – C. 175. – URL:https://doi.org/10.3390/fi17040175; Location privacy-preserving mechanisms in location-based services: A comprehensive survey // ACM Computing Surveys (CSUR / Hongo Jiang, Jie Li, Ping Zhao, Fansi Zeng, Zhu Xiao, Arun Iyengar. – 2021. – Vol. 54, N 1. – C. 1–36. – URL: https://doi.org/10.1145/3423165 (дата обращения 24.11.2025).

В результате правоприменитель сталкивается с *негативными коллизиями* юрисдикции (когда ни одно государство не может с уверенностью обосновать свою компетенцию, что может порождать отвратимость наказания) и *позитивными коллизиями* (когда несколько государств одновременно претендуют на юрисдикцию, например первая страна – по месту нахождения жертвы, вторая страна по месту регистрации корпорации-владельца, третья страна по месту нахождения дата-центра).

Высшая судебная инстанция Российской Федерации предприняла попытку адаптации упомянутого принципа к цифровой среде. В п. 19 постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”», разъясняется, что местом совершения такого преступления является «территория, на которой лицом использовалось компьютерное устройство» для выполнения действий, входящих в объективную сторону деяния. Данный подход, стремящийся найти материальный след в физическом мире, на первый взгляд представляется логичным, однако применительно к метавселенным он демонстрирует свою теоретическую и практическую несостоятельность.

Во-первых, эта позиция основана на опровержимой презумпции возможности установления реального местонахождения устройства. В условиях, когда использование средств анонимизации, делающих определение реального IP-адреса, а значит и «территории, на которой... использовалось... устройство», невозможным без содействия оператора платформы и провайдеров VPN (VPN, Tor, каскадные прокси-серверы), является не исключением, а правилом для любого технически «грамотного» злоумышленника; «территория... устройства» становится юридической фикцией, неустановимым обстоятельством. Правоприменитель, связанный таким разъяснением, как представляется, ставится в процессуальный тупик, поскольку юрисдикция государства становится зависимой не от воли законодателя, а по сути от уровня технической компетенции преступника. По формуле Пленума, юридически юрисдикция имеется (если удастся найти устройство), но фактически она недоказуема, так как для установления местонахождения устройства требуются международные следственные поручения,

которые будут исполняться годами или не исполняться вовсе, особенно с учетом турбулентности международных отношений.

Во-вторых, разъяснение Пленума игнорирует архитектуру современных цифровых (мета)преступлений. Деяние может совершаться не с одного устройства, а распределенно (DDoS), через ботнет, сеть зараженных устройств[1], находящихся в нескольких государствах, либо с использованием арендованных облачных мощностей[2], физическое расположение которых не совпадает ни с местом нахождения субъекта деяния, ни с местом нахождения жертвы. Более того, в децентрализованных метавселенных, функционирующих на базе технологий распределенного реестра (блокчейн)[3], отсутствует единый сервер, а устройство пользователя является лишь одним из тысяч равноправных узлов сети. В такой парадигме попытка локализовать locus delicti через одно устройство теряет всякий смысл.

В-третьих, делая неправомерный акцент на месте действия (locus actus), Пленум умаляет значение места наступления последствий (locus consequentiae). Для материальных составов, таких как мошенничество (ст. 159 УК РФ), в результате которого у российского гражданина списаны денежные средства со счета в российском банке, именно территория наступления вредоносного результата представляет собой гораздо более устойчивый и юридически значимый юрисдикционный базис, нежели эфемерное и зачастую недоказуемое местоположение устройства злоумышленника.

[1] Computer Crimes // American Criminal Law Review. Annual Survey of White Collar Crime / S. Bhatter, S. Hilsabeck, F. Sullivan, B. Barry. – 2025. – Vol. 62, N 3. – P. 441. – URL: https://www.law.georgetown.edu/american-criminal-law-review/aswcc/ (дата обращения 24.11.2025); Singh T. Understanding Cybercrime and Criminology // Cybersecurity, Psychology and People Hacking. Palgrave Studies in Cyberpsychology. Palgrave Macmillan. – Cham: Springer Nature Switzerland, 2025. – P. 1–15. – URL: https://doi.org/10.1007/978-3-031-85994-6_1 (дата обращения 24.11.2025).

[2] Patsakis C., Arroyo D., Casino F. The Malware as a Service Ecosystem // Malware: Handbook of Prevention and Detection. – Cham: Springer Nature Switzerland, 2024. – P. 371–394. – URL: https://doi.org/10.1007/978-3-031-66245-4_16 (дата обращения 24.11.2025).

[3] Omar M. Blockchain Technology: Enhancing Security in a Decentralized World // Defense in Depth: Modern Cybersecurity Strategies and Evolving Threats / The Institute of Electrical and Electronics Engineers, Inc. – Wiley, 2025. – C. 99–125. – URL: https://doi.org/10.1002/9781394340750.ch5 (дата обращения 24.11.2025).

**Иллюзия альтернативных принципов и угроза lex informatica**

В доктрине нередко высказывается мнение, что описанный кризис территориальности не является нерешимой проблемой, поскольку национальное законодательство (в частности статья 12 УК РФ) содержит альтернативные юрисдикционные основания, принцип активного (субъект преступления – гражданин РФ) и пассивного (жертва преступления – гражданин РФ) подданства[1]. Сторонники данной позиции утверждают, что если потерпевшим (еще шире – жертвой) от общественно опасного деяния в цифровой среде (в нашем случае в метавселенной) является гражданин РФ, государство вправе применить принцип пассивного гражданства (ч. 3 ст. 12 УК РФ) и осуществить уголовное преследование, независимо от физического места преступления.

Однако подобная аргументация, будучи формально-юридически верной, смешивает два фундаментально различных аспекта: юрисдикцию устанавливать нормы (jurisdiction to prescribe) и юрисдикцию обеспечивать их принудительное исполнение (jurisdiction to enforce)[2]. Безусловно, Российская Федерация вправе декларировать свою юрисдикцию на основании гражданства потерпевшего или субъекта преступления (в случаях, когда он находится не в пределах РФ). Но практическая реализация этого права, сбор доказательств, установление личности преступника, получение логов его действий наталкивается на необходимость получения содействия от оператора платформы, находящегося, как правило, в иностранной (иногда и недружественной) юрисдикции. Это инициирует громоздкий и в современных геополитических реалиях практически неработающий механизм международного сотрудничества (запросы о правовой помощи). Сроки исполнения таких запросов, исчисляемые месяцами и годами, не коррелируют со сроками жизни цифровых доказательств (часы или дни). Кроме того, применение ч. 3 ст. 12 УК РФ обусловлено требованием двойной криминализации (деяние должно быть наказуемо и в го-

[1] Payer A. The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries // International Criminal Law Review. – 2023. – Т. 23, № 2. – С. 175–238. – URL: https://doi.org/10.1163/15718123-bja10151 (дата обращения 24.11.2025).

[2] Sinha R., Talmon S. Germany's Position on an 'International Network Law' // GPIL-German Practice in International Law. – 2024. – P. 5. – URL: https://d-nb.info/134687655X/34 (дата обращения 24.11.2025).

сударстве, где оно совершено). Учитывая неопределимость места совершения преступления и правовую неквалифицированность многих виртуальных посягательств (например, хищение аватара) в законодательстве страны хостинга, это условие часто становится невыполнимым.

При этом следует отметить положительным принятие по инициативе Российской Федерации Всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (далее – Конвенция; Конвенция ООН против киберпреступности[1]), которая создает новую правовую реальность и предлагает инструменты для решения именно тех проблем, которые обозначены выше. Хотя Конвенция в главе III (ст. 22) во многом содержит существующие юрисдикционные подходы (территориальный, активный и пассивный персональный), ее подлинная ценность заключается не в создании новых юрисдикционных оснований, а в имплементации новых процессуальных механизмов принудительного исполнения, направленных на преодоление процедурного тупика и «разрыва в скорости» между длящимися месяцами запросами и исчезающими за часы цифровыми доказательствами.

Ключевой проблемой при расследовании преступлений в метавселенных, как было изложено, является неспособность государства оперативно получить цифровые доказательства (логи, данные о пользователе) от иностранного оператора платформы. Конвенция ООН предлагает для этого конкретные решения. Во-первых, предполагается создание сетей 24/7 (ст. 41). Конвенция обязывает каждое государство-участника назначить «контактный центр, работающий 24 часа в сутки семь дней в неделю для обеспечения предоставления неотложной помощи» по преследованию определенных преступлений. Это создает прямой, высокоскоростной канал связи между правоохранительными органами, минуя медленные дипломатические процедуры, для решения срочных задач. Во-вторых, и самое важное, предполагается создание механизмов оперативного обеспечения сохранности данных (ст. 42). Данная статья позволяет государству-участнику (например Рос-

[1] Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, принята резолюцией 79/243 Генеральной Ассамблеи от 24 декабря 2024 г.

сии) обратиться через сеть 24/7 к другому государству (где находится оператор метавселенной) с просьбой «оперативно обеспечить... сохранность электронных данных» (ст. 42.1). Самое главное, пунктом 4 ст. 42 Конвенции прямо устанавливается, что «обоюдное признание соответствующего деяния преступлением в качестве условия обеспечения такой сохранности не требуется».

Этим решается две из озвученных ранее проблем, снимаются вопросы быстрого реагирования и двойной криминализации. Запрос на сохранность (preservation) выполняется оперативно, что позволяет «заморозить» цифровые следы до их удаления. Барьер в виде отсутствия аналога преступления (например, «хищение аватара») в законодательстве запрашиваемой страны снимается на первом, самом важном этапе – этапе сохранения доказательств. Конвенция устанавливает, что сохранность данных обеспечивается на срок не менее 60 дней (ст. 42.8), что дает правоохранительным органам время на подготовку и направление уже формального запроса о взаимной правовой помощи (в соответствии со ст. 40 и 44) для получения доступа к этим данным. К моменту подачи формального запроса критически важные доказательства уже будут сохранены и не будут утеряны.

Тем не менее принятие Конвенции ООН против киберпреступности не устраняет полностью проблему своего рода «доминирования» lex informatica, но предоставляет государствам действенный многосторонний инструмент для укрепления jurisdiction to enforce. Она заменяет архаичные, неработающие механизмы запросов о правовой помощи на двухступенчатую систему:

1) немедленное сохранение данных без оглядки на двойную криминализацию через сеть 24/7;

2) последующее формальное истребование уже сохраненных данных.

Это значительно усиливает позиции национальных правоохранительных органов в борьбе с преступностью в трансграничных цифровых пространствах, включая метавселенные.

Вместе с тем встречается и иная точка зрения, исходящая из либертарианского подхода и поддерживаемая операторами платформ, которая заключается в том, что юрисдикционный вакуум формально не является проблемой, так как на деле он эффективно заполняется частноправовым регулированием транснациональных корпораций[1]

[1] Lessig L. Code: and Other Laws of Cyberspace. – 2 nd Revised ed. – New York: Basic Books, 2006. – 432 p.

(операторами метавселенных), пресловутым lex informatica. В этой парадигме условия предоставления услуг, пользовательские соглашения как бы заменяют уголовный закон, производством (расследованием) по делу занимается служба модерации, а наказанием – администратор платформы, применяющий бан, удаление аккаунта или конфискацию виртуальных активов.

Сторонники либертарианского подхода и представители цифровой индустрии видят в этом не проблему, а решение. Они указывают на эффективность такого «корпоративного» правосудия, оно транснационально, технически компетентно и, главное, оперативно[1]. Администратор платформы может заблокировать мошенника в течение минут, в то время как государственная система будет месяцами решать вопрос о подследственности.

Однако такая «приватизация» правосудия несет в себе экзистенциальную угрозу суверенитету. Во-первых, это прямое делегирование базовой функции государства (защиты граждан и монополии на принуждение) в руки частной, иногда иностранной, коммерческой структуры. Во-вторых, такое правосудие лишено каких-либо процессуальных гарантий, оно не знает презумпции невиновности, права на защиту, состязательности сторон и независимого суда. В-третьих, цели корпорации (прибыль, PR) и государства (правосудие) не совпадают. Корпорация может проигнорировать сложное мошенничество, но заблокирует пользователя за деяние, несущее репутационные риски, даже если оно не является преступным. Принятие status quo, как представляется, равносильно отказу государства от уголовно-правовой защиты своих граждан.

Цифровой суверенитет в данном контексте – это не столько контроль над цифровыми границами, сколько функциональная[2] способность государства обеспечивать верховенство своего права, защиту прав своих граждан и реализацию публичных интересов в цифровой среде. Обстоятельство, когда государство не может применить свой уголовный закон для защиты своего гражданина

[1] Schill S.W., Berger N. Eroding the Rule of Law through Private-Public Arbitration? // The Comparative Constitutional Foundations of Private-Public Arbitration. – Oxford, UK: Oxford University Press, 2025. – С. 92.

[2] Shokri A. Sovereignty in Cyberspace from the Viewpoint of International Law // Asian Journal of International Law. – 2025. – P. 1–31. – URL: https://www.cambridge.org/core/journals/asian-journal-of-international-law/article/sovereignty-in-cyberspace-from-the-viewpoint-of-international-law/2193733BFBAA268E7E211FA345942150 (дата обращения 24.11.2025).

от вымогательства в метавселенной, а единственным «защитником» выступает модератор платформы, зарегистрированной в другой стране, и будет эрозией суверенитета.

**Концептуализация расширительного толкования юрисдикции**

Необходимо разработать и легитимизировать новые доктринальные подходы к определению юрисдикции, адаптированные к цифровой реальности.

*1. Расширительное толкование территориальности (принцип эффекта или наиболее существенного воздействия)*

Следует отойти от жесткой привязки к физическому месту. Юрисдикция государства должна распространяться на любое преступление, существенные и предсказуемые вредоносные последствия которого наступают на его территории или направлены против ее граждан (независимо от их физического местонахождения в момент деяния). Этот подход (effects doctrine), давно применяемый в антимонопольном праве США[1], должен быть инкорпорирован в уголовное право. Если мошенничество в метавселенной привело к финансовому ущербу гражданина (списанию средств с его счета в банке) или причинению вреда его здоровью (например, доведение до самоубийства), место преступления должно признаваться находящимся в пределах такого государства. Это требует внесения уточнений в постановление Пленума ВС РФ о применении норм ст. 11–12 УК РФ.

*2. Концепция квазитерритории и цифрового присутствия*

В качестве доктринальной основы следует рассматривать цифровые аватары и аккаунты российских граждан как их цифровое представительство. Посягательство на аватар (например, неправомерный доступ, его хищение или использование для клеветы) должно приравниваться к посягательству на компьютерную информацию, личность или имущество гражданина, находящегося под юрисдикцией государства.

Интересным представляется введение института «приземления» для операторов метавселенных. Ключевым инструментом

[1] Martyniszyn M. Extraterritoriality in Competition Law: Progressing Narrowing of the Gaps // e-Competitions: National Competition Laws Bulletin. – 2024. – Special Issue on Extraterritoriality. Art. N 120291. – P. 2. – URL: https://pureadmin.qub.ac.uk/ws/portalfiles/portal/608361752/Extraterritoriality_in_Competition_Law-_Progressing_Narrowing_of_the_Gaps.pdf (дата обращения 24.11.2025).

восстановления суверенитета является механизм, аналогичный Федеральному закону от 01.07.2021 № 236-ФЗ (в ред. от 01.09.2022) «О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации» («о приземлении» IT-гигантов). Необходимо законодательно обязать операторов метавселенных, чья аудитория в России превышает установленный порог:

а) открывать полноценные филиалы или представительства в РФ;

б) локализовать данные российских пользователей на территории РФ (это в определенной степени уже реализовано Федеральным законом от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»);

в) создать интерфейс для оперативного взаимодействия с правоохранительными органами (СК РФ, МВД России, ФСБ России и др.).

Наличие юридического лица в Российской Федерации делает корпорацию субъектом российского права и позволяет применять к ней меры процессуального принуждения (запросы о предоставлении данных, обыски в представительстве) и ответственности (оборотных штрафов) за отказ в содействии расследованию. Это переводит проблему из плоскости международного права в плоскость внутригосударственного принуждения.

*3. Модернизация уголовно-процессуальных механизмов*

Полагаем, что УПК РФ должен быть дополнен нормами, регулирующими следственные действия в виртуальной среде, например:

а) виртуальный осмотр (процессуальная фиксация обстановки в метавселенной, при осмотре аватара, виртуального объекта, запись логов чата);

б) деанонимизация как мера принуждения (четкая процедура получения судебного разрешения на истребование у оператора платформы (ее российского представительства) данных, позволяющих идентифицировать пользователя (IP-адрес, MAC-адрес, платежные данные));

в) обеспечение сохранности цифровых доказательств (механизм быстрого (по судебному решению) «замораживания» цифровых данных (логов, активов) на серверах оператора до их формального истребования).

*4. Опосредованное принуждение доктриной юрисдикции дистрибуции*

Этот подход предлагает наиболее прагматичный и асимметричный ответ на проблему юрисдикции обеспечивать их принудительное исполнение. Он основан на признании факта, что если государство не может дотянуться до серверов метавселенной в других странах, оно в полной мере контролирует каналы доступа к этому сервису на своей территории. Доступ к метавселенной осуществляется через клиентское программное обеспечение (приложение)[1], которое дистрибутируется через централизованные магазины приложений (App Store, Google Play, RuStore, Steam и т.д.). По своему содержанию такое решение, означает, что государство устанавливает юрисдикцию не над самой метавселенной, а над операторами дистрибуции программного обеспечения, легально действующими на российском рынке.

В законодательство (например, в Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 31.07.2025) «Об информации, информационных технологиях и о защите информации» вводится норма, обязывающая оператора магазина приложений (Apple, Google, VK) незамедлительно приостановить или удалить приложение (клиент метавселенной) по решению российского суда или уполномоченного органа (Роскомнадзор) в случае, если оператор данного приложения (метавселенной) систематически (например, дважды) отказывается исполнять законные требования российских правоохранительных органов (о предоставлении данных, деанонимизации, блокировке преступного контента)). Такое решение обладает высокой вероятностью эффективной реализации. Оно не требует экстерриториальных действий. Оно является классическим примером реализации суверенитета на своей территории в отношении субъектов (Apple, Google, VK), которые здесь физически и юридически присутствуют и получают прибыль. Для оператора метавселенной угроза удаления из App Store или Google Play на многомиллионном российском рынке является гораздо более весомым аргументом, чем символический штраф или трудноисполнимый запрос о правовой помощи. Это, по сути, опосредованное принуждение. Оператор метавселенной ставится перед выбором – сотрудничать с правоохранительными органами или

[1] Понкин И.В. Технологии киберметавселенных в государственном управлении: понятие и возможности применения // Право и государство: теория и практика. – 2024. – № 11 (239). – С. 291–294.

потерять доступ ко всем своим российским пользователям. Этот юрисдикционный рычаг смещает точку давления с неуязвимого разработчика на уязвимый канал его дистрибуции.

*5. Концепция суверенизации цифровой личности*

Данный подход является наиболее фундаментальным и предлагает изменить сам объект уголовно-правовой охраны. Проблема юрисдикции возникает потому, что аватар в метавселенной рассматривается как анонимный псевдоним. Предлагается ввести в правовое поле доктрину суверенной цифровой личности (далее – СЦЛ)[1].

Государство, по аналогии с выдачей физического паспорта, должно предложить гражданам (а для определенных видов деятельности обязать их) проходить процедуру создания государственно-верифицированной цифровой личности (например на базе усиленной Единой системы идентификации и аутентификации – ЕСИА), которая становится их единственным легальным представительством в метавселенных для совершения юридически значимых действий (экономических транзакций, заключения смарт-контрактов, владения цифровой собственностью).

С момента такой верификации эта суверенная цифровая личность становится юридическим продолжением гражданина РФ в цифровом пространстве. Она становится объектом, находящимся под прямой и безусловной уголовно-правовой защитой Российской Федерации, аналогично физической территории посольства. Любое посягательство на СЦЛ (ее неправомерный доступ, мошенничество с ее использованием, клевета в ее адрес) автоматически квалифицируется как преступление, совершенное против интересов, охраняемых законодательством России (по аналогии с принципом защиты, но в расширенном толковании).

В этом случае полностью снимается вопрос о месте преступления или местонахождении преступника. Сам факт посягательства на верифицированный государством цифровой объект (СЦЛ) является достаточным и неоспоримым юрисдикционным базисом для инициирования уголовного преследования в России. Этот под-

[1] См.: Акутин А.С., Бровко А.В. Реализация алгоритма доказательства с нулевым разглашением в технологии цифровой личности в управлении информационно-технологическими процессами предприятия // Вестник ВГУ. Сер. Системный анализ и информационные технологии. – 2024. – № 2. – С. 113–122; Литвинцева Е.А., Васекин А.С. Формирование цифрового суверенитета личности: коммуникативный аспект // Коммуникология. – 2024. – Т. 12, № 3. – С. 116–127.

ход не запрещает анонимность (можно сохранять анонимные аватары для общения), но он выводит из тени всю экономически и юридически значимую деятельность. Он не ищет юрисдикцию постфактум, а проактивно создает ее до-факта, распространяя суверенитет на новый, созданный государством цифровой объект.

## Заключение

Трансграничные метавселенные ставят перед национальным уголовным правом экзистенциальный вызов, обнажая архаичность его территориальных основ. Попытки механической адаптации, подобные разъяснениям Пленума Верховного Суда РФ в постановлении от 15.12.2022 № 37, являются паллиативом, не решающим проблему по существу. Доктринальные апелляции к принципам персональности процессуально несостоятельны (в первую очередь процедурно неисполнимы), а передача правосудия на откуп корпорациям (lex informatica) равносильна капитуляции суверенитета. Единственным жизнеспособным ответом является системная реформа, сочетающая введение новой доктрины функциональной юрисдикции, основанной на правовой связи с Российской Федерацией, и создание строгого процедурного механизма цифровых представительств для принудительного исполнения национальных судебных решений.

Независимо от места совершения деяния, уголовная юрисдикция Российской Федерации должна распространяться на преступления, совершенные в электронных или информационно-телекоммуникационных сетях, включая метавселенные, если:

а) основным и непосредственным объектом посягательства являются права, свободы или законные интересы гражданина РФ либо его цифровой идентификатор, верифицированный в установленном порядке (например, через ЕСИА);

б) объектом посягательства является цифровой или виртуальный актив (включая цифровые права), принадлежащий резиденту РФ и (или) учтенный в российских системах реестров или декларированный в Российской Федерации;

в) деяние функционально направлено на причинение вреда охраняемым интересам РФ, включая критическую информационную инфраструктуру, финансовую систему или общественный порядок на территории РФ.

Это дает формально-правовое основание (юрисдикцию) для начала уголовного преследования в России, наложения ареста на

российские счета жертвы (для предотвращения дальнейших списаний), объявления преступника в международный розыск и, главное, направления запроса оператору платформы на основании собственной юрисдикции.

Любая метавселенная (или иная платформа), превышающая порог, например, в 1 млн (количество следует проработать) российских пользователей, обязана не просто открыть юрлицо, а аккредитовать в России (например, при Минцифры или Роскомнадзоре) свое цифровое представительство. Это представительство по доверенности от материнской компании уполномочено принимать и немедленно передавать на исполнение законные требования российских судов и (в установленных законом случаях) следственных органов. И, самое важное, представительство должно обладать техническими ключами доступа (API), достаточными для оперативного исполнения решений. Не отправлять запрос в страну нахождения головной организации, а исполнить здесь и сейчас.

Только такой симбиоз обновленной доктрины и эффективного принуждения позволит государству восстановить монополию на уголовное преследование и обеспечить реальную защиту граждан в новой цифровой реальности.