РИСКИ МЕТАВСЕЛЕННЫХ И ВИРТУАЛЬНЫХ ПРОСТРАНСТВ

Е. В. Коротковская

Саратовский национальный исследовательский государственный университет им. Н. Г. Чернышевского, Россия
E-mail: korotkovskaya@yandex.ru

Метавселенная, как развивающаяся парадигма Интернета следующего поколения, направлена на создание полностью иммерсивного, гиперпространственно - временного и самоподдерживающегося виртуального общего пространства, в котором люди могут играть, работать и общаться. Однако серьезные вторжения в частную жизнь и нарушения безопасности метавселенной могут препятствовать ее широкому развертыванию. Метавселенные могут стать катализаторами угроз сейчас и в будущем. В статье представлен обзор основных рисков метавселенных и виртуальных пространств.

RISKS OF METAVERSES AND VIRTUAL SPACES

E. V. Korotkovskaya

The Metaverse, as a developing paradigm of the next-generation Internet, aims to create a fully immersive, hyperspace-time and self-sustaining virtual shared space in which people can play, work and communicate. However, serious invasions of privacy and security breaches of the metaverse may prevent its widespread deployment. Metaverses can become threat catalysts now and in the future. The article provides an overview of the main risks of metaverses and virtual spaces.

Прежде всего определимся с тем, что такое метавселенная. Metaverse (Метавселенная), буквально комбинация префикса “Meta” (что означает трансцендентность) и суффикс “verse” (сокращение от universe) – это, созданный компьютерный мир с последовательной системой ценностей и независимой экономической системой, связанной с физическим миром. Термин "Метавселенная" был введен Нилом Стивенсоном в его научно-фантастическом романе "Снежная катастрофа" в 1992 году. В этом романе люди в физическом мире входят в метавселенную (параллельный виртуальный мир) и живут в ней через цифровые аватары (по аналогии с физическим "я" пользователя) с помощью оборудования виртуальной реальности (VR). С момента своего первого появления концепция метавселенной все еще развивается, используя различные инструменты, такие как вторая жизнь [1], 3D виртуальные миры [2] и ведение журнала жизни [3]. Обычно метавселенная рассматривается как полностью иммерсивное, гиперпространственно - временное и самоподдерживающееся виртуальное совместное пространство, объединяющее тройственный физический, человеческий и цифровой миры [4]. Метавселенная признана развивающейся парадигмой Интернета следующего поколения после интернета и мобильных устройств. Таким образом, метавселенная – это конвергенция физической, дополненной и виртуальной реальности в общем онлайн - пространстве. Пример

взаимодействия метавселенной и реального мира – фильм «Первому игроку приготовиться».

Интернет- революции привела к тому, что пользователи могут, как цифровые аборигены, испытать альтернативную жизнь в виртуальности. Метавселенная объединяет множество новых технологий. В частности, digital twin (цифровой двойник) создает зеркальное отражение реального мира, VR и дополненная реальность (AR) обеспечивают погружение в 3D - опыт, 5G и за его пределами обеспечивают сверхвысокую надежность и сверхнизкую задержку соединений для массивных устройств метавселенной, пригодных для носки датчики и интерфейс мозг - компьютер (BCI) обеспечивают взаимодействие пользователя и аватара в метавселенной, искусственный интеллект (ИИ) позволяет создавать и визуализировать крупномасштабные метавселенные, а блокчейн и незаменяемый токен (NFT) играют важную роль в определении подлинных прав на активы метавселенной [5]. В настоящее время, с ростом популярности интеллектуальных устройств и зрелости поддерживающих технологий, метавселенная выходит из своего зачаточного состояния в наступающую реальность в ближайшем будущем. Metaverse в последнее время привлекает все большее внимание со всего мира, и многие технологические гиганты, такие как Facebook, Microsoft, Tencent и NVIDIA, объявили о своих проектах в Metaverse.

В частности, Facebook переименовал себя в “Meta”, чтобы посвятить себя созданию будущей метавселенной [6].

Какие же проблемы обеспечения безопасности метавселенной можно выделить сегодня?

Несмотря на многообещающие перспективы метавселенной, безопасность и вопросы конфиденциальности являются главными проблемами, которые препятствуют его дальнейшему развитию. В метавселенной может возникнуть широкий спектр нарушений безопасности и вторжений в частную жизнь - от управления массивными потоками данных, повсеместного профилирования пользователей, несправедливых результатов алгоритмов искусственного интеллекта до безопасности физической инфраструктуры и человеческих жизней. Во-первых, поскольку метавселенная объединяет в себе множество новейших технологий и систем, построенных на их основе, их уязвимости и внутренние недостатки также могут быть унаследованы метавселенной. Были случаи, связанные с новыми технологиями, такие, как захват носимых устройств или облачных хранилищ, кража виртуальных валют и неправомерное использование искусственного интеллекта для создания поддельных новостей. Во-вторых, благодаря переплетению различных технологий последствия существующих угроз могут усиливаться и становиться более серьезными в виртуальных мирах, в то время как могут возникать новые угрозы, несуществующие в физическом и киберпространстве, такие как виртуальное преследование и виртуальный шпионаж [7]. В частности, персональные данные, задействованные в метавселенной, могут быть более детализированными и беспрецедентно вездесущими для создания цифровой копии реального мира, которая открывает новые горизонты для преступлений с использованием частных больших данных [8].

Например, для создания виртуальной сцены с использованием алгоритмов искусственного интеллекта пользователи неизбежно будут носить носимые устройства AR / VR со встроенными датчиками для всестороннего сбора паттернов мозговых волн, выражений лица, движений глаз, рук, речи и биометрических характеристик, а также окружающей среды. Кроме того, поскольку пользователи должны быть однозначно идентифицированы в метавселенной, это означает, что гарнитуры, VR- очки или другие устройства могут быть использованы для незаконного отслеживания реального местоположения пользователей [9]. Наконец, хакеры могут использовать систему уязвимости и компрометирующие устройства как точки входа для вторжения в реальное оборудование, такое как бытовая техника, чтобы угрожать личной безопасности, и даже угрожать критическим инфраструктурам, таким как системы электросетей, высокоскоростные железнодорожные системы и системы водоснабжения, с помощью атак advanced persistent threat (APT) [10]. Тем не менее, существующие меры безопасности все еще могут быть неэффективны и не обладать адаптивностью для приложений метавселенной. В частности, внутренние характеристики метавселенной, включая иммерсивность, гиперпространственно- временную устойчивость, масштабируемость и гетерогенность, могут вызвать ряд проблем для эффективного обеспечения безопасности.

1) Полное погружение в метавселенную в режиме реального времени приносит не только чувственные удовольствия от безупречной виртуальной среды, но и проблемы безопасного объединения массивных мультимодальных чувствительных к пользователю больших данных для взаимодействия между пользователями и аватарами / средами.

2) Из- за углубляющегося размывания границы между реальным и виртуальным, метавселенная сделает факты и вымысел более запутанными, такими как события Deepfake (подделки), особенно для нормативных актов и цифровой криминалистики.

3) Масштабируемость в метавселенной указывают на то, что пользователи могут свободно перемещаться по различным субметавселенным одновременно в разных сценах и режимах взаимодействия, что также создает проблемы для обеспечения быстрой авторизации сервиса, аудита соответствия требованиям и обеспечения подотчетности при бесперебойном обслуживании.

4) Виртуальные миры в крупномасштабной метавселенной могут быть очень разнородными с точки зрения аппаратной реализации, коммуникационных интерфейсов и программного обеспечения, что так же создает огромные трудности взаимодействия.

Наиболее значимыми рисками метавселенных и виртуальных пространств выступают угрозы конфиденциальности в метавселенной.

Цифровая жизнь в метавселенной, конфиденциальность пользователя, включая конфиденциальность местоположения, привычки, стиль жизни и так далее, может быть нарушена в течение жизненного цикла услуг передачи данных, включая восприятие, передачу, обработку, управление и хранение данных. Перечислим основные угрозы конфиденциальности в метавселенной:

1) Повсеместный сбор данных. Для иммерсивного взаимодействия с аватаром требуются всепроникающие действия по профилированию пользователя на неоправданно детализированном уровне [8], включая выражения лица, движения глаз и рук, речь и биометрические характеристики, и даже паттерны мозговых волн. Кроме того, с помощью передовых технологий XR и HCI можно облегчить анализ физических движений и даже включить отслеживание пользователя [9]. Например, датчики движения и четыре встроенные камеры в шлеме Oculus помогают отслеживать направление головы и движения, рисовать комнаты, а также отслеживать местоположение и окружающую среду в режиме реального времени с точностью до миллиметра. Если это устройство будет взломано злоумышленниками, серьезные преступления могут быть совершены на основе собранных больших объемов конфиденциальных данных. Другим примером является привлекательный виртуальный офис (например, Horizon Workroom и Microsoft Mesh), что может создать значительные риски для безопасности и конфиденциальности сотрудников. С одной стороны, разговоры сотрудников, электронные письма, которые они отправляют, URL-адреса, которые они посещают, их поведение и даже тон их голосов могут контролироваться менеджерами. С другой стороны, иммерсивное рабочее место может быть подвержено другим проблемам безопасности и конфиденциальности, таким как вторжения, слежка и самозванцы.

2) Утечка конфиденциальной информации при передаче данных. В системах метавселенной обширная личная информация, собираемая на носимые устройства, передается по проводным и беспроводным каналам связи, конфиденциальность которых должна быть запрещена неавторизованным лицам/службам. Несмотря на то, что коммуникации зашифрованы и информация передается конфиденциально, злоумышленники все равно могут получить доступ к необработанным данным путем подслушивания по определенному каналу и даже отслеживать местоположение пользователей с помощью дифференциальных атак.

3) Утечка конфиденциальной информации при обработке данных. В службах метавселенной агрегирование и обработка массивных данных, собранных от человеческого тела необходимы для создания и рендеринга аватаров и виртуальных сред, в которых может произойти утечка конфиденциальной информации пользователей. Например, объединение личных данных (принадлежащих разным пользователям) в центральное хранилище для обучения персонализированных моделей внешнего вида аватара может нарушать конфиденциальность пользователей и существующие правила реального мира, такие как Общие правила защиты данных (GDPR). Кроме того, злоумышленники могут сделать вывод о конфиденциальности пользователей (например, предпочтениях), анализируя и связывая опубликованную обработку результатов в различных виртуальных пространствах.

4) Утечка конфиденциальности в облачном/пограничном хранилище. Хранение частной и конфиденциальной информации (например, профилирование пользователей) крупных пользователей на облачных серверах или перифе-

рийных устройствах также может вызвать проблемы с раскрытием конфиденциальности. Например, хакеры могут выводить информацию о конфиденциальности пользователей путем частых запросов с помощью дифференциальных атак и даже компрометировать облачное/пограничное хранилище с помощью распределенных атак типа "отказ в обслуживании" (DDoS). В 2006 году была создана база данных клиентов Second Life (игры метавселенной). Данные пользователя были взломаны, включая незашифрованные имена пользователей и адреса, а также зашифрованные платежные реквизиты и пароли.

5) Мошеннические или скомпрометированные конечные устройства. В метавселенной на телах людей и их окружении будет размещено больше носимых датчиков, которые позволят аватарам устанавливать естественный зрительный контакт, фиксировать жесты рук, отражать выражение лица и так далее в режиме реального времени. Значительный риск заключается в том, что эти носимые устройства могут дать абсолютно достоверное представление о том, кто вы есть, как вы говорите, ведете себя, чувствуете и выражаете себя. Использование поддельных или скомпрометированных носимых устройств конечные устройства (например, очки виртуальной реальности) в метавселенной становятся входом для утечек данных и вторжений вредоносных программ, и проблема может стать более серьезной с ростом популярности носимых устройств для входа в метавселенную [9]. При манипулировании мошенническими или скомпрометированными конечными устройствами аватары в метавселенной могут превратиться в источник сбора данных, тем самым нарушая конфиденциальность пользователя. Например, поскольку продвинутые носимые устройства, такие как шлемы Oculus и тактильные перчатки, могут отслеживать движения глаз и жесты рук, хакеры могут воссоздавать действия пользователя и даже конфиденциальные пароли для личных учетных записей, следуя движениям глаз и пальцев при вводе кодов на виртуальной клавиатуре.

6) Угрозы цифровым следам. Поскольку модель поведения, предпочтения, привычки и действия аватаров в метавселенной могут отражать реальные статусы их физических аналогов, злоумышленники могут собирать цифровые отпечатки аватаров и использовать сходство, связанное с реальными пользователями, для облегчения точного профилирования пользователей и даже незаконной деятельности [4]. Например, аватар может осуществлять виртуальное преследование/ шпионаж, следуя за вашим аватаром и записывая все ваши цифровые следы, например, покупательское поведение, чтобы облегчить атаки социальной инженерии.

7) Возможность установления связей между идентичностями в троичных мирах. По мере того, как метавселенная ассимилирует реальность в себя, человеческий, физический и виртуальный миры плавно интегрируются в метавселенную, вызывая проблемы с идентификацией в трех мирах. Например, злонамеренный игрок А в Roblox может отслеживать другого игрока Б по имени, появившемуся над соответствующим аватаром игрока Б и определить его/ее положение в реальном мире. Другим примером является то, что хакеры могут отслеживать местоположение пользователей с помощью Гарнитуры виртуаль-

ной реальности или с помощью очки [9].

8) Угрозы индивидуальной конфиденциальности. Аналогично существующему Интернету сервисные платформы, отдельные пользователи обычно демонстрируют индивидуальные предпочтения конфиденциальности для различных сервисов или объектов взаимодействия в различных субметавселенных. Например, пользователь в Roblox может быть более чувствителен к денежным операциям, чем к социальным активностям. Кроме того, пользователи/аватары могут быть более чувствительными при взаимодействии с незнакомцами, чем знакомые, друзья или родственники. Однако существуют проблемы при разработке индивидуальных политик сохранения конфиденциальности для управления персональными данными при рассмотрении аватаров в метавселенной как индивидуальных субъектов информации, а также как характеристики пользователей и субметавселенных.

Таким образом, риски метавселенной обусловлены тем, что пользователи будут переносить в мета-мир свои ценности, специфику мышления и поведения, оказывая тем самым влияние на физический мир и получать от этого отрицательные последствия.

В метавселенных регуляторы не смогут контролировать цепочки продаж и возникновение виртуальных политических партий, новых форм агитаций и протестов. Еще одной угрозой является использование расширенной реальности (XR) для ощущения тактильных импульсов.

Выделим еще ряд рисков, которые несут метавселенные.

Определяющий риск приведет к необходимости разработки ПО новейшего поколения и соответствующим им протоколов и оборудования. Сейчас распространены взломы сайтов для выкупа. В сфере носимых устройств и IoT проблемы с безопасностью кратно возрастут. Причем хакеры будут использовать традиционные виды атак и внедрять их в платформы метавселенных. Например, из-за взломанных кодов пользователь не сможет зайти в свой виртуальный офис или дом. Вполне вероятен сценарий, когда хаккеры будут требовать выкуп за восстановление доступа.

Учащаться взломы IoT. Сервисные платформы метавселенной и оборудование виртуальной реальности будут уязвимы перед киберпреступниками. И даже это не будет доминирующей угрозой.

В метавселенных в первую очередь изменится социальная инженерия. Можно предположить, что киберпреступники будут взламывать аккаунты пользователей и под видом их аватаров, общаться с остальными пользователями, получать частные данные от конкретного человека. Будет, тем самым, суперутечки персональных данных с метавселенных. Возникнет проблема разработки протоколов защиты персональных данных пользователей.

Фишинг данных превзойдет себя. Софт по поддержке разнообразных метавселенных создается в быстром темпе, что неизбежно вызовет появление значительного числа уязвимостей. Ими обязательно воспользуются группировки хакеров. Тем более, что их уровень технической оснащенности становится все более высоким. Уже работают группы кибернаемников, занимающихся похи-

щением информации от бирж по заказу конкурентов и организованные группы, оснащение которых не уступает спецслужбам.

Вполне реально могут возникать зависимости пользователей от метавселенных, могут появиться новые формы психических расстройств и зависимостей, гораздо серьезнее и сродни наркотической.

В заключении отметим, что метавселенные станут катализаторами угроз, которые действуют сейчас. Эти угрозы будут мощнее и изощреннее, чем сейчас. К сожалению, подобная ситуация приведет к мощным социально-экономическим ущербам как общества в целом, так и отдельным компаниям. Вопрос о решении этих угроз создателями метавселенных до сих пор остается неясным.

СПИСОК ЛИТЕРАТУРЫ

1. *Sanchez J.,* “Second life: An interactive qualitative analysis,” in Society for Information // Technology & Teacher Education International Conference. 2007. pp. 1240-1243.

2. *Dionisio J. D. N., Gilbert R.,* “3D virtual worlds and the metaverse: Current status and future possibilities” // ACM Computing Surveys (CSUR). 2013. Vol. 45. №. 3. Pp. 1-38.

3. *Bruun A., Stentoft M. L.,* “Lifelogging in the wild: Participant experiences of using lifelogging as a research tool,” // IFIP Conference on Human-Computer Interaction. 2019. Pp. 431-451.

4. *Ning H., Wang H., Lin Y., Wang W., Dhelim S., Farha F., Ding J., Daneshmand M.* “A survey on metaverse: the state-of-the-art, technologies, applications, and challenges,” // arXiv preprint arXiv:2111.09673. 2021.

5. *Lim W. Y. B., Xiong Z., Niyato D., Cao X., Miao C., Sun S., Yang Q.,* “Realizing the metaverse with edge intelligence: A match made in heaven // arXiv preprint arXiv:2203.05471. 2022.

6. Facebook Inc. rebrands as Meta to stress ’metaverse’ plan. 2021. [Electronic resource]. URL: Available: https://machinaresearch.com/news /press-release-global-internet-of-things-market-to-grow-to-27-billion-devices-generating-usd3-trillion-revenue-in-2025/ (date of application: 22.09.2022).

7. *Leenes R.,* “Privacy in the metaverse: Regulating a complex social construct in a virtual world // The Future of Identity in the Information Society. 2008. Pp. 95-112.

8. *Falchuk B., Loeb S., Neff R.* “The social metaverse: Battle for privacy,” // IEEE Technology and Society Magazine. 2018. Vol. 37. № 2. Pp. 52-61.

9. *Shang J., Chen S., Wu J., Yin S.,* “ARSpy: Breaking location-based multi-player augmented reality application for user location tracking,” // IEEE Transactions on Mobile Computing. 2022. Vol. 21. №. 2. Pp. 433-447.

10. *Hu P., Li H., Fu H., Cansever D., Mohapatra P.,* “Dynamic defense strategy against advanced persistent threat with insiders,” // IEEE Conference on Computer Communications (INFOCOM). 2015. Pp. 747-755.