ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭПОХУ ЦИФРОВИЗАЦИИ НА ПРИМЕРЕ РАСПРОСТРАНЕНИЯ МЕТАВСЕЛЕННОЙ

Э. И. ЛЕСКИНА,

канд. юрид. наук, доц. кафедры информационного права и цифровых технологий
ФГБОУ ВО «Саратовская государственная юридическая академия»

В эпоху, когда данные провозглашены новой нефтью, деятельность многих субъектов направлена на создание технологий, обеспечивающих генерацию, сбор, обработку и последующее использование различных данных. Доходы от подобной деятельности огромны и растут с каждым годом. Так, на 2021 г. компания Байтдэнс (TikTok) оценивается примерно в 400 млрд долларов США. Активность собираемых данных в настоящее время возрастает еще большими темпами вследствие, в том числе, становления и развития новой, гораздо более масштабной виртуальной реальности, получившей название метавселенная.

О метавселенной в качестве нового интернета, всеобъемлющего виртуального мира, уже говорят как о пространстве, где человек будет проводить большую часть своего времени. Однако сопутствующей проблемой являются проблемы безопасности, конфиденциальности, возникающие при такой новой форме взаимодействия. Количество данных, поступающих в связи с пользованием метавселенной, периферическими устройствами значительно увеличивается; собираются новые виды данных.

Термин метавселенная образован от английского «meta» – трансцендентность и «verse» – мир. Под метавселенной понимают коллективное виртуальное пространство, в котором объединяются физическая, дополненная и виртуальная реальность. Понимается метавселенная и в качестве парадигмы Интернета нового поколения, направленной на создание общего самоподдерживающегося виртуального социального пространства, характеризующегося признаками иммерсивности и многомерности [1, с. 3]. Метавселенную понимают как суперэкосистему виртуальной реальности, сочетающую в себе функционирование различных технологий (искусственный интеллект, виртуальная и дополненная реальность, блокчейн, Интернет вещей и т.д.) [2, с. 8]. Компоненты этой экосистемы взаимодействуют друг с другом, состоят в динамическом равновесии, создавая единый виртуальный мир.

В настоящее время создаются или совершенствуются периферические устройства для подключения – очки, линзы, шлемы, наушники, перчатки,

датчики, костюмы для сканирования движений и передачи их в виртуальное пространство. Эти устройства накапливают огромные массивы данных о пользователях. Эти данные многообразны, и возможности, связанные с получением информации постоянно развиваются. Так, М. Миллером установлено, что 5 минут сбора данных о движениях пользователя, собранных с шлема, достаточно для того, чтобы идентифицировать физическое лицо с точностью 95 % [3, с. 5].

Управление массивными потоками данных, круптомасштабные объемы профилирования пользователей, ошибки в алгоритмах искусственного интеллекта, все это может возникать и в метавселенной, но в гораздо больших масштабах, нежели имеет место быть в настоящее время. Даже сами персональные данные в условиях метавселенной могут иметь более детализированный характер, распространяться более активно и широко, что само по себе создает новые угрозы для их неправомерного использования. Может иметь место отслеживание движений, мимики пользователей, их окружающего пространства, эмоциональных реакций, нейронных импульсов и т.д. [4, с. 55]. В целом, в эпоху метавселенной будут возникать новые данные в результате разработки нового оборудования и учета ранее не собираемых данных (например, движений глаз, мимики).

Кража персональных данных может привести к краже личности пользователя метавселенной. В этом случае виртуальная социальная жизнь может быть утеряна, как и цифровые активы, банковские реквизиты. Так, в 2022 г. на торговой площадке Opensea NFT были взломаны учетные записи 17 пользователей, а ущерб составил 1,7 миллионов долларов.

Кража данных может привести к имитации личности, когда преступник может выдать себя за другое лицо, собрав биологические и поведенческие данные, возможно создание фальшивого аватара. Дипфейки здесь могут выти на совершенно новый уровень. В результате могут совершаться мошенничества, преступления против близких пользователя, данные которого были украдены. В настоящее время существуют технологии, которые способны точно копировать тональность и другие особенности голоса, воспроизводить походку, жесты аватаров. Кроме того, возможно формирование характеристик аватара, вызывающего доверие, симпатию или другие желательные реакции пользователей.

Наконец, посягательства на персональные данные могут выражаться в психологическом манипулировании пользователями. Это может быть политическое принуждение, вовлечение в экстремистские группировки, вербовка социально и психологически нестабильных людей в запрещенные организации, секты. Также возможно возникновение платформ, использующих лиц, страдающих игровой зависимостью.

Угрозы информационной безопасности в области метавселенной можно сгруппировать по следующим направлениям:

1) несанкционированный доступ к персональным данным. Эпоха метавселенной будет характеризоваться генерирование новых типов персональных данных в результате аналитики биометрической информации, распорядка дня, привычек пользователей. Периферийные устройства могут считывать отпечатки пальцев пользователя, данные радужки глаза, другой важной биометрической информации. В качестве персональных данных может являться и внешний вид аватара. Аналитика таких данных будет проводится в режиме реального времени. Необходимо решение вопросов об уничтожении указанной информации;

2) неправомерное использование данных пользователя или аватара. Из-за возможной несовместимости систем субметавселенных такие действия становится сложно отследить в масштабах всей метавселенной. Вместе с тем, данные могут быть раскрыты преднамеренно как злоумышленниками, так и в целях таргертированной рекламы;

3) противоправные действия в отношении необработанных данных (raw data). Такие данные могут подвергаться атакам, в результате чего изменяться, заменяться, удаляться. Все это мешает нормальной деятельности пользователей, функционированию объектов и аватаров [5, с. 25];

4) введение ложных системных данных, которые могут вводить пользователей в заблуждение, создавать проблемы при обучении систем искусственного интеллекта, изменениям будут подвергаться инструкции. Все это будет приводить к неисправностям оборудования, угрозам личной безопасности пользователя. Также указанные в данном и предыдущем пункте нарушения могут приводить к созданию ложных корреляций в работе искусственного интеллекта, машинного обучения, что в дальнейшем приведет к предвзятым моделям, ошибкам профилирования, прогнозирования и т.д.

Одним из способов обеспечения информационной безопасности являются квантовые технологии. В 2021 г. в России была запущена квантовая сеть во исполнение «дорожной карты» по квантовым коммуникациям. Сеть стала самой крупной в Европе и второй по величине в мире, а до 2024 г. планируется запуск 7 тыс. км квантовых сетей. Система способна передавать большие данные, сохраняя информацию и обеспечивая беспрецедентный уровень безопасности, исходя из принципов квантовой физики. Категории суперпозиции, запутанности, квантовой неопределенности и др. предоставляют новые возможности для защиты информации, а значит, и новые пути обработки данных.

Так, применяемые квантовые криптографические конструкции, в частности, сопряженное кодирование, посредством поляризации фотона, обеспечивают безопасность хранения и передачи данных. Гарантией безопасности связи является использование метода квантового распределения ключей. Субъекты обработки персональных данных могут создать общий криптографический ключ. Любой субъект при попытке получить этот ключ должен измерить квантовые состояния, что приведет к их изменению. Кроме того, попытки такого несанкционированного доступа будут незамедлительно отслеживаться. Используются метод и постоянной генерации ключей. В результате гарантируется безопасность передачи данных, в том числе и аудиоинформации, как по магистральным линиям связи, так и в рамках сетей и даже при распределенных реестрах, например, блокчейн [6, с. 114]. В России создан отечественный квантовый генератор случайных чисел на основе интерференции лазерных импульсов. Методы квантовой телепортации делают расшифровку перехваченного сообщения невозможной. Все это значительно снижает возможности кибератак.

Несомненно, действенным способом обеспечения информационной безопасности является повышение уровня информационной грамотности. Информированность населения о последствиях погружения в метавселенную, пользования шлемами, перчатками, костюмами и другими устройствами, знания в области кибербезопасности, преступной деятельности в метавселенной, способов психологического воздействия, – все это даст эффективные результаты в области предотвращения незаконных посягательств.

Итак, становление и развитие метавселенной создает условия и для посягательств на информационную безопасность. Многообразие биометрической информации, форм психологического давления и манипуляции приводит к новым посягательствам в киберпространстве. Децентрализация метавселенной говорит о необходимости выработки единого международного подхода в указанной сфере, особенно в части трансграничного оборота данных. Несомненно, действенным способом обеспечения информационной безопасности является повышение уровня информационной грамотности, развитие кадрового потенциала в сфере цифровых технологий как в публичном, так и частном секторе, формирование «цифрового» доверия населения к государству. Другой стороной обеспечения информационной безопасности в метавселенной является развитие в Российской Федерации квантовых технологий, внедрение таких технологий в сферу информационной безопасности. Все это будет способствовать противостоянию незаконным деяниям, посягающим на безопасность и конфиденциальность.

ЛИТЕРАТУРА

1. Wang, Yuntao & Su, Zhou & Zhang, Ning & Liu, Dongxiao & xing, rui & Luan, Tom Hao & Shen, Xuemin. A Survey on Metaverse: Fundamentals, Security, and Privacy // https://arxiv.org/pdf/2203.02662.pdf (дата обращения 30.09.2023).
2. Ruoyu Zhao, Yushu Zhang, Youwen Zhu, Rushi Lan, Zhongyun Hua. Metaverse: Security and Privacy Concerns // JOURNAL OF LATEX CLASS FILES, 2021. VOL. 14, NO. 8. P. 7–14.
3. Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, Jeremy N Bailenson. Personal identifiability of user tracking data during observation of 360-degree VR video // Scientific Reports, № 10, 2020, p. 1–10.
4. B. Falchuk, S. Loeb, and R. Neff. The social metaverse: Battle for privacy // IEEE Technology and Society Magazine, 2018, vol. 37, no. 2, p. 52–61.
5. Z. Su, Y. Wang, Q. Xu, and N. Zhang. LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue // IEEE Transactions on Dependable and Secure Computing. 2022. vol. 19, no. 1, p. 19–32.
6. A. Duplinsky, E. Kiktenko, N. Pozhar, M. Anufriev, R. Ermakov, A. Kotov, A. Brodsky, R. Yunusov, V. Kurochkin, A. Fedorov, Y. Kurochkin, Quantum-secured data transmission in urban fibre-optic communication lines // Journal of Russian Laser Research, 2018. № 39 (2), p. 113–119.