УДК: 004.056.

УГРОЗЫ БЕЗОПАСНОСТИ В МЕТАВСЕЛЕННЫХ И МЕХАНИЗМЫ ИХ НЕЙТРАЛИЗАЦИИ

В. В. Бондаренко, М. Н. Осипов, К. В. Протасов
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: Метавселенные, NFT, невзаимозаменяемые токены, биометрическая аутентификация, виртуальная реальность

Метавселенные представляют собой интегрированные цифровые пространства, в которых пользователи взаимодействуют через трехмерные аватары, при этом возникают новые угрозы информационной безопасности, связанные с нарушением приватности, деанонимизацией и компрометацией цифровых идентификаторов. Необходимы математически обоснованные методы, позволяющие оперативно реагировать на изменения многомерных данных – пространственных, биометрических, поведенческих, учитывая контекст взаимодействия, также динамика виртуальных миров подразумевает постоянное изменение границ «личного пространства» и характеров взаимодействий между участниками, что затрудняет применение статичных правил безопасности, к тому же традиционные методы зачастую ориентированы на централизованные системы, тогда как метавселенная предполагает децентрализованный характер данных и идентификации. [1, 2, 3]

В основе анализа лежит математическое моделирование личного пространства пользователей, которое представлено как метрика в трехмерном пространстве, где каждое приближение одного аватара к другому можно оценить с помощью геометрических неравенств. Такое представление позволяет задать формальные условия для защиты личных зон, в которых устанавливаются минимальные безопасные расстояния между участниками, а также ввести понятие доверенных зон, где допускается ограниченный доступ на основе криптографических протоколов. Наряду с этим используется информационно-теоретический подход, позволяющий оценить утечку конфиденциальных данных посредством взаимной информации и энтропии, что дает возможность количественно определить степень компрометации данных и принять соответствующие меры по их защите.

Особое внимание уделяется проблеме идентификации и аутентификации в условиях децентрализованной метавселенной, где традиционные централизованные системы не обеспечивают необходимого уровня безопасности. В данном контексте предложены решения, основанные на использовании непередаваемых NFT-токенов,

представляющих собой уникальные цифровые удостоверения личности, а также децентрализованных идентификаторов (DID). Такие методы позволяют не только гарантировать уникальность и неподделываемость идентификаторов, но и сохранить приватность, так как данные о пользователе распределены и защищены криптографическими средствами. Наряду с этим, внедрение биометрической аутентификации и непрерывного мониторинга поведения пользователя позволяет значительно снизить риск мошеннических действий, а механизм проверки подлинности реализуется как посредством цифровых подписей, так и с использованием доказательств с нулевым разглашением.

Ключевым моментом является интеграция различных уровней защиты, где геометрические доверенные зоны сочетаются с криптографическими протоколами и методами дифференциальной приватности. Формализация угроз позволит определить, при каких условиях вероятность успешного вторжения или компрометации сведений становится пренебрежимо малой, а также оценить эффективность мер, направленных на снижение информационных утечек.

Математическая модель идентификации базируется на принципах, где каждая операция аутентификации требует наличия криптографического доказательства владения приватным ключом. Такая система, усиленная механизмами многофакторной аутентификации и биометрического контроля, должна демонстрировать высокую устойчивость. В совокупности эти методы создают основу для надежной защиты цифровых активов и личной информации, что имеет решающее значение для формирования доверия пользователей к виртуальным пространствам метавселенных.

Сочетание NFT-токенов, децентрализованных идентификаторов, биометрической аутентификации и методов дифференциальной приватности обеспечивает необходимый уровень защиты, позволяющий минимизировать вероятность компрометации приватной информации и создать безопасную виртуальную среду общего пользования.

Список использованных источников

1.Олин Р. А. Метавселенные как часть цифровой трансформации / Р. А. Олин // Устойчивое развитие в неустойчивом мире: Сборник научных статей Международной научно-практической конференции, Самара, 23 мая 2023 года. – Самара: Самарский государственный экономический университет, 2023. – С. 297-306. – DOI 10.46554/UR-2023-pp.297. – EDN USQROQ.

2.Олин Р. А. Влияние автономных агентов с искусственным интеллектом на инновационные процессы в корпоративной среде / Р. А. Олин // Актуальные тренды в развитии науки, экономики, образования: Сборник научных статей Всероссийской научно-практической конференции, Самара, 17 июня 2024 года. – Самара: Самарский государственный экономический университет, 2024. – С. 18-23. – EDN KFZBZR.

3.Олин Р. А. Инновационный менеджмент предприятия в условиях взаимодействия с машинными клиентами и автономными агентами на основе искусственного интеллекта / Р. А. Олин, К. В. Портнов, Е. С. Шатрова // Журнал монетарной экономики и менеджмента. – 2024. – № 3. – С. 218-224. – DOI 10.26118/2782-4586.2024.24.43.033. – EDN OJZVMH.

4.Maslova O., Shusharina N., Pyatin V. The Neurosociological Paradigm of the Metaverse // Frontiers in Psychology. 2025. Vol. 15. P. 1371876. DOI:10.3389/fpsyg.2024.1371876.
URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2024.1371876/full (дата обращения: 21.03.2025).

5.Kirasirova L., Maslova O., Pyatin V. Impact of virtual agent facial emotions and attention on N170 ERP amplitude: comparative study // Frontiers in Behavioral Neuroscience. 2025. Vol. 19. Article 1523705. DOI: 10.3389/fnbeh.2025.1523705. URL: https://www.frontiersin.org/articles/10.3389/fnbeh.2025.1523705/full (дата обращения: 19.03.2025).

6.Шарипов Р. Р. Проблемы при разработке систем распознавания пользователей по клавиатурному почерку / Р. Р. Шарипов, А. Н. Ситников // Вестник Технологического университета. – 2019. – Т. 22, № 10. – С. 143-147. – EDN CFTZWL.

Бондаренко Владимир Владимирович, к.ф.-м.н., доцент каф. безопасности информационных систем, bondarenko.vv@ssau.ru.

Осипов Михаил Николаевич, к.ф.-м.н., доцент, зав. каф. безопасности информационных систем, osipov7@yandex.ru.

Протасов Кирилл Витальевич, студент, спец. «Информационная безопасность», protasovkirill44@gmail.com

УДК 519.7; 004.07; 519. 216

ВЕРОЯТНОСТНЫЕ МОДЕЛИ ОБЪЕКТОВ НАБЛЮДЕНИЙ

В.П. Цветов
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: стохастические матрицы, недетерминированные системы, вероятностные биты

В докладе определяются основные математические конструкции, которые предлагается использовать для моделирования и последующего изучения систем объектов или процессов, для которых построение детерминированных моделей затруднительно или нецелесообразно. Каноническими примерами таких объектов являются сетевые узлы или исполняемые процессы операционных систем, понимаемые как Шенноновские источники информации [1-3], комплексы датчиков систем