

УДК 004.056.57

РАЗРАБОТКА ЗАЩИЩЕННОЙ СИСТЕМЫ ГОЛОСОВОЙ ВЕРИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

Жигалко Даниил Евгеньевич, Салита Даниил Сергеевич

Алтайский государственный университет, Барнаул
zhigalkodanya@gmail.com, d.s.salita@gmail.com

DEVELOPMENT OF A SECURE USER VOICE VERIFICATION SYSTEM USING BLOCKCHAIN TECHNOLOGY

Zhigalko Daniil E., Salita Daniil S.

Altai State University, Barnaul
Zhigalko Daniil E., Salita Daniil S.

Аннотация. В статье рассматривается проблема безопасного хранения биометрических данных в условиях уязвимости централизованных систем. Предложено решение на основе децентрализованной архитектуры, сочетающей технологию блокчейн, для обеспечения целостности данных и нейросетевые модели для извлечения биометрических признаков. В качестве ядра системы используется модель Titanet_large из фреймворка NVIDIA NeMo, преобразующая голосовой сигнал в компактный вектор признаков (эмбединг). Эмбединги хранятся в локальной цепочке блоков, где каждый блок криптографически связан с предыдущим с помощью алгоритма SHA-256. Для взаимодействия с пользователем реализован Telegram-бот, обеспечивающий интерфейс для регистрации и верификации по голосу. Алгоритм верификации основан на расчете косинусного сходства между векторами. Разработанный прототип демонстрирует практическую реализуемость подхода, обеспечивая повышенный уровень безопасности за счет децентрализации и отказа от хранения исходных аудиоданных.

Ключевые слова: голосовая биометрия, блокчейн, верификация, эмбединг, децентрализованное хранение, Titanet, нейросетевые модели

Abstract. The article addresses the problem of secure storage of biometric data in the context of vulnerabilities in centralized systems. A solution based on a decentralized architecture is proposed, combining blockchain technology to ensure data integrity and neural network models for extracting biometric features. The system core is the Titanet_large model from the NVIDIA NeMo framework, which converts a voice signal into a compact feature vector (embedding). The embeddings are stored in a local blockchain, where each block is cryptographically linked to the previous one using the SHA-256 algorithm. A Telegram bot is implemented for user interaction, providing an interface for voice registration and verification. The verification algorithm is based on calculating the cosine similarity between vectors. The developed prototype demonstrates the practical feasibility of the approach, providing an increased level of security through decentralization and the avoidance of storing original audio data.

Keywords: voice biometrics, blockchain, verification, embedding, decentralized storage, Titanet, neural models

Для цитирования: Жигалко Д.Е., Салита Д.С. Разработка защищенной системы голосовой верификации пользователей с применением технологии блокчейн // Проблемы правовой и технической защиты информации. 2025. № 13. С. 12–16.

For citation: Zhigalko D.E., Salita D.S. Development of a secure user voice verification system using blockchain technology. *Legal and Technical Problems of Information Security*. 2025. No. 13. P.12–16.

Современные информационные системы сталкиваются с растущими требованиями к надежности и безопасности механизмов идентификации пользователей. Традиционные методы аутентификации, основанные на паролях, демонстрируют уязвимость к фишингу и утечкам данных, что стимулирует активное развитие биометрических технологий [1]. Голосовая биометрия представляет особый интерес как естественный для пользователя способ удаленной верификации, не требующий специализированного оборудования [2]. Однако широкое внедрение биометрических систем порождает новую проблему — безопасное хранение биометрических шаблонов, которые, в отличие от паролей, невозможно изменить в случае компрометации. Централизованные хранилища данных создают риски масштабных утечек и несанкционированного доступа, что обуславливает необходимость поиска альтернативных архитектурных решений [3].

Перспективным направлением является применение технологии блокчейн, которая обеспечивает децентрализованное хранение, криптографическую целостность и прозрачность операций с данными [4]. Сочетание блокчейн с современными методами обработки голосовых сигналов открывает возможности для создания устойчивых систем биометрической идентификации.

В данной работе представлен прототип системы защищенного хранения голосовых биометрических данных, сочетающий нейросетевые методы извлечения признаков с технологией распределенного реестра. Основное внимание уделено технической реализации архитектуры, алго-

ритмам обработки данных и метрикам верификации.

Разработанная система построена по модульному принципу и включает три основных компонента: модуль обработки аудиосигналов и извлечения признаков, модуль формирования и хранения блоков данных, модуль верификации пользователей.

Модуль обработки аудиосигналов реализован на базе нейросетевой модели Titanet из фреймворка NVIDIA NeMo, специально оптимизированной для задач идентификации диктора [5]. Входной аудиофайл в формате WAV (частота дискретизации 16 кГц, моно) подвергается предварительной обработке, включающей подавление шумов и нормализацию сигнала. Затем аудиоданные преобразуются в спектрограмму с использованием 128 мел-коэффициентов и шагом окна 10 мс. На выходе модели формируется эмбединг — вектор признаков фиксированной длины 192 значения типа float32 (768 байт), отражающий индивидуальные акустические характеристики голоса пользователя.

Модуль формирования блоков данных организует хранилище эмбедингов в структуре, имитирующей блокчейн, структура представлена на рисунке 1. Каждый блок содержит следующие поля: PreviousHash (хэш предыдущего блока по алгоритму SHA-256, 32 байта), Timestamp (временная метка в формате UNIX, 8 байт), Metadata (JSON-структура с информацией о пользователе и параметрах записи, ≈300 байт), VoiceEmbedding (эмбединг, 768 байт), CurrentHash (хэш текущего блока, 32 байта). Общий объем одного блока составляет 1150-1300 байт.

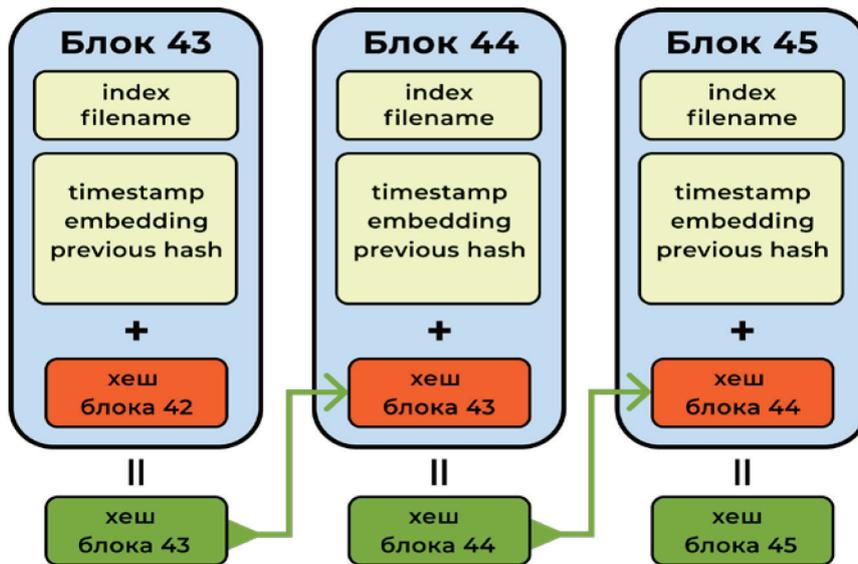


Рисунок 1. Алгоритм записи эмбединга в блокчейн

Для обеспечения целостности данных используется алгоритм хеширования SHA-256. Хэш текущего блока вычисляется на основе конкатенации значений PreviousHash, Timestamp, Metadata и VoiceEmbedding. Полученная строка передается на вход хеш-функции, результатом которой является 256-битный хэш, выступающий уникальным идентификатором блока.

Процесс добавления новых биометрических данных в систему включает последова-

тельность этапов, представленную на рисунке 2. На первом этапе выполняется обработка и очистка аудиофайла пользователя. Затем из подготовленного аудиосигнала извлекается спектрограмма и генерируется эмбединг с помощью модели Titanet. На следующем этапе формируется структура блока и выполняется сериализация данных. После этого вычисляется SHA-256 хэш блока, и завершающим этапом является добавление блока в локальный JSON-реестр, моделирующий блокчейн.

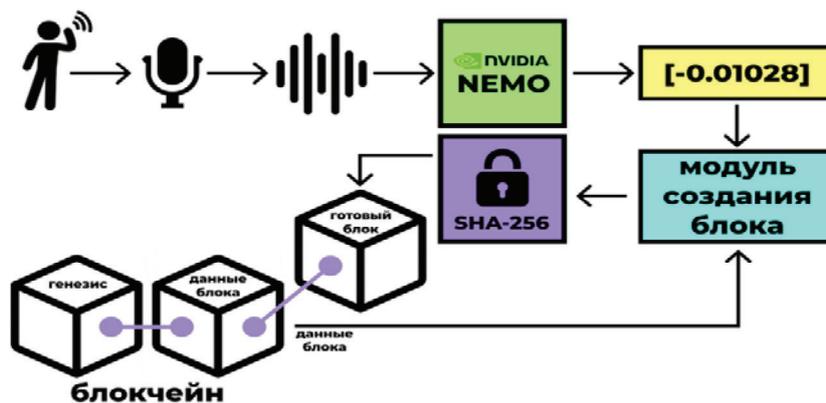


Рисунок 2. Алгоритм записи эмбединга в блокчейн

Основное преимущество использования эмбедингов вместо исходных аудиозаписей заключается в компактности представления данных и невозможности восстановления

исходного речевого сигнала из векторного представления, что существенно повышает конфиденциальность хранимой биометрической информации.

Процесс верификации пользователей реализован на основе сравнения вновь полученных эмбедингов с эталонными образцами, хранящимися в блокчейне. Для оценки

степени сходства векторов используется метрика косинусного сходства, вычисляемая по формуле (1):

$$\text{similarity} = 1 - \cos(A, B) = 1 - \frac{A \cdot B}{\|A\| \times \|B\|}, \quad (1)$$

где A и B — сравниваемые векторы эмбедингов.

Расчет косинусного сходства реализован с использованием библиотеки SciPy. В ходе тестирования системы установлено пороговое значение 0.75, при превышении которого голос считается подтвержденным, и пользователь успешно верифицируется. Данный метод демонстрирует устойчивость к variations речевой интонации и скорости произнесения, что делает его эффективным для тексто-независимых систем распознавания.

Для обеспечения удобного взаимодействия с пользователем разработан интерфейс в виде Telegram-бота, позволяющий записывать голосовые сообщения, сохранять их в блокчейн и проходить процедуру верификации. Бот реализован с использованием библиотеки python-telegram-bot и обеспечивает интуитивно понятный процесс работы с системой.

При получении голосового сообщения бот выполняет его конвертацию из формата OGG в WAV с параметрами 16 кГц, моно, после чего запускается процесс обработки аудио и извлечения эмбединга. Пользователю предоставляется выбор между сохранением голосового шаблона в блокчейн и прохождением верификации.

Разработанный прототип системы демонстрирует техническую реализуемость подхода к защищенному хранению голосовых биометрических данных на основе технологии блокчейн. Предложенная архитектура обладает потенциалом для масштабирования и может служить основой для создания полнофункциональных систем биометрической идентификации, предназначенных для применения в различных областях, включая финансовый сектор, государственные услуги и корпоративные системы безопасности.

Библиографический список

1. Прошева Е.К., Невмержицкий П.И. Блокчейн — новая революция // Бизнес-образование в экономике знаний. 2018. № 1 (9). С. 17–23.
2. Мебония М.А. Технология блокчейн. примеры блокчейна и его применение // Вестник науки: международный научный журнал. 2022. № 12 (57) Т. 3. С. 435–438.
3. Чурилин Г.Н., Максимова Е.А. Биометрия в информационной безопасности // НБИ технологии. 2019. № 4. Т. 13. С. 30–35.
4. Артемьев К.И. Блокчейн: возникновение, особенности использования и регулирования // Отечественная юриспруденция. 2018. № 4 (29). С. 40–45.
5. Степанов И.Е. Применение технологии блокчейн для обеспечения надежности и безопасности данных в интернете вещей // Вестник науки: международный научный журнал. 2023. № 4 (29). С. 762–768.
6. Бождай А.С., Гудков П.А., Гудков А.А. Встраиваемая система идентификации по голосовым биометрическим показателям // Открытое образование. 2011. № 2. С. 181–184.
7. Исаева Д.Г. О блокчейн-технологии // Экономика и бизнес: теория и практика. 2024. № 4 (122). С. 32–41.
8. Бланк Д.А. Анализ блокчейн-экосистем // Аудиторские ведомости. 2025. № 1. С. 44–48.

9. Хэ М. Сущность блокчейн как многофункциональной информационной технологии цифровой экономики // Теория и практика современной науки. 2025. № 3 (117). С. 167–172.

10. Можаров Г. П. Текстонезависимый метод идентификации человека по его голосу // Инженерный журнал: наука и инновации. 2012. № 3 (159). С. 167–178.

11. Брюхомицкий Ю.А. Верификация динамических биометрических параметров личности на основе вероятностной нейронной сети // Известия Южного федерального университета. Технические науки. 2020. № 3 (233). С. 52–60.

12. Кузенбаев Б.А., Абдрахманова Н.Ж. Исследование и анализ современных крипто-

систем для защиты компьютерной безопасности // Теория и практика современной науки. 2024. № 3 (117). С. 5–11.

13. Сергиенко И.А., Рукинова Е.А., Бурса И.А. Криптовалюты и блокчейн: новые горизонты для инвестиций // Региональная и отраслевая экономика. 2025. № 2. С. 182–187.

14. Елена Р.Р. Нейросети в судебной экспертиологии и экспертной практике: проблемы и перспективы // Вестник Университета имени О.Е. Кутафина. 2024. № 3 (127). С. 22–33.

15. Воробьева И.Б. Риски, сопутствующие цифровой трансформации деятельности следователя в процессе расследования преступлений // Вестник Саратовской государственной юридической академии. N23. № 3 (152). С. 155–163.