ХЕШИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕХНОЛОГИИ БЛОКЧЕЙН ПРИ ЭЛЕКТРОННОМ ГОЛОСОВАНИИ

А.В. Сидоренко, А.В. Валенда

В последнее время системы электронного голосования находят все более широкое распространение. Под электронным голосованием обычно подразумевается процесс голосования с помощью компьютеризированного оборудования.

При этом существенное значение приобретают вопросы обеспечения безопасности, что связано с предоставлением таких услуг, как конфиденциальность и целостность данных, аутентификация объектов и источника данных. Технология блокчейна [1] может обеспечить не только надежный канал передачи информации, но и способ преодоления потенциальных угроз, уязвимостей и атак. Блокчейн представляет собой новую технологию, возникшую в поле биткоинов и демонстрирующую, что с помощью объединения одноранговых сетей с криптографическими алгоритмами можно предоставить необходимые возможности для того,

чтобы сделать операции внутри системы более гибкими, автономными и безопасными [2]. Блокчейн является, по сути, общедоступной хронологической базой данных транзакций. Данные сгруппированы в наборы, называемые блоками. Каждый блок содержит информацию об определенном количестве транзакций, ссылку на предыдущий блок в цепочке блоков и ответ на задачу, известную как «доказательство работы». Она основана на криптографических вычислениях, в частности вычислении значений хеш-функции, которые дают непредсказуемые числовые последовательности. Блокчейн инкапсулирует все транзакции внутри блока в цифровом отпечатке, которым и является хеш. Хеш-функции в блокчейнах гарантируют «необратимость» всей цепочки транзакций.

В данной работе предложена система электронного голосования, в которой для формирования хеш-функции применяются хаотические отображения. Среди исследованных хаотических отображений выбраны: логистическое отображение, тент-отображенние и отображение Чирикова. Проведен вычислительный эксперимент, в котором в качестве критерия производительности выбрано время, необходимое для генерации одного блока блокчейна. Показано, что использование логистического отображения при хешировании позволяет получить оптимальное значение и повысить производительность на 5–7 %.

Литература

1. Nakamoto S. Bitcoin: a Peer-to-Peer Electronic Cash System. – 2008.

2. Chi L., Zhu X. Hashing techniques: a survey and taxonomy // ACM Computing Surveys. – 2017. – Vol. 50, no. 1. – P. 1–36. – https://doi.org/10.1145/3047307.