

**ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В СФЕРЕ МЕДИЦИНЫ, СВЯЗАННАЯ С  
ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ХРАНЕНИЯ ДАННЫХ**

**Зонова Д.Ю. (Университет ИТМО)**

**Научный руководитель – кандидат экономических наук, доцент Гаврилюк Е.С.  
(Университет ИТМО)**

**Научный консультант – кандидат медицинских наук, Лобанова Н.Ю.  
(Кировский ГМУ)**

**Введение.** Цифровая трансформация является ключевым фактором развития современной медицины, предлагая перспективы значительного увеличения доступности медицинской помощи, улучшения качества обследования пациентов, оптимизации рабочих процессов и повышения метрик экономической эффективности. Одним из главных элементов этой трансформации становится внедрение технологии блокчейн для хранения и управления медицинскими данными, что обеспечивает повышенный уровень безопасности, прозрачности и достоверности информации для всех участников здравоохранения.

Традиционные системы хранения медицинских данных, как правило, централизованы и поэтому уязвимы для кибератак и несанкционированных доступов и изменений. Блокчейн, благодаря своей децентрализованной и криптографически защищенной структуре, представляет собой более надежный способ хранения и управления медицинскими данными.

**Основная часть.** По оценкам в 2021 году общий объем создаваемой информации о состоянии здоровья превысил 2000 эксабайт, а прогнозируемый ежегодный рост составляет 48% [1]. В последние годы объем медицинских данных стремительно увеличивается, так за 9 месяцев 2024 года в среднем в сутки регистрируется более 4 млн. документов – столько же, сколько в 2019 году регистрировалось за целый год [2].

С расширением цифровой трансформации здравоохранения медицинские учреждения сталкиваются с новыми вызовами в области кибербезопасности. Согласно данным MTC RED, организации в сфере здравоохранения являются наиболее частыми целями кибератак, поскольку злоумышленники стремятся обойти существующие средства защиты. Увеличивается число кибератак, а также их масштабы становятся все более значительными. Как сообщил технический руководитель направления MTC RED SOC Ильназ Гатауллин, на такие атаки приходится 36% всех зарегистрированных киберинцидентов [3].

Одним из факторов, способствующих росту киберугроз, является широкое распространение медицинских IoT-устройств. Кроме того, хранение большого объема медицинских данных в облачных сервисах также создает угрозы безопасности: данные могут быть перехвачены или изменены в процессе передачи.

В условиях глобальной нестабильности вопросы кибербезопасности приобретают особую значимость. В частности, число атак на российский сектор здравоохранения увеличивается ежегодно [2].

Решение этих проблем возможно за счет внедрения киберфизических систем, основанных на технологиях четвертой промышленной революции. Использование передовых решений, таких как аналитика больших данных (Big Data), облачные вычисления, виртуализация, контейнеризация, IoT, искусственный интеллект (ИИ) и блокчейн, позволит автоматизировать работу медицинского персонала, улучшая качество предоставляемых услуг [4, 5].

Применение гибридного блокчейна с высокой скоростью обработки транзакций, поможет снизить уровень киберинцидентов для медицинских систем, требующих быстрого обмена данными.

В медицинской сфере критически важна защита персональных данных пациентов. Использование permissioned blockchain позволяет контролировать, всех участников процесса записи и чтения данных, обеспечивая соответствие требованиям Федерального закона №152-

ФЗ «О персональных данных» и ГОСТ Р 57580-2017.

**Выводы.** Использование технологии блокчейн для хранения данных является важным элементом цифровой трансформации в сфере медицины, обеспечивая высокий уровень безопасности, прозрачности и эффективности. Блокчейн может значительно улучшить управление рабочими процессами в медицине: медицинское страхование, ведение и хранение качественных и количественных медицинских показателей, данных телемедицины и биометрии, отслеживание поставок лекарственных средств и др., способствуя повышению качества медицинской помощи и снижению рисков кибератак.

#### **Список использованных источников:**

1. Гиверц П. Конвергенция технологий ИИ, блокчейна и IoT – новый спектр возможностей для здравоохранения в условиях, нарастающих киберугроз // Здравмединфо [Электронный ресурс]. – URL: [https://medsoft.pro/2022/presentation/Day2/12\\_00\\_Конвергенция\\_технологий\\_ИИ\\_MedSoft.pdf](https://medsoft.pro/2022/presentation/Day2/12_00_Конвергенция_технологий_ИИ_MedSoft.pdf) (дата обращения: 07.02.2025).
2. XXV Ежегодный международный конгресс «Информационные технологии в медицине» [Электронный ресурс]. – URL: [https://itmcongress.ru/novostdetalno\\_4\\_758/](https://itmcongress.ru/novostdetalno_4_758/) (дата обращения: 07.02.2025).
3. МТС RED: за первую половину 2024 года медицинские учреждения РФ на 32% чаще становились жертвами кибератак// Все публикации подряд «Хабр» [Электронный ресурс]. – URL: <https://habr.com/ru/news/831676/> (дата обращения: 07.02.2025).
4. Agbo C.C., Mahmoud Q.H., Eklund J.M. Blockchain technology in healthcare: a systematic review // Healthcare (Basel). – 2019. – Vol. 7(2). – p. 56.
5. Cernian A., Tiganoaia B., Sacala I., et al. PatientDataChain: A Blockchain-Based Approach to Integrate Personal Health Records // Sensors (Basel). – 2020. – Vol. 20 (22). – p. 6538.