Почему цифровое здравоохранение терпит молчаливые неудачи: социотехническая теория рисков, связанных с информационными технологиями в здравоохранении

Источник: Frontiers in Digital Health

Оригинал: https://www.frontiersin.org/articles/10.3389/fdgth.2026.1785086

безопасность пациентов | информационные технологии в медицине | организация здравоохранения | управление рисками | цифровое здравоохранение

Введение

Информационные технологии в здравоохранении (**Health Information Technology, HIT**) в настоящее время являются неотъемлемой частью оказания медицинской помощи, обеспечивая ведение клинической документации, назначение лекарственных препаратов, диагностику и координацию ухода. Хотя эти технологии приносят значительную пользу, они также создали новые риски для безопасности пациентов, которые зачастую трудно предвидеть, обнаружить или контролировать. Многие проблемы безопасности, связанные с **HIT**, возникают не из-за изолированных технических сбоев или индивидуальных ошибок, а вследствие сложных взаимодействий между цифровыми системами, клинической практикой, организационными структурами и механизмами управления. Таким образом, традиционные модели безопасности пациентов, ориентированные на дискретные ошибки или линейную причинно-следственную связь, недостаточны для объяснения того, как цифровые риски возникают и сохраняются на практике.

Методы/теоретический подход

В данной статье разрабатывается социотехническая теория рисков, связанных с **HIT**, основанная на науке о безопасности пациентов и теории социотехнических систем. Теория опирается на эмпирические данные исследований проблем безопасности, связанных с **HIT**, основанных на анализе инцидентов, и синтезирует доказательства из описаний реальных инцидентов. В работе используется концептуальный подход к построению теории, основанный на целенаправленном итеративном изучении соответствующей литературы по безопасности медицинских ИТ, социотехническим системам и моделям безопасности пациентов, ориентированным на устойчивость (**resilience-oriented frameworks**). Вместо анализа единого набора данных, в статье выявляются повторяющиеся механизмы, посредством которых цифровые риски возникают, остаются скрытыми, распространяются в различных контекстах, а также становятся поддающимися устранению или нет.

Результаты/теоретические положения

Предложенная теория концептуализирует риск, связанный с **HIT**, как динамический процесс, включающий четыре взаимосвязанных механизма: **возникновение риска**, **сокрытие риска**, **распространение риска** и **восстанавливаемость**. Риски возникают вследствие несоответствий между дизайном системы, её конфигурацией и клиническими рабочими процессами; они скрываются за счет автоматизации, фрагментации информации и адаптивных обходных путей (**workarounds**); они распространяются через тесно связанные цифровые инфраструктуры и общие зависимости; а их возможность устранения зависит от организационной способности к обнаружению, эскалации и обучению. В совокупности эти механизмы объясняют, почему инциденты, связанные с **HIT**, могут затрагивать множество пациентов или служб, почему приписывание вины отдельной ошибке человека вводит в заблуждение и почему проблемы безопасности могут сохраняться, несмотря на корректирующие усилия.

Обсуждение/последствия

Переосмысливая инциденты, связанные с **HIT**, как проявления уязвимостей на системном уровне, а не как изолированные сбои, эта социотехническая теория обеспечивает целостную объяснительную базу для понимания цифровой безопасности пациентов. Она подчеркивает, как риски могут незаметно развиваться в рамках рутинной практики, варьироваться по

степени видимости и масштабу, и акцентирует внимание на важности организационного обучения, управления и устойчивости в управлении цифровыми рисками безопасности.
