

Тот же ИИ, который помогает пациентам, используется для нападения на них, говорит руководитель больницы

Источник: MedCity News

Автор: Karen Habercoss

Дата публикации: 2026-07

Оригинал: <https://medcitynews.com/2026/07/ai-cybersecurity-hospital/>

ИИ в здравоохранении

информационная безопасность

кибербезопасность

регулирование

управление рисками

Искусственный интеллект (ИИ) играет все более центральную роль в уходе за пациентами в больницах по всей стране, однако те же модели, которые стимулируют эти инновации, также используются хакерами против поставщиков медицинских услуг.

Киберпреступники и государства используют ИИ для автоматизации и масштабирования своих атак со скоростью и точностью, которых не существовало еще несколько лет назад, заявила Карен Хаберкосс, директор по информационной безопасности и конфиденциальности в University of Chicago Medicine.

Она отметила, что киберпреступники используют ИИ по тем же причинам, что и больницы — для автоматизации задач и работы с большей скоростью и в большем масштабе.

«Риски необходимо сбалансировать», — заметила Хаберкосс в интервью в этом месяце.

Здравоохранение остается наиболее атакуемой отраслью в стране, и, по ее словам, эта проблема усугубляется объемом устаревших технологий (**legacy technology**), которые все еще используются во многих системах здравоохранения.

Эта старая инфраструктура не может быть заменена в одночасье, поэтому организациям приходится сосредотачиваться на сегментации и изоляции таких систем для снижения риска, пояснила Хаберкосс.

Дополнительным фактором является растущая сложность сторонних поставщиков, многие из которых теперь внедряют собственные инструменты ИИ в свои продукты. Хаберкосс отметила, что ее организация рассматривает надзор за поставщиками как непрерывный процесс, а не как разовую проверку по списку. Это включает в себя регулярный аудит партнеров, чтобы убедиться, что их методы обеспечения безопасности и конфиденциальности по-прежнему соответствуют стандартам самой системы здравоохранения.

Такой тип постоянного контроля стал необходимым по мере ускорения внедрения ИИ с обеих сторон уравнения безопасности, добавила Хаберкосс.

Чтобы управлять этой все более сложной сетью рисков, Хаберкосс сообщила, что за последние несколько лет UChicago Medicine разработала многоуровневую систему управления ИИ (**AI governance system**).

Она включает в себя руководящий комитет, который курирует подкомитеты, специализирующиеся на приеме ИИ, инвентаризации, образовании и обучении, а также аудите и мониторинге. Отдельный кросс-функциональный комитет, который Хаберкосс возглавляет совместно с директором по аналитике системы здравоохранения, объединяет врачей, юристов, специалистов по комплаенсу и других руководителей высшего звена. Третий комитет фокусируется именно на клинических сценариях использования, объединяя руководителей из числа медсестер и врачей с ее командой для проверки новых инструментов перед тем, как они попадут к пациентам.

Любой новый инструмент ИИ — будь то внедренный через контракт с поставщиком, по запросу врача или в рамках исследовательского проекта факультета — проходит через все три комитета, прежде чем будет одобрен, сказала Хаберкосс. Она отметила, что такая избыточность является намеренной.

«Если вам кажется, что вы обсудили это с достаточным количеством людей, скорее всего, это не так», — заявила Хаберкосс, добавив, что решения в области ИИ часто затрагивают федеральные законы и законы штатов, которые ни один отдел не может отслеживать в одиночку.

Цель состоит в том, чтобы ни одно подразделение организации не принимало решения об ИИ изолированно, заявила она.

Перевод выполнен: 21.07.2026 | ai4med.ru

Машинный перевод. Рекомендуем сверять с оригиналом при клиническом использовании.