Кибервзломы медицинских устройств: анализ сообщений FDA о безопасности в ответ на опасения пациентов

Источник: Frontiers in Digital Health

Дата публикации: 2025

Оригинал: https://www.frontiersin.org/articles/10.3389/fdgth.2026.1701551

FDA | безопасность данных | интернет вещей (IoT) | кибербезопасность | медицинские устройства | регулирование

Введение

Растущая интеграция подключенных медицинских устройств и технологий интернета вещей (**IoT** — Internet of Things) в здравоохранение значительно улучшила уход за пациентами и операционную эффективность. Однако эта стремительная цифровая трансформация также привнесла серьезные уязвимости в кибербезопасность медицинских устройств, создавая риски для безопасности пациентов и конфиденциальных данных о здоровье. Угрозы кибербезопасности могут позволить несанкционированный удаленный доступ к устройствам, вызвать сбои в работе оборудования и привести к утечкам данных. По мере того как медицинские устройства становятся все более взаимосвязанными внутри систем здравоохранения, обеспечение их безопасности становится критическим приоритетом для регулирующих органов, производителей и поставщиков медицинских услуг.

Методы

В данном исследовании с использованием метода систематического качественного контент-анализа изучаются сообщения по безопасности кибербезопасности, выпущенные Управлением по санитарному надзору за качеством пищевых продуктов и медикаментов США (**FDA** — Food and Drug Administration) в период с 2013 по 2025 год. Анализ сосредоточен на определении частоты оповещений, степени серьезности уязвимостей и потенциальных рисков, представляющих угрозу для инфраструктуры здравоохранения и безопасности пациентов. В исследовании также рассматриваются регуляторные меры и нормативно-правовые базы, внедренные FDA для решения проблем рисков кибербезопасности в медицинских устройствах.

Результаты

Анализ показал, что FDA выпустило 18 сообщений по безопасности, связанных с нарушениями кибербезопасности в медицинских устройствах. Среди зарегистрированных уязвимостей 94% были классифицированы как имеющие высокий уровень риска, что указывает на серьезные потенциальные последствия, включая несанкционированный удаленный доступ к медицинским устройствам, возможные сбои в работе устройств и раскрытие конфиденциальных данных пациентов. Кроме того, результаты демонстрируют заметное увеличение количества сообщений FDA по безопасности кибербезопасности с течением времени, что отражает растущую серьезность и распространенность угроз кибербезопасности в медицинских технологиях.

Обсуждение

Полученные результаты подчеркивают необходимость разработки более надежных стратегий кибербезопасности в здравоохранении. Сотрудничество между производителями медицинских устройств, поставщиками медицинских услуг и регулирующими органами, наряду с непрерывным мониторингом и соблюдением нормативных требований, необходимо для защиты безопасности пациентов и конфиденциальных данных о здоровье в условиях все более взаимосвязанной среды здравоохранения.