Вне радаров: как неодобренный ИИ усложняет киберриски в здравоохранении

Источник: MedCity News

Оригинал: https://medcitynews.com/2026/07/off-the-radar-how-unapproved-ai-is-complicating-healthcare-cyber-risk/

информационная безопасность | кибербезопасность | регулирование | теневой ИИ | управление рисками

В сфере здравоохранения существует скрытая теневая экономика, и клиническое выгорание является её источником финансирования. Пока ИТ-отделы больниц месяцами проверяют платформы корпоративного уровня, изнуренные врачи и медсестры берут дело в свои руки. Они не ждут завершения циклов закупок. Вместо этого персонал незаметно вставляет данные пациентов в бесплатные, неодобренные веб-инструменты просто для того, чтобы справиться с административной нагрузкой. Неудивительно, что «теневой ИИ» (**Shadow AI**) представляет собой невидимый риск, который часто остается незамеченным системами управления рисками.

Выгорание стимулирует теневую экономику

Здравоохранение погрязло в долгах — административных долгах. И медицинский персонал потихоньку проводит «спасательную операцию». Спросите любой ИТ-отдел больницы о его стратегии в области искусственного интеллекта, и они укажут на инструменты визуализации корпоративного уровня или тщательно проверенные прогностические модели. Спросите утомленного врача на одиннадцатом часу смены, и реальность будет выглядеть совершенно иначе.

Под давлением нарастающей тяжести ведения карт и документации врачи, медсестры и административные работники берут дело в свои руки. Они не ждут многомесячных циклов ИТ-закупок. Вместо этого они копируют истории болезни пациентов в бесплатные веб-сервисы для суммаризации (обобщения текста), неодобренные приложения для транскрибации и несанкционированные расширения для браузеров, просто чтобы удержаться на плаву.

Это и есть зарождение «теневого ИИ» (**Shadow AI**). Это стремительно расширяющаяся экономика непроверенного и неконтролируемого использования технологий, которая функционирует параллельно с официальными клиническими рабочими процессами. Важно понимать, что это не злонамеренная внутренняя угроза. Это рациональный побочный продукт системного клинического выгорания, столкнувшегося с высокодоступным потребительским программным обеспечением, — и это происходит совершенно незаметно.

Риск: расширение поверхности атаки в тени

Основная опасность **Shadow AI** заключается не в самой технологии, а в утечке данных (**data egress**), которую она создает — в самой «теневой» составляющей этого явления. Когда сотрудник вставляет сложную карту пациента или неанонимизированный план лечения в бесплатный онлайн-инструмент, эти данные не исчезают просто так после того, как инструмент сформирует резюме. В большинстве моделей, ориентированных на потребителя, эта информация поглощается, хранится и используется для обучения программного обеспечения в целях его дальнейшего улучшения.

Без заключенного Соглашения о деловом партнере (**BAA** — Business Associate Agreement), обычная административная хитрость мгновенно превращается в серьезное нарушение закона **HIPAA** (Закон о переносимости и подотчетности страхования медицинского страхования) и прямую утечку данных.

Более того, подобная практика создает профиль риска, крайне уязвимый для третьих лиц. Киберпреступники прекрасно знают, что больничные брандмауэры (файерволы) надежны, поэтому они переключают внимание на более слабые звенья: слабо защищенные ИИ-стартапы с венчурным капиталом, в которые сотрудники здравоохранения ежедневно передают данные.

Для руководства это создает значительный разрыв в осведомленности. Традиционные платформы обнаружения и реагирования на конечных точках (**EDR** — Endpoint Detection and Response) и системы сетевой безопасности созданы для обнаружения вредоносного ПО или несанкционированной передачи файлов; они практически слепы, когда сотрудник просто переходит по легитимно выглядящему URL-адресу и взаимодействует с расширением веб-браузера. Нельзя обезопасить то, чего вы не видите, а в данный момент организации здравоохранения накапливают скрытые кибер-обязательства с каждым нажатием клавиши.

Эффект домино на рынке: слепое пятно андеррайтинга

Это слепое пятно распространяется далеко за пределы ИТ-отдела, осложняя работу корпоративного управления рисками. В прошлом картирование кибер-ответственности было стандартной формальностью. Андеррайтеры и риск-менеджеры оценивали осязаемую, предсказуемую инфраструктуру — такие вещи, как прочность брандмауэра, показатели фишинга среди сотрудников и графики установки обновлений серверов.

Shadow AI разрушает эту традиционную структуру андеррайтинга. Поскольку ИИ-инструменты потребительского уровня работают полностью за пределами корпоративного периметра, они представляют собой не поддающуюся количественной оценке переменную. Когда система здравоохранения готовится к ежегодной оценке рисков или продлению страховых полисов, руководители должны подтверждать абсолютную безопасность своих механизмов контроля данных. Однако если сотни сотрудников самостоятельно загружают проприетарные данные или защищенную медицинскую информацию (**PHI** — Protected Health Information) на внешние серверы больших языковых моделей (**LLM**), эти корпоративные заверения непреднамеренно становятся неточными.

Финансовые последствия этого слепого пятна существенны. Если произойдет утечка данных через непроверенное стороннее ИИ-приложение, о котором руководство не знало, организации могут столкнуться с катастрофическими регуляторными штрафами и крайне сложным процессом подачи страховых претензий. Страховщики не могут оценивать риски, которые они не могут измерить, и в настоящее время отрасль пытается понять, насколько глубоко простирается эта скрытая угроза.

Решение: переход от тотальных запретов к защитным барьерам

Многие из нас видели, как руководители пытаются решить подобные проблемы путем внесения в «черные списки» «запрещенных» инструментов или всех потребительских ИИ-платформ в корпоративной сети. Но запреты редко работают. Вместо этого жесткие меры заставляют отчаявшихся сотрудников становиться еще изобретательнее, используя личные устройства или прибегая к обходным путям, просто чтобы не отставать от ежедневных административных задач.

На самом деле работает замена жесткого принуждения на реалистичный надзор. Другими словами, если руководители здравоохранения хотят обезопасить свои границы данных, они должны внедрить более прагматичную стратегию. Они должны признать то, что действительно необходимо сотрудникам для успешной работы, при этом обеспечивая безопасность предприятия.

- **Внедряйте инструменты непрерывного обнаружения:** команды безопасности не могут полагаться на статические аудиты. Организациям необходимо развернуть инструменты видимости на сетевом уровне, которые могут отслеживать исходящие потоки данных и выявлять несанкционированные вызовы **API** к внешним языковым моделям в режиме реального времени.
- **Создавайте беспрепятственные пути одобрения:** основным драйвером **Shadow AI** является медленный темп корпоративных ИТ-закупок. Создание процесса ускоренной проверки специально для недорогих, но высокоэффективных административных ИИ-инструментов позволит клиническим командам внедрять безопасные альтернативы до того, как они впадут в отчаяние и начнут скачивать непроверенные расширения для браузеров.
- **Пересмотрите подход к обучению персонала:** стандартное обучение комплаенсу (соответствию нормативным требованиям) часто имеет мало реального эффекта. Для большинства сотрудников это просто галочка в списке дел. Тем не менее, руководители должны показать клиницистам, как вставка заметки о пациенте в бесплатный веб-инструмент может превратить обычную попытку сэкономить время в масштабную утечку конфиденциальности.

Внесение в черные списки и ограничения не решают проблему. Они заставляют изнуренных сотрудников искать новые, непроверенные обходные пути. Вместо того чтобы пытаться запретить всё, руководители здравоохранения должны предоставить одобренные, безопасные пути для выполнения административных задач.

Фото: WhataWin, Getty Images

Джастин Козак — исполнительный вице-президент в Founder Shield, технологически продвинутом коммерческом страховом брокерском агентстве. Он возглавляет практику в области наук о жизни (Life Sciences), имея более 10 лет опыта управления рисками в Hub International, PBC, а теперь в Founder Shield. Он начал свою карьеру со степени бакалавра истории в Делавэрском университете, где его глубокое понимание прошлого подпитывает его интуицию в мире страхования. Неудивительно, что специализацией Джастина является разработка индивидуальных страховых программ для развивающихся рынков с небольшим объемом исторических данных. Он любит проводить время со своей молодой семьей и является преданным болельщиком команды «Филлис».

Данный пост опубликован в рамках программы MedCity Influencers. Любой желающий может опубликовать свое мнение о бизнесе и инновациях в здравоохранении на MedCity News через MedCity Influencers. Нажмите здесь, чтобы узнать, как это сделать.
