УДК 004.056

РАЗРАБОТКА МЕТОДОЛОГИИ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ЗДРАВООХРАНЕНИЯ, ИСПОЛЬЗУЮЩИХ ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ

Пересторонина О.В.
Научный руководитель – Профессор Лившиц И.И.
Университет ИТМО

Рассмотрена готовность медицинских учреждений, как субъектов критической информационной инфраструктуры (КИИ), к внедрению и обеспечению защищенности искусственного интеллекта и обрабатываемых им данных. Рассмотрены преимущества внедрения искусственного интеллекта в сфере здравоохранения.

Введение. Сегодня медицинские учреждения стремительно информатизируются, переходят к комплексной автоматизации, отвечающей требованиям информационного прогресса общества: интеграция в единое информационное пространство, внедрение технологий электронных реестров и медицинских карт. Информатизация медицины является одним из критериев оказания качественной и своевременной медицинской помощи, а также эффективного управления здравоохранением. В связи с этим, встает вопрос о внедрении искусственного интеллекта (ИИ) в качестве помощника для обеспечения сверхточной (или прецизионной) медицины, в рамках которой появится возможность назначать индивидуальное лечение каждому отдельному человеку, учитывая его уникальные генетические и другие особенности.

Согласно Федеральному Закону №187-ФЗ, информационные и телекоммуникационные системы медицинских учреждения относятся к объектам КИИ, так как организации, функционирующие в сфере здравоохранения, являются субъектами КИИ. Соответственно, встает вопрос о более внимательном подходе к защите медицинских учреждений, в особенности тех, которые планируют использовать ИИ для повышения качества оказываемых услуг (например, SOPHiA AI – приложения по диагностике рака, которое по результатам анализа клинической картины может предложить эффективную схему лечения).

Основная часть. Тема обеспечения информационной безопасности является актуальной и по сей день. В особенности на объектах, которые работают с информацией конфиденциального характера и достаточно крупным информационным оборотом, но которые не имеют должной компетенции в этой области. Более того, являющегося субъектом КИИ.

Первым этапом повышения уровня защищенности медицинского учреждения является процедура категорирования со всеми сопутствующими этапами (определение активов, перечня объектов, подлежащих категорированию, определение модели угроз и модели нарушителя и др.). По полученным результатам обозначается категория значимости объектов и, в соответствии с требованиями законодательства для определенной категории, базовый набор требований обеспечения защищенности.

Далее должна проводиться оценка реализованных мер защиты. Методы оценки могут выбираться разнообразные, в зависимости от решения руководителя структурного подразделения, отвечающего за обеспечение безопасности или непосредственного руководителя организации. Однако существуют более предпочтительные методы оценивания, которые содержатся в российских и международных стандартах (например, стандарт ISO/IEC 15408, ГОСТ Р ИСО/МЭК 27005-2010, Методика оценки угроз безопасности информации от ФСТЭК, NIST Special Publication 800–26 «Security Self-Assessment Guide for Information Technology Systems» и другие).

По результатам оценки можно сделать вывод об уровне защищенности активов организации. В общем случае, для медицинских учреждений этот показатель довольно низкий. Отсюда можно сделать вывод, что область медицины еще не готова к внедрению ИИ по своему уровню компетенции и возможностей в области информационной безопасности.

Если рассмотреть внедрение ИИ в качестве примера, то нужно учитывать, что добавление нового элемента в системе приводит к понижению уровня защищенности, так как появляются новые уязвимости и угрозы. ИИ использует алгоритмы и программное обеспечение, чтобы аппроксимировать знания человека при анализе медицинских данных. Применение ИИ в медицине сейчас развивается в различных направлениях: от возможности удаленной помощи пациенту до разработки лекарственных препаратов и использования технологий машинного обучения в сфере протезирования с учетом анатомических особенностей человека.

В связи с появлением нового незащищенного элемента системы, необходимо заново провести оценку уровня защищенности, чтобы иметь представление, закрывают ли реализованные меры защиты требования законодательства для ИИ. В целом, ИИ рассматривается как программно-аппаратный комплекс и при определения требований в области информационной безопасности следует учитывать специфику обрабатываемых данных. В этой работе ИИ рассматривается как объект КИИ, а значит, для него применяются требования согласно законодательству в области КИИ (ФЗ №187, ПП №127, Приказ ФСТЭК №239 и т.д.).

Выводы. На данный момент внедрение ИИ в медицинское учреждение не оправдано в связи с недостаточной информатизацией в сфере здравоохранения. Однако, при рассмотрении безопасности ИИ необходимо следовать законодательным мерам согласно обрабатываемой информации (например, для персональных данных – это ФЗ №152 «О персональных данных»).

Пересторонина О.В. (автор) Подпись

Лившиц И.И. (научный руководитель) Подпись