УДК 004.056.53

РАЗРАБОТКА СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА В СИСТЕМЕ, ОПЕРИРУЮЩЕЙ МЕДИЦИНСКИМИ ДАННЫМИ

Самойлов М.Б. (Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Коржук В.М.
(Университет ИТМО)
Научный консультант - Керимбай А.
(Университет ИТМО)

Введение. В современном обществе обработка, хранение и передача медицинских данных стали неотъемлемой частью здравоохранительных систем. Обеспечение конфиденциальности этих данных, в частности персональных, становится приоритетом, так как медицинские данные подпадают под особые требования по защите приватности и обработке, которые описаны в 152 Федеральном законе [1]. Нарушения безопасности в этой области могут иметь серьезные последствия, включая утечку чувствительной информации и нарушение доверия между пациентами и медицинскими учреждениями. Облачные сервисы, предоставляя эффективные механизмы хранения и защиты информации, выделяются как важное средство. Их применение в обработке медицинских данных становится все более популярным в силу своей гибкости, масштабируемости и возможности обеспечения высокого уровня конфиденциальности. Облачные технологии позволяют создавать защищенные среды для хранения и обработки медицинских данных, обеспечивая надежные механизмы авторизации и аутентификации, тем самым разграничивая доступ, обеспечивая требуемый уровень конфиденциальности. Это позволяет эффективного управлять доступом, а также обеспечивать высокую степень защиты от угроз в облачных сервисах.

Целью проекта является повышение уровня защищенности системы, оперирующей медицинскими данными.

Основная часть.

Разрабатываемая система является частью проекта по созданию системы хранения и взаимодействия с медицинскими данными, которая включает в себя:

- полную инфраструктуру для агрегации медицинских данных;
- разработку моделей искусственного интеллекта на базе медицинских данных;
- интерфейс для взаимодействия врачей с обученными моделями.

В данной системе будут использоваться медицинские данные, конфиденциальность которых необходимо сохранять. Банк данных угроз [2] определяет актуальные угрозы для облачных сервисов и хранящихся там данным, где на безопасность системы воздействуют как внутренние, так и внешние нарушители. Для обеспечения соответствующего уровня защиты информации будут использоваться сертифицированные ФСТЭК средств защиты информации, что гарантирует соответствие ГОСТам, техническим регламентам и нормативным актам.

Система разграничения доступа играет решающую роль в предотвращении указанных угроз. Она позволяет определить и ограничить доступ к медицинским данным только соответствующим, авторизованным пользователям. Разграничение прав помогают минимизировать риски внутреннего и внешнего воздействия на систему обработки медицинских данных. В рамках работы для каждого средства защиты и сервера для хранения или обработки информации будет указана методика разграничения доступа, определены необходимые пользователи с необходимыми для функционирования правами с использованием механизмов авторизации и аутентификации.

Выводы.

Разработана система разграничения доступа в системе, оперирующей медицинскими данными, обеспечивающая высокий уровень защищенности, соответствуя требованиям законодательства и этическим нормам в сфере здравоохранения.

Результаты моделирования и тестов будут представлены в будущей выпускной квалификационной работе.

Список использованных источников:

1. Российская Федерация. Законы. О персональных данных : Федеральный закон № 152-ФЗ : [принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г.]. – Москва : Проспект ; Санкт-Петербург : Кодекс, 2024.
2. ФСТЭК. Банк данных угроз безопасности информации ФСТЭК [Электронный ресурс]. – 2023. – URL: https://bdu.fstec.ru/

Автор_____ Самойлов М.Б.

Научный руководитель_____Коржук В.М.

Научный консультант_____Керимбай А.