УДК 004.652.4
DOI: 10.46548/21vek-2020-0950-0019

РАЗРАБОТКА ЗАЩИЩЁННОЙ БАЗЫ ДАННЫХ ДЛЯ ТЕЛЕМЕДИЦИНСКОЙ СИСТЕМЫ

Миков Дмитрий Александрович, кандидат технических наук,
доцент кафедры «Компьютерные системы и сети»
Московский государственный технический университет имени Н.Э. Баумана
(105005, Россия, Москва, ул. 2-я Бауманская, 5, e-mail: MikovDA@yandex.ru)

Аннотация. Телемедицинские системы, осуществляющие дистанционный мониторинг состояния здоровья пациентов, работают с информацией, составляющей врачебную тайну, и персональными данными. Обеспечение информационной безопасности в данной сфере является жизненно важной для функционирования таких систем задачей. Помимо управления информационными рисками и обеспечения безопасной передачи данных, остаётся нерешённой задача эффективного хранения информации, связанная с разработкой базы данных, позволяющей реализовать защищённую среду хранения информации. В статье определён круг задач, решаемых телемедицинской системой, представлены этапы процесса её функционирования, определены критерии принятия решений. На основе рассмотренных принципов построения и особенностей реализации представлена структурная схема телемедицинской системы, состоящая из трёх слоёв. Описаны принципы функционирования подсистем, их структурных компонентов и элементов, включая взаимодействие между базой данных и серверной частью, построена диаграмма деятельности. Сформулирована совокупность требований к телемедицинской базе данных, обеспечивающих эффективность её функционирования и защищённость хранимой и обрабатываемой ей информации, определён круг выполняемых ей типовых запросов. Проведён сравнительный анализ дискреционной, мандатной и ролевой моделей управления доступом в телемедицинской базе данных. Разработана политика управления доступом к данным на основе ролевой модели.

Ключевые слова: защита информации, информационная безопасность, телемедицина, врачебная тайна, персональные данные, базы данных, диаграмма деятельности, ролевое управление доступом.

DEVELOPMENT OF A SECURE DATABASE FOR THE TELEMEDICINE SYSTEM

Mikov Dmitry Alexandrovich, candidate of engineering sciences,
associate professor of the department of «Computer systems and networks»
Bauman Moscow State Technical University
(105005, Russia, Moscow, 2-nd Baumanskaya, 5, e-mail: MikovDA@yandex.ru)

Abstract. Telemedicine systems that carry out remote monitoring of the health status of patients work with information constituting a medical secret and personal data. Ensuring information security in this area is a vital task for the functioning of such systems. In addition to information security risk management and ensuring secure data transfer, the problem of efficient information storage remains unresolved, associated with the development of a database that allows implementing a secure information storage environment. The article defines the range of tasks solved by the telemedicine system, presents the stages of the process of its functioning, defines the decision-making criteria. Based on the considered construction principles and implementation features, a structural diagram of a telemedicine system consisting of three layers is presented. The principles of the functioning of subsystems, their structural components and elements, including the interaction between the database and the server part, are described, an activity diagram is constructed. The set of requirements for the telemedicine database is formulated, ensuring the effectiveness of its functioning and the security of the information stored and processed by it, and the range of typical performed queries is determined. A comparative analysis of the discretionary, mandatory and role-based access control in the telemedicine database is carried out. A data access control policy based on a role model is developed.

Keywords: data protection, information security, telemedicine, medical secrecy, personal data, database, activity diagram, role-based access control.

Введение. В системах, осуществляющих дистанционный мониторинг состояния объектов, жизненно важным является вопрос обеспечения информационной безопасности [1, 2]. Это особенно актуально в телемедицинских системах, предназначенных для дистанционной оценки состояния здоровья пациентов [3, 4]. Все созданные модели угроз информационной безопасности телемедицинских систем выявляют проблему защиты как при передаче, так и при хранении данных [5, 6].

Независимо от используемых технологий хранения данных, конфиденциальность, целостность и/или доступность информации в телемедицинских системах может быть нарушена за счёт несанкционированных воздействий, в том числе и целенаправленного характера [7, 8]. С учётом наличия информации, составляющей врачебную тайну, и персональных данных в телемедицинских системах любое нарушение информационной безопасности может стать критичным [9, 10]. Надёжность функционирования телемедицинских систем зависит от управления информационными рисками, обеспечения

безопасной передачи данных и эффективного хранения информации [11].

Целью данной работы является исследование последнего аспекта – формулирование совокупности принципов разработки базы данных, позволяющих реализовать защищённую среду хранения информации в телемедицинской системе.

Материалы и результаты исследования. Проектированию базы данных предшествует моделирование предметной области, для чего необходимо предварительно провести анализ с учётом современных потребностей в информации при принятии врачебных решений и выделить совокупность задач телемедицинской системы [12]:

1) описание диагноза;

2) классификация согласно действующим методикам и стандартам;

3) сбор данных о нежелательных побочных воздействиях;

4) исследование методов лечения на совместимость;

5) выбор наиболее эффективного алгоритма лечения;

6) поддержка принятия окончательного врачебного решения.

То есть исследуемая предметная область тесно связана с процессом перебора вариантов и поиска методов лечения. Можно представить функционирование телемедицинской системы в виде следующих этапов [13]:

1) описание состояния пациента на основе дистанционного сбора данных, включая проведение анализов и постановку диагноза;

2) анализ ограничений при наличии аллергии, нарушении функций отдельных подсистем организма;

3) выбор наиболее эффективного алгоритма лечения;

4) прогнозирование вариантов результата лечения, включая оценку безопасности и вероятности появления побочных воздействий.

В соответствии с теорией принятия решений необходимо идентифицировать критерии выбора, множество альтернатив и алгоритм выбора альтернатив на основе критериев. Для телемедицинской системы существуют следующие критерии принятия решений [14]:

1) диагноз пациента;

2) алгоритм лечения;

3) потенциально возможные побочные воздействия (например, из-за аллергических реакций).

Рассмотренные принципы построения и особенности реализации позволили представить следующую структурную схему телемедицинской системы (рис. 1).

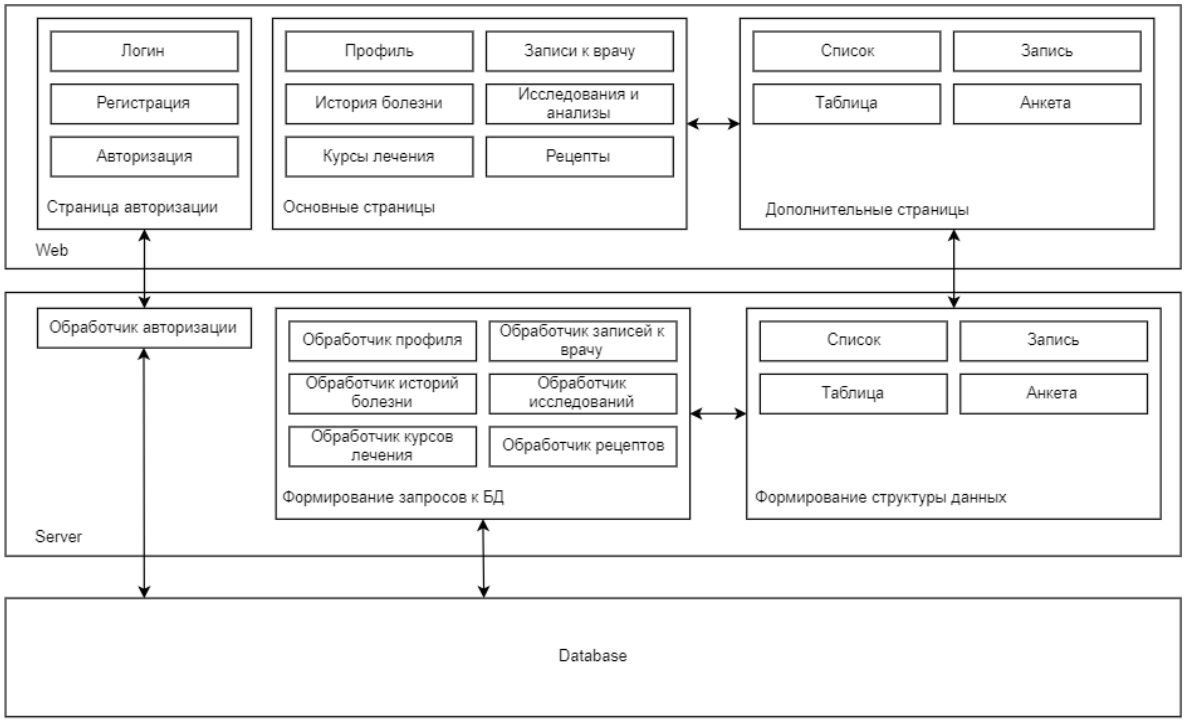

Рисунок 1 – Структурная схема телемедицинской системы

Структура делится на три слоя: *web* – включает то, что находится на стороне клиента; *server* – включает то, что находится на стороне сервера; *database* – база данных [15].

У страницы авторизации на стороне сервера отдельный обработчик по причине того, что запросы к ней будут происходить часто, и нет необходимости формировать особые структуры данных наподобие списков, так как взаимодействие происходит короткими сообщениями.

Для основных страниц необходимо структурировать данные особым образом, чтобы корректно отображать списки, записи, таблицы и анкеты. Для этого существуют дополнительные страницы, которые

берут задачу визуализации этих структур данных на себя.

На стороне сервера находятся классы, которые структурируют данные под формат, необходимый конкретной дополнительной странице. Например, класс «список» создаёт структуру данных, которую может обработать дополнительная страница «список» и т.д.

Для каждой основной страницы существует запрос к базе данных, который выполняет извлечение необходимых данных для класса, формирующего структуру данных. У каждого такого запроса существует свой обработчик в области формирования запросов к базе данных.

На основе выявленных особенностей предметной области выполнено её моделирование. При помощи унифицированного языка моделирования *UML* разработана диаграмма деятельности, позволяющая учитывать всю необходимую для принятия решения информацию (рис. 2).

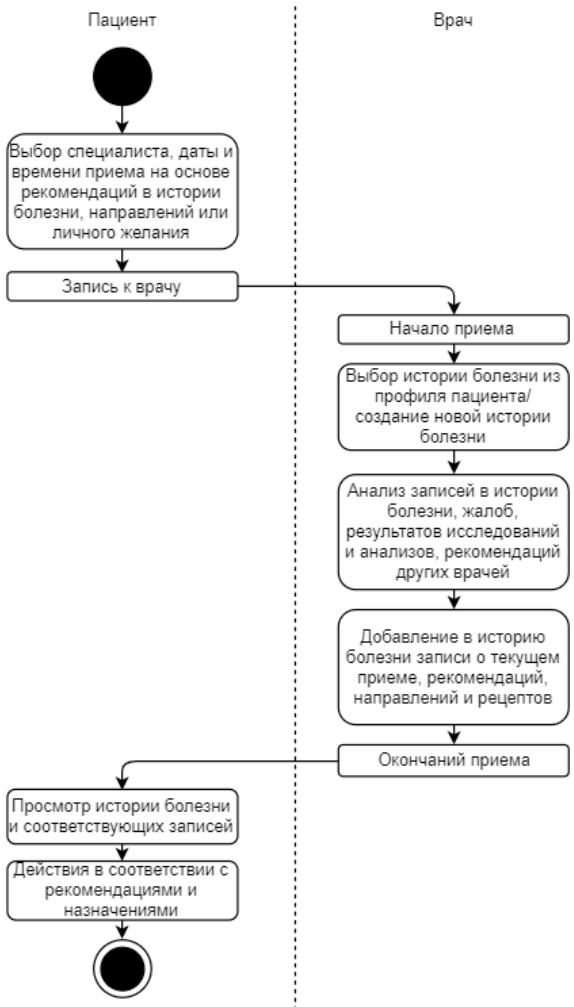

Рисунок 2 – Диаграмма деятельности

Требования к телемедицинской базе данных. При переносе разработанной модели предметной области в реляционную СУБД необходимо обеспечить соответствие следующим требованиям к схеме данных [16]:

1) схема данных должна давать полное представление о предметной области;

2) в схему данных должны быть включены все необходимые для выполнения запросов таблицы и их атрибуты соответственно;

3) наименования таблиц должны быть уникальными;

4) наименования атрибутов в пределах одной таблицы должны быть уникальными;

5) необходимо гарантировать однозначную трактовку схемы данных;

6) каждое отношение должно содержать первичный ключ;

7) схема данных должна быть гибкой, способной дополняться без масштабных преобразований существующей схемы данных при необходимости выполнения новых запросов;

8) список таблиц должен быть минимальным;

9) таблица создаётся только в том случае, если без неё невозможно выполнить запрос;

10) список атрибутов должен быть минимальным;

11) атрибут включается в таблицу только в том случае, если без него описание предметной области не будет исчерпывающим;

12) первичный ключ таблицы должен быть минимальным, с невозможностью исключения из него атрибутов без нарушения однозначной идентификации.

Телемедицинская база данных должна обеспечить выполнение следующих запросов [17]:

1) идентификация пользователя;

2) подключение к истории болезни и другой архивной информации;

3) создание списков пациентов;

4) создание исчерпывающего набора данных о пациенте;

5) добавление результатов анализов и осмотров;

6) добавление и редактирование медицинских данных о пациенте;

7) формирование шаблонов;

8) подключение к дополнительным данным (лабораторная информация, лекарственные средства, международная классификация болезней, медиафайлы).

Политика управления доступом. Наконец, для обеспечения безопасной работы с данными необходимо разработать политику управления доступом к данным в соответствии с одной из перечисленных моделей [18-20]: дискреционное управление доступом; мандатное управление доступом; ролевое управление доступом.

Дискреционное управление доступом нецелесообразно, поскольку в телемедицинской базе данных количество пользователей и ресурсов будет исчисляться сотнями и тысячами, то есть перечисление допустимых типов доступа для каждой пары «субъект – объект» является неоправданно громоздкой задачей. Мандатное управление доступом с его жёстким разграничением на основе меток доступа являются ключевым отличием систем защиты государственной тайны и не подходят для телемедицинской системы, где необходима более гибкая настройка. Ролевое управление доступом наиболее эффективно для ре-

шения стоящей задачи, поскольку нет необходимости в перечислении допустимых типов доступа для каждой пары «субъект – объект», которые заменяются назначением каждому пользователю соответствующей роли. В то же время отсутствует жёсткая привязка к меткам доступа, что обеспечивает гибкую политику управления доступом (табл. 1).

Таблица 1 – Политика управления доступом

Роль	**Данные медицинского учреждения**	**Данные персонала**	**Данные пациентов**	**Системные данные**
Администратор	Чтение Запись Создание Удаление	–	–	Чтение Запись Создание Удаление
Главный врач	Чтение Запись	Чтение Запись Создание Удаление	Чтение Запись Создание	–
Заместитель главного врача	Чтение	Чтение Запись Создание Удаление	Чтение Запись Создание	–
Заведующий отделением	Чтение	Чтение Запись	Чтение Запись Создание	–
Дежурный врач	Чтение	Чтение	Чтение Запись Создание	–
Врач	Чтение	–	Чтение Запись Создание	–
Медсестра	Чтение	–	Чтение Запись Создание	–

Заключение. Важной задачей при проектировании телемедицинской системы является обеспечение гибкого взаимодействия между базой данных и пользователем. Эффективность проектирования телемедицинской базы данных зависит от полноты объектной модели предметной области и соблюдения совокупности требований при её преобразовании в реляционную модель. Защищённость информации в телемедицинской базе данных обеспечивается ролевой политикой управления доступом, основанной на группировке пользователей по ролям, без назначения прав доступа каждому пользователю в отдельности, что характерно для дискреционной модели, и без жёсткой привязки к меткам доступа, что характерно для мандатной модели.

СПИСОК ЛИТЕРАТУРЫ:

1. Булдакова Т.И., Джалолов А.Ш. Анализ информационных процессов и выбор технологий обработки и защиты данных в ситуационных центрах // Научно-техническая информация. Серия 1. 2012. №6. С. 16-22.

2. Анализ информационных рисков виртуальных инфраструктур здравоохранения / Т.И. Булдакова, С.И. Суятинов, Д.А. Миков // Информационное общество. 2013. №4. С. 6.

3. Концептуальная модель виртуального центра охраны здоровья населения / В.С. Анищенко, Т.И. Булдакова, П.Я. Довгалевский, В.Б. Лифшиц, В.И. Гриднев, С.И. Суятинов // Информационные технологии. 2009. №12. С. 59-64.

4. Булдакова Т.И., Кривошеева Д.А. Угрозы безопасности в системах дистанционного мониторинга // Вопросы кибербезопасности. 2015. №5. С. 45-50.

5. Булдакова Т.И., Миков Д.А. Методика анализа информационных рисков с применением нейро-нечёткой сети // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2015. №4. С. 13-17.

6. Venkatasubramanian K.K., Banerjee A., Gupta S.K.S. PSKA: Usable and secure key agreement scheme for body area networks // IEEE Transactions on Information Technology in Biomedicine. 2010. Vol. 14, no 1. Pp. 60-68.

7. Булдакова Т.И., Суятинов С.И. Модельный подход к защите данных в телемедицинских системах // Вестник Технологического университета. 2016. Т. 19. №23. С. 85-87.

8. Миков Д.А., Булдакова Т.И., Сюзев В.В., Смирнова Е.В. Анализ методов интеллектуального моделирования информационных процессов в системах дистанционного мониторинга состояния объектов // Проблемы современной науки и образования. 2018. №13 (133). С. 23-27.

9. Миков Д.А. Формирование защищённой экспертной системы поддержки принятия решений в медицинской диагностике // Электронный журнал: наука, техника и образование. 2019. №4 (27). С. 79-84.

10. Миков Д.А., Булдакова Т.И., Сюзев В.В., Смирнова Е.В., Бауман Ю.И. Модели оценки защищённости данных в информационно-управляющих системах реального времени // Проблемы современной науки и образования. 2019. №11-1 (144). С. 15-20.

11. Булдакова Т.И., Миков Д.А., Соколова А.В. Управление информационными рисками в телемедицинских системах // Сборник трудов XIII Всероссийского совещания по проблемам управления ВСПУ-2019. Институт проблем управления им. В.А. Трапезникова РАН. 2019. С. 2512-2516.

12. Гильманшина А.Л. Анализ литературы и нормативно-правовой базы в области защиты персональных данных // Вестник науки. 2019. Т. 2. №3 (12). С. 13-16.

13. Долматов А.В., Долматов Е.А. Проблемы и особенности правового регулирования защиты персональных данных // Юрист ВУЗа. 2019. №5. С. 13-23.

14. Климов В.А. Как защитить персональные данные в лечебном учреждении // Главврач. 2019. № 4. С. 63-65.

15. Рогова О.С., Добржинская Т.Ю., Фоминова Е.Р. Анализ защищённости распределённых систем и методов тестирования // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2019. №2. С. 43-45.

16. Гаршина В.В., Степанцов В.А. Способы защиты баз данных от несанкционированного доступа // В сборнике: Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-методической конференции. Под ред. Д.Н. Борисова. Воронеж, 2019. С. 683-686.

17. Комилов Х.И., Иванищева А.А., Гехаев М.Д. Эффективность гибридных алгоритмов для защиты баз данных // Инновационная наука. 2019. №3. С. 43-45.

18. Тур Д.Е., Цирулева В.М. Анализ математических методов выявления аномальных SQL-запросов к базам данных // В сборнике: Математические методы управления. Сборник научных трудов. Тверь, 2019. С. 112-126.

19. Солодков А.М., Цирулева В.М. Исследование способов обнаружения аномалий в SQL-запросах к базам данных // В сборнике: Столетие физико-математического образования в Верхневолжском регионе. Сборник научных трудов научной конференции. 2018. С. 109-115.

20. Линник О.В., Галушка В.В. Модель распределённого представления симметричного ключа при сквозном шифровании баз данных // Синергия Наук. 2019. №31. С. 1033-1040.

Статья поступила в редакцию 10.04.2020
Статья принята к публикации 10.06.2020