Лиманова Наталия Игоревна

док. тех. наук, профессор, ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия, г. Самара

Шевченко Виталий Сергеевич

студент, ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия, г. Самара

ОСОБЕННОСТИ РАЗРАБОТКИ БАЗЫ ДАННЫХ КАК ОСНОВЫ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Аннотация. Разработка базы данных как основы медицинской информационной системы (МИС) — это критически важный и многоэтапный процесс, объединяющий технологические и организационные аспекты. В статье рассматриваются ключевые требования к проектированию базы данных: надежность, масштабируемость, безопасность и соответствие специфике медицинских учреждений. Особое внимание уделяется вопросам защиты данных, в том числе контролю доступа, шифрованию, логированию действий пользователей, защите от внутренних и внешних угроз. Описаны архитектурные подходы, поддерживающие работу с разнотипными медицинскими данными, а также необходимость гибкой интеграции с внешними системами и масштабирования. Представлены принципы ролевого доступа, механизмы резервного копирования и стратегии обеспечения непрерывности работы системы. Подчеркивается, что база данных в МИС — это не просто хранилище, а фундамент цифровой медицины, влияющий на качество обслуживания и безопасность пациентов.

The development of a database as the foundation of a Medical Information System (MIS) is a critical and multifaceted process that encompasses both technological and organizational dimensions. This article outlines the essential requirements for database design in healthcare: reliability, scalability, security, and

alignment with medical workflows. Special attention is given to data protection mechanisms, including access control, encryption, user activity logging, and defense against internal and external threats. The paper discusses architectural strategies for managing heterogeneous medical data and emphasizes the need for flexible integration with external systems and scalability over time. Role-based access models, backup strategies, and business continuity measures are described in detail. The article concludes that a well-designed database is not merely a storage system, but a foundational component of digital healthcare, directly impacting patient safety and quality of care.

Ключевые слова: медицинская информационная система, база данных, безопасность данных, шифрование, контроль доступа, ролевая модель, резервное копирование, масштабируемость, интеграция систем, цифровая медицина

Keywords: medical information system, database, data security, encryption, access control, role-based model, backup, scalability, system integration, digital healthcare

Разработка базы данных как основы медицинской информационной системы (МИС) представляет собой сложный и многоэтапный процесс, в котором критически важны как технологические, так и организационные аспекты. Современная медицина всё больше опирается на информационные технологии для повышения качества обслуживания пациентов, оптимизации рабочих процессов и обеспечения безопасности медицинских данных. Центральным элементом в структуре любой МИС является база данных, служащая хранилищем для всех видов информации: от персональных данных пациентов до истории болезни, результатов исследований и логистики медицинского учреждения.

Основной особенностью проектирования базы данных для МИС является необходимость обеспечить высокий уровень надежности, масштабируемости и безопасности. В отличие от многих других сфер, где потеря или утечка данных может повлечь в основном экономические убытки,

в медицине такие инциденты могут напрямую угрожать здоровью и жизни пациентов. Поэтому в процессе разработки закладываются строгие механизмы контроля доступа, шифрования и резервного копирования.

Прежде всего, особое внимание уделяется контролю доступа к данным. В медицинских системах принцип минимальных привилегий реализуется строго и последовательно: каждый пользователь системы должен иметь доступ только к тем данным и функциям, которые необходимы ему для выполнения своих обязанностей. Это достигается с помощью ролевой модели доступа, в рамках которой пользователи группируются по профессиональным ролям — врач, медсестра, лаборант, администратор и т.д., а каждому классу назначается определённый набор прав. Более того, поддерживается двухфакторная аутентификация и верификация через биометрические данные или смарт-карты, что существенно снижает риск несанкционированного доступа.

Для защиты данных от внешних атак база данных изолируется в закрытом контуре с ограниченным количеством точек входа. Серверы, на которых она размещена, защищаются с помощью современных межсетевых экранов (firewalls), систем обнаружения и предотвращения вторжений (IDS/IPS), а также механизмов сегментирования сети. Коммуникации между модулями системы, а также между клиентскими приложениями и сервером базы данных, шифруются по протоколам TLS/SSL, исключая возможность перехвата данных в процессе передачи.

Особое внимание уделяется шифрованию хранимых данных. В МИС применяется как симметричное, так и асимметричное шифрование, в зависимости от контекста. Персональные данные пациентов, результаты анализов, медицинская документация — всё это хранится в зашифрованном виде, а ключи шифрования управляются через защищённые хранилища (например, HSM — Hardware Security Module). Кроме того, предусмотрена технология маскировки данных (data masking), при которой на этапе просмотра или обработки вместо настоящих данных отображаются

псевдонимы или частично скрытая информация, особенно в случае доступа со стороны неполномочных лиц.

Существенным элементом обеспечения безопасности базы данных является аудит действий пользователей. Каждое действие в системе логируется и отслеживается: кто, когда и с какого устройства получил доступ к каким данным, производил ли изменения, экспортировал ли информацию и т.д. Это позволяет не только оперативно реагировать на инциденты, но и проводить ретроспективный анализ в случае утечки или ошибки. Логирование сопровождается системой оповещения и мониторинга, которая уведомляет администраторов о подозрительной активности в реальном времени.

Неотъемлемой частью стратегии безопасности является защита от внутренних угроз. Несмотря на распространённое мнение о внешних хакерах, статистика показывает, что значительная часть инцидентов связана с действиями сотрудников внутри организации — как умышленными, так и по неосторожности. В связи с этим важно реализовать политику "нулевого доверия" (zero trust), при которой каждый доступ требует повторной проверки, а любые попытки обхода регламентов автоматически блокируются. Дополнительно проводятся регулярные тренинги и тестирование персонала на знание принципов кибербезопасности.

Для защиты от потери данных при технических сбоях разрабатывается многоуровневая система резервного копирования. Создаются ежедневные, еженедельные и месячные бэкапы, хранящиеся в разных физических и облачных хранилищах. При этом каждый бэкап тестируется на возможность восстановления, что позволяет обеспечить непрерывность работы даже в случае сбоев серверного оборудования или действий вредоносного программного обеспечения, такого как ransomware.

Важным направлением является защита от атак с использованием уязвимостей приложений, взаимодействующих с базой данных. Использование механизмов защиты от SQL-инъекций, постоянное обновление программного обеспечения и проведение тестов на проникновение (penetration

testing) являются обязательными мерами. Современные платформы также используют технологии контейнеризации и виртуализации, что позволяет изолировать компоненты системы и минимизировать масштаб потенциального ущерба.

Проектирование структуры базы данных требует учета множества факторов. В МИС обычно обрабатываются разнотипные и разнородные данные: текстовые записи, изображения (например, снимки МРТ), числовые параметры лабораторных анализов, сигнальные данные от медицинского оборудования. Поэтому архитектура базы данных должна быть гибкой и адаптивной, поддерживающей как реляционные, так и нереляционные модели хранения информации. Современные системы часто используют гибридный подход, сочетая традиционные СУБД (например, PostgreSQL или Oracle) с документно-ориентированными или графовыми базами данных, чтобы эффективно управлять объемом и разнообразием данных.

При разработке базы данных также необходимо учитывать особенности рабочих процессов медицинских учреждений. Информация должна быть не только надежно сохранена, но и доступна в режиме реального времени различным категориям пользователей: врачам, медсестрам, администраторам, фармацевтам и другим специалистам. Это требует четкой ролевой модели доступа и продуманной логики взаимодействия между модулями системы. Например, врач должен иметь доступ к полной истории болезни пациента, включая лабораторные результаты и визуализации, в то время как регистратор видит лишь минимальные анкетные данные для записи на прием.

Важной задачей является обеспечение целостности и непротиворечивости данных. В условиях, когда пациент может обращаться в разные отделения или даже учреждения, система должна исключать дублирование и обеспечивать сквозную идентификацию. Это реализуется за счет введения уникальных идентификаторов, систем верификации и стандартных форматов ввода данных. Также важно, чтобы база данных поддерживала возможность отслеживания изменений — аудита действий

пользователей, что особенно актуально в случае медицинских споров или проведения клинических исследований.

Интеграция базы данных с внешними системами и сервисами является еще одной особенностью разработки. МИС должна взаимодействовать с лабораторными системами, электронными рецептами, страховыми компаниями, государственными регистрами и мобильными приложениями пациентов. Это требует реализации стандартов обмена данными, интерфейсов API и протоколов безопасности. Разработка такой интеграции должна предусматривать устойчивость к сбоям, синхронизацию и автоматическое разрешение конфликтов данных.

Неотъемлемым этапом разработки является тестирование и валидация базы данных. В медицинских системах ошибки могут иметь критические последствия, поэтому каждый элемент должен быть протестирован в условиях, приближенных к реальной эксплуатации. Это включает нагрузочное тестирование, моделирование аварийных ситуаций, проверку восстановления из резервных копий и многократную проверку логики обработки данных.
Особое внимание уделяется вопросам масштабирования. С течением времени объем данных в медицинской системе неизбежно растет, особенно если учреждение использует МИС в течение многих лет. База данных должна быть спроектирована с возможностью горизонтального и вертикального масштабирования, поддержкой архивирования устаревшей информации и оптимизации запросов.

Таким образом, разработка базы данных для медицинской информационной системы представляет собой ключевой этап в создании эффективной, безопасной и устойчивой цифровой среды в сфере здравоохранения. Это не просто техническая задача, а комплексное решение, в котором пересекаются интересы врачей, пациентов, администраторов и разработчиков. Грамотно спроектированная база данных становится основой, на которой строится всё остальное — от интерфейса пользователя до аналитических панелей и поддержки принятия клинических решений. Именно

поэтому к её разработке следует подходить с максимальной ответственностью и глубоким пониманием как IT-технологий, так и специфики медицинской практики.

Список литературы:

1. Назаренко Г.И., Гулиев Я.И., Ермаков Д.Е. Медицинские информационные системы: теория и практика. Под ред. Г.И. Назаренко, Г.С. Осипова. — М.: Физматлит, 2005. — 320 с.

2. Гулиев Я.И., Малых В.Л. Архитектура HL-X поддержки документов в медицинских информационных системах. — Информационно-управляющие системы, 2009, №2, с. 63–69.

3. Базаркин А.Н. Разработка темпоральной модели данных в медицинской информационной системе. — Программные продукты и системы, 2009, №2, с. 34–40.

4. Фохт О.А., Цветков А.А. Защита персональных данных: новое в законодательстве и вопросы практического применения в медицинских информационных системах. — Врач и информационные технологии, 2013, №5, с. 44–51.

5. Гулиев Я.И., Белышев Д.В. Исследование методов представления темпоральной медицинской информации посредством интерфейса «Боткинский лист». — Труды международной конференции «Программные системы: теория и приложения», ИПС РАН, Переславль-Залесский, 2006: В 2 т. / Под ред. С.М. Абрамова. — М.: Физматлит, Т.1, с. 73–92.