УДК 004

БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ В МЕДИЦИНСКИХ БАЗАХ: МАТЕМАТИЧЕСКИЕ МЕТОДЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

В.И. Брагинец, 2 курс
Научный руководитель – **Я.В. Богатко**, ассистент
Полесский государственный университет

В последние годы защита данных в здравоохранении стала крайне важной из-за увеличения зависимости медицинских учреждений от информационных технологий[1,с.45]. Цифровой формат хранения личных данных пациентов, результатов анализов и истории болезней делает их уязвимыми для киберугроз. Утечки информации могут вызывать финансовые потери и подрывать доверие пациентов к учреждениям[3,с.38]. Это требует разработки эффективных методов защиты данных, учитывающих специфику работы в данной области. Актуальность статьи заключается в необходимости анализа существующих способов защиты информации в медицинских базах данных, а также в оценке их эффективности для выбора оптимальных решений.

Безопасность данных в здравоохранении критически важна, поскольку утечки могут угрожать конфиденциальности пациентов и их здоровью [2,с.115]. Современные медицинские системы должны учитывать не только технические, но и психологические, организационные и правовые аспекты. Атаки на медицинские базы данных становятся всё более изощрёнными, что подчеркивает необходимость комплексного подхода к защите информации, включая математические методы и современные технологии [4, с. 87].

Существует множество подходов к защите данных в медицинских учреждениях, и среди них можно выделить несколько ключевых методов. Один из наиболее распространенных способов — это использование шифрования данных. Данный метод позволяет защитить информацию от несанкционированного доступа, так как даже в случае утечки данные остаются недоступными для чтения без необходимого ключа. Однако стоит отметить, что шифрование требует значительных вычислительных ресурсов и может замедлять работу системы, особенно в условиях большого объема данных [2, с. 118].

Другим важным аспектом является применение многоуровневой аутентификации, которая требует от пользователей проходить несколько этапов проверки личности [3, с. 42]. Это значительно увеличивает безопасность, так как даже в случае компрометации одного уровня защиты, доступ к данным остается заблокированным. В то же время, это может привести к увеличению времени доступа для сотрудников медицинских учреждений и снижению удобства использования системы [2, с. 120].

Также следует учесть внедрение современных систем мониторинга и анализа событий безопасности, которые позволяют в реальном времени отслеживать активности в сети и выявлять подозрительные действия. Однако такие решения требуют значительных затрат на оборудование и обучение персонала [2, с. 128].

Каждый из вышеупомянутых методов обладает своими преимуществами и недостатками. Шифрование данных обеспечивает высокий уровень защиты, но требует значительных ресурсов и может затруднять доступ в экстренных ситуациях. Многоуровневая аутентификация повышает безопасность, но порой прогресс может стоить времени и усложнять рабочие процессы. Системы мониторинга помогают выявлять и предотвращать кибератаки, но также нуждаются в постоянном обновлении и доработке, что влечет за собой дополнительные издержки.

Моделирование угроз является важным компонентом управления безопасностью данных. Для разработки эффективной модели угроз необходимо анализировать потенциальные уязвимости системы, идентифицировать возможные угрозы и оценить риски. Для этого можно использовать математические модели, например, метод анализа иерархий (AHP) для взвешивания рисков и моделирования вероятности атак. Этот подход позволит не только выявить наиболее уязвимые точки в системе, но и определить приоритеты в её защитных мерах.

Шифрование данных представляет собой одно из основных направлений в обеспечении информационной безопасности. Наиболее распространённые алгоритмы шифрования, такие как AES (Advanced Encryption Standard) и RSA (Rivest-Shamir-Adleman), обеспечивают высокий уровень защиты, но требуют значительных вычислительных ресурсов. Применение математических моделей для оценки эффективности алгоритмов шифрования позволяет оптимизировать их параметры. Например, можно использовать теорию информации для анализа энтропии шифротекстов и выявления потенциальных слабых мест в алгоритмах.

Совсем недавно в качестве перспективного направления стали рассматривать квантовые алгоритмы шифрования, которые могут значительно повысить безопасность передачи данных, используя принципы квантовой механик

Система контроля доступа (СКД) в медицинских учреждениях должна быть многоуровневой и учитывать различные аспекты безопасности. Использование математических моделей, таких как модели предельного состояния и стохастические модели, может быть полезно при разработке динамических систем контроля доступа, которые адаптируются под изменяющиеся угрозы и требования к защите данных [4, с. 93].

Одним из методов реализации СКД являются ролевые модели (RBAC), которые позволяют назначать права доступа на основе ролей пользователей. Однако современные угрозы требуют более гибких и адаптивных систем, учитывающих влияние контекста на уровень доступа. Внедрение контекстного контроля доступа (CBAC) вероятно будет полезным для обеспечения защиты данных в реальном времени, принимая во внимание условия окружающей среды.

Применение математических методов в сочетании с информационными технологиями даёт возможность создать более комплексные и надёжные системы защиты данных. Например, использование машинного обучения для анализа поведения пользователей может существенно повысить уровень защиты от внутренних угроз. Алгоритмы машинного обучения способны выявлять аномалии в действиях пользователей и автоматически инициировать защитные меры.

В рамках статьи важно рассмотреть не только отдельные методы защиты, но и комбинации подходов, что может значительно усилить уровень безопасности. Наиболее эффективной стратегией может стать интеграция нескольких методов, таких как шифрование и многоуровневая аутентификация, вместе с постоянно обновляемыми системами мониторинга и анализа. Такое комплексное решение обеспечит защиту на нескольких уровнях и позволит минимизировать риски утечки данных.

Таким образом обеспечение безопасности и защиты данных в медицинских базах является многогранной проблемой, требующей комплексного подхода и активного взаимодействия между математическими методами и современными информационными технологиями. Разработка моделей угроз, применение алгоритмов шифрования и создание многоуровневых систем контроля доступа – ключевые элементы, которые помогут повысить уровень защиты критической информации в здравоохранении. Данное направление будет продолжать развиваться, предлагая новые решения для защиты данных в условиях быстро меняющегося технологического ландшафта.

Список использованных источников

1. Петренко А.Ю., Сидорова М.В. Проблемы защиты информации в здравоохранении: современные подходы и решения // Журнал медицинской информатики и телемедицины. – 2021. – № 2. – С. 45–60.

2. Ковалев И.С. Влияние киберугроз на безопасность медицинских данных: аналитический обзор / И.С. Ковалев // Вопросы кибербезопасности. – 2022. – № 3. – С. 112–126.

3. Яковлева Н.А. Оценка применения технологий защиты информации в медицинских учреждениях // Проблемы ИТ в здравоохранении. – 2023. – № 1. – С. 35–50.

4. Усова А.Е., Дементьев В.А. Информационная безопасность в здравоохранении: проблемы и перспективы / А.Е. Усова, В.А. Дементьев // Вестник информационных технологий. – 2023. – Т. 15, № 4. – С. 85–97.