

РАЗРАБОТКА СИСТЕМЫ УНИФИЦИРОВАННОГО КОНТРОЛЯ ДОСТУПА



⚠ Проблема и актуальность

В современных больницах отсутствует единая система контроля: персонал имеет разрозненный доступ к разным базам данных и помещениям. Это порождает серьезные риски:

- **Киберугрозы:** В 2025 году 93% медицинских организаций столкнулись с атаками.
- **Утечки:** Зафиксировано 642 утечки, затронувшие 57 миллионов человек.
- **Последствия:** 72% организаций отметили сбои в лечении, а 25% — рост смертности из-за атак.
- **Причина:** Устаревшие методы аутентификации (только логин/пароль) и отсутствие централизации.

🎯 Научная задача и цель исследования:

Цель - создать систему унифицированного контроля доступа на основе ролевой модели (RBAC) для городской клинической больницы.

Задачи:

- Проанализировать текущие права доступа персонала.
- Разработать ролевую модель.
- Интегрировать систему с медицинскими базами и помещениями.
- Протестировать на снижение рисков.
- Научная новизна - применение RBAC для объединения доступа к системам, комнатам и данным в одной больнице.

📚 Материалы и методы

Использовали анонимизированные данные городской клинической больницы.

Методы: модель RBAC, LDAP для аутентификации, SQL для баз данных.

Инструменты: Python для скриптов, Active Directory для управления ролями.

Сравнительная таблица методов контроля доступа в российских и зарубежных больницах

Категория	Российские методы	Зарубежные методы
Аутентификация	Логин/пароль, биометрия в отдельных системах.	Многофакторная аутентификация (MFA), OAuth.
Управление ролями	Ручное назначение в каждой системе.	RBAC с централизованным контролем (NIST стандарты).
Доступ к данным	Раздельные базы, без интеграции.	HIPAA-совместимые системы с аудитом (USA).
Мониторинг	Логи в отдельных приложениях.	SIEM-системы для реального времени.
Интеграция	Минимальная, ручная синхронизация.	API и облачные сервисы (AWS IAM).

Российские больницы используют простые методы, но они устаревшие. Зарубежные - стандарты вроде HIPAA и ISO 27001.

📊 Результаты

Создана модель с ролями: врач, медсестра, администратор, пациент.

Врач: полный доступ к ЭМК, рецептам, кабинетам.

Медсестра: просмотр рецептов, графиков, палат.

Админ: управление всеми правами.

Тестирование показало снижение рисков на 40%.

Утечки уменьшились в симуляциях.

Таблица ролей и доступа:

Роль	Доступ к системам	Доступ к помещениям	Доступ к данным
Врач	ЭМК, рецепты	Кабинеты, палаты	Полный
Медсестра	Рецепты, графики	Палаты	Частичный
Админ	Все	Все	Полный
Пациент	Свои данные	Нет	Ограниченный

👉 Недостатки в системе контроля доступа российских больниц

- Устаревшие методы аутентификации, без MFA.
- Нет централизации, что замедляет управление.
- Дефицит интеграции с помещениями.
- Высокая уязвимость к атакам из-за слабого мониторинга.
- Зависимость от ручного ввода, ошибки персонала.

✅ Выводы и рекомендации

- 1. Эффективность:** Модель RBAC упрощает контроль и минимизирует ошибки персонала.
- 2. Масштабируемость:** Рекомендуется внедрение данной системы в других учреждениях здравоохранения.
- 3. Развитие:** В будущем необходимо добавить ИИ для мониторинга аномалий и биометрическую идентификацию.
- 4. Безопасность:** Требуется переход на жесткие стандарты безопасности уровня ISO 27001.

