Риск	Контрмера		План реализации контрмер			
			Действие	**Ответственный**	**Результат**	**Срок**
Раскрытие данных	**Превентивные барьеры**	Ролевая модель доступа	Создание ролевой модели	Сотрудник ИБ	Актуальная ролевая модель	Учесть при разработке системы
			Настройка доступа для всех ролей	Системный администратор	Доступы ограничены для всех ролей	
		Проверка кандидата СБ при найме	Включение в процесс найма этап проверки СБ	HR, СБ	К работе допускаются только сотрудники, прошедшие проверку	При трудоустройстве
		Журналирование	Ведение журнала действий пользователей и уведомление о несанкционированных действиях	Системный администратор	Своевременное реагирование на неправомерные действия	По событию
		Тестирование персонала на знание регламентов ИБ	Проведение тестирования персонала на знание регламентов ИБ	HR	Осведомленность персонала о правилах и рекомендациях к ИБ	При трудоустройстве, далее - 1 раз в год
		Организация обучения по ИБ	Проведение обучающих мероприятий по ИБ	HR	Своевременно обученные сотрудники	При трудоустройстве, далее - 1 раз в год
		Ограничение возможности копирования/выгрузки данных	Ограничения возможности выгрузки данных из системы	Сотрудник ИБ, Системный администратор	Пользователь не может выгрузить данные из системы с рабочего места	Учесть при разработке системы
			Ограничение подключения внешних носителей к АРМ	Системный администратор		
		Децентрализованное хранение данных	Реализация децентрализованного хранения данных	Системный администратор	Распределение данных между множеством узлов для уменьшения риска их полной уязвимости	Учесть при разработке системы
		Двухфакторная авторизация	Реализация функции двухфактороной авторизации в системе	Сотрудник ИБ	Снижение риска несанкционированного доступа	Учесть при разработке системы
		Шифрование данных	Реализация функции шифрования данных в системе	Сотрудник ИБ	Дополнительный уровень защиты для критически важных данных	Учесть при разработке системы
		Регулярное обновление паролей	Реализация функции периодического обновления паролей	Сотрудник ИБ	Снижение риска несанкционированного доступа	1 раз в 3 месяца - для внутренних пользователей 1 раз в год - для пациентов

Риск	Контрмера		План реализации контрмер			
			Действие	Ответственный	Результат	Срок
	Реактивные	Анализ инцидента	Провести анализ ситуации, выявить причины утечки и оценить уровень ущерба, действуя по разработанному регламенту	Сотрудник ИБ	Минимизация последствий утечки	По событию
		Блокировка учетной записи	Блокировка учетной записи, с которой произошла утечка	Системный администратор	Предотвращение дальнейшей утечки данных	По событию
		Изолировать часть системы	Изолировать затронутые системы от остальной инфраструктуры	Системный администратор	Предотвращение дальнейшей утечки данных	По событию
		Сброс всех паролей в системе	Инициировать сброс всех паролей в системе	Системный администратор	Предотвращение несанкционированного доступа к учётным записям пользователей	По событию
DoS, DDoS атаки	Превентивные	Мониторинг трафика	Использование систем мониторинга, которые отслеживают и анализируют сетевой трафик	Системный администратор Сотрудник ИБ	Своевременное обнаружение подозрительного трафика	На постоянной основе
		Фильтрация трафика	Использование систем фильтрации для блокировки подозрительных пакетов и источников трафика	Системный администратор Сотрудник ИБ	Своеременная блокировка подозрительного трафика	На постоянной основе
		Ограничение количества запросов	Настройка лимитов на количество запросов от одного IP-адреса	Системный администратор Сотрудник ИБ	Контроль количества запросов к серверу	На постоянной основе
		Использование DDoS-защиты от провайдеров	Использование услуг защиты от DDoS-атак, предоставляемых провайдерами	Системный администратор Сотрудник ИБ	Дополнительный уровень защиты от DDoS-атак	На постоянной основе
	Реактивные	Анализ инцидента	Провести анализ ситуации для выявления источника атаки, действуя по разработанному регламенту	Сотрудник ИБ	Минимизация последствий атаки	По событию
		Использование резервных серверов	Переключение на резервные серверы	Системный администратор Сотрудник ИБ	Сохранение доступности системы	По событию
		Ужесточение параметров ограничения трафика	Временное введение жестких лимитов на трафик	Системный администратор Сотрудник ИБ	Сохранение доступности системы	По событию