Проблема информационной безопасности	Описание актуальных решений
Недостаточная защита данных, передающихся от импланта к ЦОД по беспроводному каналу связи 1. **[К]** Перехват данных - злоумышленник может перехватить и прочитать данные, передаваемые между имплантом и внешними устройствами, ввиду слабого или отсутствующего шифрования трафика, или передаваемые данные в ходе обновления ПО. 2. **[К]** Атака MITM - возможность вмешательства в коммуникацию между устройствами ввиду слабой и/или отсутствующей аутентификации, что может привести к изменению команд или данных. 3. **[К]** Легко проходимая аутентификация - в случае внедрения злоумышленника в систему работы медицинского импланта необходимо, чтобы	1. Протоколы шифрования Внедрение современных протоколов шифрования, таких как TLS или DTLS, для защиты данных при передаче. Также предотвращает бóльшую часть сценариев атаки типа MITM 2. Алгоритмы шифрования Использование симметричных (AES) и/или ассиметричных (RSA) алгоритмов шифрования для защиты данных на уровне устройства. 3. Аутентификация a. Цифровые сертификаты - используются для проверки подлинности устройств и пользователей. Позволяют убедиться в том, что данные передаются только между доверенными сторонами. (описать подробнее) b. Многофакторная аутентификация - её использования для доступа

перед злоумышленником встали более сложные препятствия второго уровня защиты (первый уровень - базовая защита соединения с помощью шифрования, например) для получения доступа к импланту. Иначе доступ к импланту перейдет к злоумышленнику, что может являться угрозой для жизни пациента.	к функциям импланта помогает повысить уровень безопасности.
Уязвимости в программном обеспечении 1. **[Ц], [Д]** Ошибки в коде - могут привести к сбоям в работе устройства, его взлому или отказу в работе. **{Ж}** 2. **[**Может нарушаться любое свойство информации - в зависимости от неисправленных уязвимостей и того, как злоумышленник их эсплуатирует**]** Устаревшая версия ПО - может оставить импланты уязвимыми для широкого спектра уже известных атак.	1. Ошибки в коде a. Проведение регулярного аудита и тестирования программного обеспечения на наличие уязвимостей. b. Внедрение системы управления изменениями для контроля версий ПО. 2. Устаревшая версия ПО a. Регулярные (примерно раз в полгода) обновления программного обеспечения и прошивки устройств для устранения известных ранее уязвимостей, путем проводного

	b. Автоматизация процесса обновления, чтобы обеспечить своевременное внедрение патчей безопасности. Обновление возможно реализовать с минимальными рисками информационной безопасности в том случае, если медицинский имплант представляет модульную систему. Например, модуль управления данными может быть отделен от модуля управления функциями устройства. В таком случае можно обновить модуль управления данными, т.к. изменение функций устройства представляет из себя более масштабную задачу, чем регулярное обновление - необходимо создание нового ПО для работы устройства с новыми функциями.
[Ц], [Д] Физический доступ к	1. Ограничение доступа к

устройству - при его получении злоумышленник может изменить настройки или отключить устройство.	медицинским имплантам, используя специализированные помещения или места для хранения оборудования. Например, запираемый шкаф. 2. Разработка четких протоколов по обеспечению безопасности и защиты данных, касающихся работы с медицинскими имплантами. 3. Регулярные тренинги для обучения медицинского персонала по вопросам безопасности, чтобы сотрудники могли своевременно распознавать атаки физического доступа и вовремя применить заранее подготовленный экстренный протокол (пункт выше).