СТАНДАРТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕДИЦИНСКИХ ИМПЛАНТОВ

Стандарт информационной безопасности медицинских имплантов

Настоящий стандарт разработан с целью описания ключевых угроз информационной безопасности медицинских имплантов, их подробного анализа, а также формирования рекомендаций по защите на основе российских нормативных документов. Документ предназначен для производителей, поставщиков и специалистов в области кибербезопасности и здравоохранения.

1. Перехват данных при передаче

1. Краткое описание проблемы

Имплант передаёт чувствительные медицинские данные на внешние устройства через беспроводные каналы связи (Bluetooth, Wi-Fi). Эти данные могут быть перехвачены злоумышленниками.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Конфиденциальность, целостность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Sniffing-пакетов, Man-in-the-Middle-атаки, использование уязвимостей Bluetooth Classic и BLE.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Использование защищённых протоколов (TLS), шифрование данных на уровне транспорта и приложений, взаимная аутентификация устройств.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Обеспечить поддержку современных криптографических протоколов;

б) Правовые:

б) Документировать безопасность передачи данных согласно и GDPR.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

2. Несанкционированный удалённый доступ

1. Краткое описание проблемы

Устройства могут быть подвержены атаке через интернет или локальную сеть при отсутствии строгой аутентификации.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Конфиденциальность, доступность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Атаки с использованием паролей по умолчанию, уязвимостей API или отсутствия аутентификации.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Реализация многофакторной аутентификации, уникальных ключей, мониторинг доступа, журналирование действий.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Разработка системы авторизации и ведения логов;

б) Правовые:
б) Придерживаться требований к защите персональных данных и безопасности по 27001.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

3. Подмена управляющих команд

1. Краткое описание проблемы

Злоумышленник может отправить на устройство ложные команды, влияющие на его функционирование (например, изменение режима стимуляции кардиостимулятора).

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Целостность, безопасность пациента

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Replay-атаки, внедрение через вредоносные приложения на устройстве управления (телефоне, планшете).

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Применение цифровых подписей команд, контроль времени исполнения, межмодульная аутентификация.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Реализовать модуль верификации команд;

б) Правовые:
б) Выполнять ГОСТ Р 56939-2016 по защите информации в медицинских ИС.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

4. Уязвимость при обновлении прошивки

1. Краткое описание проблемы

При обновлении программного обеспечения может возникнуть риск установки модифицированной версии ПО с вредоносным кодом.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Целостность, конфиденциальность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Внедрение поддельной прошивки, отсутствие проверки подлинности, фальсификация процесса обновления.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Использование защищённого загрузчика, проверка цифровой подписи, механизмы отката к безопасной версии.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Использовать ГОСТ Р ИСО/МЭК 27001-2021 для обеспечения ИБ в ПО;

б) Правовые:
б) Включить обязательную проверку целостности кода при установке обновлений.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

5. Физический доступ к устройству

1. Краткое описание проблемы

Злоумышленник может получить доступ к устройству в случае прямого контакта (например, при замене внешнего контроллера).

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Доступность, конфиденциальность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Замена внешнего модуля управления на модифицированный, взлом через интерфейс обслуживания.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Аппаратное шифрование, блокировка интерфейсов при подозрительной активности, контроль доступа к сервисным портам.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Реализовать физические методы защиты по ГОСТ Р 50922-2006;

б) Правовые:
б) Инструктировать персонал и пациентов о рисках несанкционированного доступа.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

6. Недокументированные функции

1. Краткое описание проблемы

Программное обеспечение может содержать недекларированные функции (бэкдоры), которые могут использоваться злоумышленником.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Целостность, безопасность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Использование производственных отладочных функций, преднамеренные уязвимости в коде.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Ревизия кода, сертификация по ГОСТ Р ИСО/МЭК 15408, независимая экспертиза программных компонентов.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Обеспечить аудит ПО сторонними экспертами;

б) Правовые:
б) Исключить внедрение необоснованных скрытых функций согласно требованиям ФСТЭК

России.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

7. Компрометация облачного хранилища

1. Краткое описание проблемы

Данные с медицинского устройства могут синхронизироваться с облаком. При взломе сервиса возможна утечка информации.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Конфиденциальность, доступность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Взлом сервисов хранения, фишинг, слабая аутентификация.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Применение ГОСТ 28147-89 при шифровании, разграничение доступа, авторизация с использованием усиленной аутентификации.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Хранить персональные данные на территории РФ (в соответствии с 152-ФЗ);

б) Правовые:
б) Информировать пользователей об обработке и защите их данных в облаке.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

8. Атаки на батарею импланта

1. Краткое описание проблемы

Имплант может подвергаться атакам, которые ускоряют разрядку батареи, тем самым выводя устройство из строя.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Доступность, физическая безопасность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Создание непрерывных запросов, частое пробуждение устройства, провокация на активацию функций.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Ограничение частоты запросов, автономный режим энергосбережения, обнаружение аномального потребления.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Проектировать устройства в соответствии с ГОСТ Р 52350.0-2005 (электробезопасность);

б) Правовые:
б) Обеспечить пользовательский контроль за уровнем заряда и предупреждения при сбоях.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

9. Утечка данных через Bluetooth при сопряжении

1. Краткое описание проблемы

Во время первой настройки или переподключения импланта к устройству существует риск подключения злоумышленника.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Конфиденциальность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Использование слабых PIN-кодов, атака 'bluejacking' или 'bluesnarfing'.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Установка уникальных ключей сопряжения, ограничение времени активации Bluetooth-интерфейса, ГОСТ Р 56428-2015.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Проектировать механизмы сопряжения с учётом рекомендаций ФСТЭК;

б) Правовые:
б) Предоставлять техническую документацию по безопасному использованию.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

10. Атака через вредоносные мобильные приложения

1. Краткое описание проблемы

Имплант может быть управляем с телефона. Вредоносные приложения на устройстве пользователя могут вмешаться в управление.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Целостность, безопасность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Внедрение вредоносного кода в приложения для мониторинга, утечка ключей управления.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Изоляция ПО управления, проверка целостности приложения, подписи и сертификация через Минцифры РФ.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Разрабатывать мобильное ПО в соответствии с ГОСТ Р ИСО/МЭК 27034;

б) Правовые:
б) Контролировать обновления и публикацию приложения в сторах.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

11. Ошибка настройки безопасности по умолчанию

1. Краткое описание проблемы

Устройство может поставляться с небезопасными заводскими параметрами, которые не меняются при установке.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Конфиденциальность, целостность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Использование стандартных паролей, открытые сетевые порты, неотключённые диагностические интерфейсы.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Принцип Secure by Default, требование смены пароля при первом включении, отключение ненужных сервисов.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Внедрять политику безопасной конфигурации (ГОСТ Р 57580);

б) Правовые:
б) Обучать врачей и технический персонал настройке ИБ.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

12. Отказ от обновлений и устаревшее ПО

1. Краткое описание проблемы

Устройства, выпущенные несколько лет назад, могут не поддерживать современные методы защиты.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Целостность, доступность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Взлом через известные уязвимости, использование устаревших шифров.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Политика жизненного цикла ПО, поддержка обновлений не менее 5 лет, удалённая проверка актуальности защиты.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) ГОСТ Р ИСО/МЭК 30111 (управление уязвимостями);

б) Правовые:
б) Регистрация обновлений и сроков поддержки в технической документации.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

13. Несанкционированное клонирование внешнего устройства управления

1. Краткое описание проблемы

Мошенник может скопировать внешний контроллер (например, наручный пульт или приложение) и управлять имплантом.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Конфиденциальность, безопасность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Подделка сигнала, использование публично доступного ПО для копирования команд.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Биометрическая аутентификация, защита по MAC-адресу и серийному номеру устройства, генерация одноразовых ключей.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) ГОСТ Р 59717-2021 (методы аутентификации);

б) Правовые:

б) Включение инструкции о невозможности замены устройства без повторной инициализации.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

14. Атаки через беспроводные зарядные устройства

1. Краткое описание проблемы

Некоторые импланты имеют функцию беспроводной зарядки, которая может использоваться для внедрения команд.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Целостность, физическая безопасность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Модификация зарядного устройства, использование скрытого радиоканала.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Фильтрация команд, изоляция канала питания от командного интерфейса, сертификация зарядных модулей.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) Применять ГОСТ 60601-1 по электробезопасности;

б) Правовые:
б) Информировать пользователей о рисках использования неоригинальных зарядных устройств.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.

15. Манипулирование параметрами телеметрии

1. Краткое описание проблемы

Имплант может отправлять ложные данные в медицинскую систему, что приведёт к неправильным диагнозам.

Угроза может проявляться при эксплуатации устройства как в стационарных условиях, так и при использовании импланта пациентом в повседневной жизни. Потенциальные последствия включают вмешательство в работу медицинского устройства, что может повлиять на здоровье или даже жизнь пациента.

2. Нарушаемые свойства информации

Целостность, достоверность

Дополнительно: возможны правовые риски, связанные с нарушением законодательства РФ в области персональных данных и медицинской тайны.

3. Подробный сценарий эксплуатации угрозы

Вредоносное вмешательство в канал передачи телеметрии, ошибка калибровки или фальсификация значений.

Например, злоумышленник может использовать общедоступные инструменты для сканирования сети и перехвата передаваемой информации. Возможна реализация атак с использованием мобильных приложений и вредоносных устройств, находящихся в непосредственной близости от пациента.

4. Подробное описание методов защиты

Проверка данных на стороне врача, контроль времени передачи, цифровая подпись измерений.

Алгоритм защиты включает в себя следующие шаги:
- Определение всех точек доступа к устройству;
- Применение криптографических методов на уровне передачи и хранения данных (ГОСТ 28147-89, ГОСТ Р 34.10-2012);
- Внедрение контроля доступа по принципу наименьших привилегий;
- Реализация периодического мониторинга событий безопасности;
- Проведение регулярной ревизии уязвимостей устройства и обновления прошивки;
- Информирование пользователей о безопасном использовании и возможных рисках.

5. Обязанности производителя

а) Технические:
а) ГОСТ Р 52633.4-2006 (надежность измерений);

б) Правовые:
б) Обеспечить функции калибровки и журналирования изменений.

Производитель должен включить в документацию описание реализованных мер защиты и указать, какие ГОСТ и нормативные акты РФ были применены. Также необходимо организовать систему приёма сообщений об инцидентах информационной безопасности от пользователей и медицинского персонала.