Аннотация – В этом документе освещаются кибер-угрозы медицинским и коммуникационным технологиям и потенциальные риски и уязвимости в связанных протоколах. Документ разработан для того, чтобы помочь организациям здравоохранения и медицинским работникам понять важность обеспечения безопасности их технологических систем для защиты данных пациентов и обеспечения непрерывности оказания медицинской помощи.

I. Введение

Интеграция устройств Интернета вещей (IoT) в секторах здравоохранения и общественного здоровья привела к значительному прогрессу в уходе за пациентами. Однако эти преимущества сопряжены с рядом проблем и угроз кибербезопасности, которые необходимо устранить для защиты конфиденциальной медицинской информации и обеспечения непрерывности предоставления медицинских услуг. Ниже представлен обзор угроз кибербезопасности в этих секторах с уделением особого внимания таким устройствам, как кардиостимуляторы, интеллектуальные инфузионные насосы, аппараты магнитно-резонансной томографии, а также более широким последствиям для медицинских технологий и протоколов связи.

Безопасность цифровых технологий в здравоохранении и секторе общественного здравоохранения имеет первостепенное значение для обеспечения защиты пациентов, конфиденциальности и целостности медицинских услуг. Организации здравоохранения должны применять комплексный подход к обеспечению безопасности данных, сети и устройств, внедряя шифрование, защищённые протоколы связи и надёжные меры безопасности. Соблюдение правил HIPAA и соблюдение передовых практик и стандартов, например CISA, HHS и DICOM, необходимы для смягчения последствий кибер-угроз и обеспечения безопасного использования цифровых технологий в здравоохранении

II. Отрасли

Кибератаки на медицинские технологии могут затронуть широкий спектр отраслей, выходящих за рамки непосредственного сектора здравоохранения:

- **Поставщики медицинских услуг**: больницы, поликлиники и частные клиники полагаются на медицинские технологии при оказании помощи пациентам. Кибератаки могут сорвать операции, задержать лечение и поставить под угрозу безопасность пациентов.
- **Технологические компании в области здравоохранения**: фирмы, разрабатывающие и поддерживающие медицинское программное обеспечение и устройства, могут пострадать от кражи интеллектуальной собственности, потери доверия клиентов и финансов.
- **Страховые компании**: страховщики могут столкнуться с исками, связанными с кибератаками на медицинские технологии, включая расходы, связанные с утечкой данных, восстановлением системы и требованиями об ответственности.
- **Фармацевтика и биотехнологии**: эти отрасли полагаются на медицинские данные для проведения исследований и разработок. Кибератаки могут привести к потере запатентованных исследовательских данных и нарушить цепочку поставок важнейших лекарств.
- **ИТ-услуги здравоохранения**: компании, предоставляющие ИТ-поддержку и услуги организациям здравоохранения, могут быть косвенно затронуты кибератаками на своих клиентов, что приводит к репутационному ущербу и финансовым потерям.
- **Правительство и регулирующие органы**: государственным учреждениям здравоохранения и регулирующим органам, потребуется реагировать на кибератаки на медицинские технологии, влияющие на общественное здравоохранение и потенциально ведущие к изменениям в законодательстве.
- **Службы неотложной помощи**: кибератаки, нарушающие работу медицинских технологий, могут привести к задержкам в реагировании на чрезвычайные ситуации и переводе пациентов, что скажется на службах скорой и неотложной медицинской помощи.
- **Юридические услуги и комплаенс-услуги**: юридические фирмы и комплаенс-консультанты могут столкнуться с ростом спроса на услуги по мере того, как организации здравоохранения будут прорабатывать правовые последствия кибератак.
- **Фирмы по обеспечению кибербезопасности**: увеличение спроса на услуги кибербезопасности от организаций здравоохранения, стремящихся к защите от будущих инцидентов.
- **Пациенты и общественность**: пациенты могут столкнуться с нарушениями в обслуживании, неприкосновенности частной жизни и потерей доверия к системе здравоохранения.

III. Общие уязвимости и угрозы

Сектор здравоохранения всё больше полагается на цифровые технологии для управления информацией о пациентах, медицинских процедурах и коммуникациях. Эта цифровая трансформация, несмотря на свои преимущества, создаёт значительные риски для безопасности, включая утечку данных, несанкционированный доступ и кибератаки, которые могут поставить под угрозу безопасность пациентов, конфиденциальность и целостность медицинских услуг.

Распространённые кибер-угрозы медицинским технологиям и протоколам коммуникационных технологий включают нарушение работы, деградацию и уничтожение устройств, отравление данными, кражу личных и проприетарных данных, несанкционированный доступ к медицинскому программному обеспечению. Эти угрозы усугубляются расширением ИТ-среды в здравоохранении, использованием медицинских устройств с поддержкой искусственного интеллекта (ИИ) и машинного обучения (ML), а также растущей зависимостью от беспроводной связи, включая 5G.

Медицинские устройства, такие как кардиостимуляторы, интеллектуальные инфузионные насосы и аппараты магнитно-резонансной томографии, могут быть уязвимы к кибер-инцидентам из-за отсутствия протоколов шифрования данных, плохой сегментации сети и не устранённых уязвимостей. Кроме того, медицинскому программному обеспечению, такому как DICOM и PACS, может не хватать надлежащей проверки входных данных, так как они передаются открытым текстом. Также использование некачественные крипто-алгоритмы, что делает их уязвимыми для несанкционированного доступа и модификации данных.

A. Интеллектуальные инфузионные насосы

Эти устройства подключаются к внутренним сетям больницы через Wi-Fi или Ethernet и передают состояние, оповещения и аварийные сигналы на центральные станции мониторинга / управления, а также данные в электронные медицинские карты (EHR).

B. Аппараты МРТ

Аппараты МРТ могут быть подключены к внутренней сети больницы, а снимки могут кодироваться и отправляться в программное обеспечение для архивирования изображений и системы связи (PACS) через систему цифровой визуализации и коммуникаций в медицине (DICOM). Изображения PACS могут храниться локально и быть доступными в веб-сервисе EHR, потенциально предоставляя врачам несанкционированный доступ к сетевым устройствам, включая компьютеры.

C. Кардиостимуляторы

Кардиостимуляторы и другие электронные устройства, имплантируемые в сердце (CIED), эволюционировали и теперь включают беспроводное подключение для мониторинга и программирования. Такое подключение, хотя и полезно для ухода за пациентами, создаёт уязвимости. Кибератаки потенциально могут привести к неисправности устройства или несанкционированному доступу к данным пациента, что представляет значительный риск для здоровья

D. Устройства Интернета вещей

Многие устройства Интернета вещей в здравоохранении не имеют надёжных средств контроля безопасности, что делает их уязвимыми для несанкционированного доступа и утечки данных, например ввиду проблем с шифрованием данных, их передачей в открытом виде и небезопасным хранением паролей.

E. Сторонние поставщики

Устройства и программное обеспечение, предоставляемые сторонними поставщиками, могут вносить уязвимости в сети здравоохранения, предоставляя бэкдор для кибератак.

F. Медицинское программное обеспечение

В таких программах, как DICOM и PACS, может отсутствовать надлежащая проверка входных данных и использоваться небезопасные протоколы связи, что увеличивает риск несанкционированного доступа и манипулирования данными.

G. Радиочастотные помехи

Радиочастотные помехи могут нарушать связь между устройствами, приводя к потере или неправильной обработке данных, что может иметь прямые последствия для ухода за пациентами.

H. Подключение к сети 5G

Внедрение технологии 5G в здравоохранении создаёт новые уязвимости из-за расширения возможностей для атак и потенциальных рисков в цепочке поставок.

IV. Риски

Устранение рисков требует комплексного подхода к обеспечению безопасности данных, сети и устройств.

A. Безопасность данных

Безопасность данных в здравоохранении предполагает защиту конфиденциальной информации о пациентах от несанкционированного доступа, разглашения и кражи. Специальные законодательные решения, например HIPAA, устанавливает стандарт защиты данных пациентов, требующий шифрования электронной защищённой медицинской информации (ePHI), уникальной идентификации пользователя и журналов аудита для мониторинга доступа и использования PHI. Шифрование — это важнейшая технология защиты данных во время передачи, использования и хранения, гарантирующая, что данные не будут прочитаны посторонними лицами. Кроме того, принятие безопасных протоколов связи, таких как те, которые описаны DICOM, имеет важное значение для сохранения конфиденциальности и целостности информации о пациенте.

B. Сетевая безопасность

Сетевая безопасность в секторе здравоохранения предполагает защиту инфраструктуры, поддерживающей

передачу и хранение медицинских данных. Это включает в себя обеспечение безопасности беспроводных сетей, внедрение брандмауэров и использование виртуальных частных сетей (VPN) для шифрования передаваемых данных. Агентство по кибербезопасности и инфраструктурной безопасности (CISA) предоставляет ресурсы и передовой опыт для укрепления сетевой защиты и смягчения кибер-угроз. Организации здравоохранения также должны убедиться, что их меры сетевой безопасности соответствуют правилам HIPAA и другим соответствующим стандартам.

C. Безопасность устройства

Безопасность устройств направлена на защиту медицинских и мобильных устройств, используемых в медицинских учреждениях, от кибер-угроз. Это включает внедрение надёжных механизмов аутентификации, шифрование данных, хранящихся на устройствах, и регулярное обновление программного обеспечения для устранения уязвимостей в системе безопасности. Растущее использование устройств Интернета медицинских вещей (IoMT) создаёт дополнительные проблемы безопасности, требуя от организаций здравоохранения принятия комплексных мер для защиты этих устройств от взлома и несанкционированного доступа

V. Последствия атак

Последствия кибератаки на медицинские технологии могут быть серьёзными и широкомасштабными, затрагивая пациентов, организации здравоохранения и производителей медицинского оборудования.

- **Нарушение безопасности**: кибератаки на медицинские устройства могут привести к сбоям в работе, деградации или разрушению этих устройств, потенциально подвергая опасности здоровье и жизни пациентов.
- **Потеря конфиденциальных данных**: хакеры могут украсть или раскрыть конфиденциальные данные пациентов, включая личную информацию, записи о лечении и финансовые отчёты, что приведёт к нарушению конфиденциальности и потенциальной краже личных данных.
- **Финансовые и юридические штрафы**: организации здравоохранения могут столкнуться со значительными штрафами, юридическими последствиями и санкциями за неспособность обеспечить надлежащую защиту данных пациентов и соблюдение нормативных актов.
- **Ущерб репутации**: кибератаки могут подорвать доверие пациентов и нанести ущерб репутации организаций здравоохранения и производителей медицинского оборудования
- **Сбои в работе**: кибер-инциденты могут вызывать длительные сбои в ИТ или производстве, парализуя важнейшие службы здравоохранения и угрожая существованию пострадавших организаций.
- **Препятствие инновациям**: постоянная угроза кибератак может ограничить внедрение новых технологий и инноваций в секторе здравоохранения

A. Умные инфузионные насосы

Последствия кибератак на интеллектуальные инфузионные насосы могут быть серьёзными и потенциально опасными для жизни. Интеллектуальные инфузионные насосы — это подключённые к сети устройства, которые доставляют лекарства и жидкости пациентам. Согласно исследованию Palo Alto Networks 75% инфузионных насосов имеют недостатки в кибербезопасности, что подвергает их повышенному риску взлома хакерами

В свою очередь, это может привести к различным последствиям, в том числе:

- **Несанкционированный доступ**: хакеры могут получить несанкционированный доступ к инфузионным насосам, что потенциально позволяет им изменять способ подачи лекарств для внутривенного введения. Пациенты будут получать неправильные дозировки, которые могут быть вредными или даже смертельными.
- **Перехват незашифрованных сообщений**: некоторые инфузионные насосы передают незашифрованные сообщения, которые могут быть перехвачены хакерами, что приводит к раскрытию конфиденциальных данных пациента, таких как медицинские записи и личная информация.
- **Использование известных уязвимостей**: инфузионные насосы могут иметь известные бреши в системе безопасности, например имена пользователей и пароли остаются неизменными по сравнению с заводскими настройками устройства по умолчанию. Это может быть легко использовано хакерами, потенциально подвергая пациентов риску или раскрывая личные данные.
- **Нарушение работы служб**: нарушение работы медицинских служб приведёт к отключению программного обеспечения, потере доступа к медицинским записям и невозможности оказания надлежащей медицинской помощи. В крайних случаях медицинские учреждения могут быть вынуждены перенаправить пациентов в другие медицинские центры или отменить операции.

B. МРТ

Последствия кибератаки на аппараты МРТ многогранны и могут существенно повлиять на безопасность пациентов, целостность данных и операции здравоохранения.

- **Риски для безопасности пациентов**: кибератаки могут привести к манипуляциям с МРТ-изображениями, что потенциально может привести к неправильным диагнозам. Например, злоумышленники могут изменять изображения, чтобы удалить опухоль или ошибочно добавить её, что приведёт к ошибочному диагнозу и неправильному лечению с рисками летального исхода

- **Перебои в предоставлении медицинских услуг**: аппараты МРТ имеют решающее значение для диагностики и мониторинга различных состояний. Кибератака может вывести из строя эти машины, что приведёт к задержкам в диагностике и лечении. В критических ситуациях даже небольшие задержки могут иметь серьёзные последствия для здоровья пациента.
- **Атаки программ-вымогателей**: аппараты МРТ, как и другие медицинские устройства, уязвимы для атак программ-вымогателей. Такие атаки могут блокировать доступ к компьютерам или шифровать изображения, требуя выкуп за восстановление доступа. Это не только нарушает работу медицинских служб, но и подвергает риску данные пациентов.
- **Раскрытие конфиденциальных данных**: Аппараты МРТ подключены к больничным сетям, что делает их потенциальными точками входа для злоумышленников, которые используют их для доступа и кражи конфиденциальных данных пациентов, включая личную и медицинскую информацию, что имеет юридические и финансовые последствия для поставщиков медицинских услуг.
- **Операционные и финансовые последствия**: восстановление после кибератаки на аппараты МРТ может быть дорогостоящим и занимать много времени. Поставщикам медицинских услуг может потребоваться замена или ремонт скомпрометированных устройств, и они могут столкнуться с потенциальными юридическими штрафами и потерей доверия со стороны пациентов.
- **Проблемы с регулированием**: строгие правила затрудняют проведение базовых обновлений на медицинских ПК, подключённых к аппаратам МРТ, усложняя усилия по защите от кибератак. Медленный процесс разработки медицинских устройств визуализации также делает их уязвимыми перед растущими кибер-угрозами

C. Кардиостимуляторы

Последствия кибератаки на кардиостимуляторы могут быть серьёзными и потенциально опасными для жизни. Уязвимости кибербезопасности в кардиостимуляторах впервые были обнаружены хакерами в 2011 году, и с тех пор они находили различные бреши в системе безопасности. В 2017 году Управление по контролю за продуктами питания и лекарствами США (FDA) отозвало имплантируемый кардиостимулятор из-за опасений, что его могут взломать

Потенциальные последствия для кардиостимуляторов включают:

- **Прямая угроза жизни пациента**: злоумышленники потенциально могут завладеть устройством, изменив функции стимуляции или нанеся неподходящий удар электрическим током, что может привести к серьёзным осложнениям для здоровья или даже смерти.
- **Разрядка аккумулятора**: определённые типы атак, например, связанные с непрерывной отправкой команд на кардиостимулятор, могут привести к быстрому разряду аккумулятора, что потребует раннего хирургического вмешательства для замены устройства, что создало бы дополнительный риск для здоровья пациента.
- **Несанкционированный доступ к личным и медицинским данным**: кардиостимуляторы могут хранить и передавать данные, касающиеся здоровья пациента и работы устройства. Кибератаки ставят под угрозу конфиденциальность этих данных, что приведёт к потенциальному неправомерному использованию личной информации.
- **Потеря доверия к медицинским устройствам**: широко распространённые сведения об уязвимостях и успешных атаках могут подорвать доверие общественности к кардиостимуляторам и другим медицинским устройствам. Эта потеря уверенности может удержать пациентов от выбора потенциально спасающих жизнь методов лечения

D. Медицинские устройства Интернета вещей

Кибератаки на медицинские устройства Интернета вещей могут иметь серьёзные последствия для ухода за пациентами, включая человеческие жертвы. Основной целью для атакующих являются устройства Интернета вещей (IoT) и Интернета медицинских вещей (IoMT), которые, в свою очередь, были основной причиной 21% всех атак программ-вымогателей в сфере здравоохранения. В топ-10 прикроватных устройств, представляющих наибольший риск для безопасности, входят инфузионные насосы, устройства VoIP, ультразвуковые аппараты, мониторы пациентов и дозаторы лекарств.

- **Риски для безопасности пациентов**: прямые угрозы жизни пациентов из-за нарушения функциональности медицинских устройств Интернета вещей, таких как кардиостимуляторы, инсулиновые помпы и аппараты искусственной вентиляции лёгких. Например, злоумышленники могут изменить настройки или функциональность устройства, что приведёт к ненадлежащему обращению или выходу из строя.
- **Утечка данных**: медицинские устройства Интернета вещей часто собирают и передают конфиденциальные данные пациентов. Кибератаки могут привести к несанкционированному доступу к этим данным, что приведёт к нарушению конфиденциальности, краже личных данных и потенциальному неправильному использованию личной медицинской информации.
- **Сбои в работе**: злоумышленники могут нарушать работу медицинских учреждений, выводя из строя устройства, что приводит к задержкам в диагностике, лечении и оказании медицинской помощи. Это будет оказывать каскадное воздействие на поток пациентов и пропускную способность больницы.

- **Финансовые затраты**: последствия могут стать значительным финансовым бременем для организаций здравоохранения, включая расходы, связанные с заменой или ремонтом устройств, реагированием на утечку данных, увеличением страховых взносов и потенциальной юридической ответственностью.
- **Потеря доверия**: Пациенты могут не решаться использовать определённые медицинские устройства или делиться своими данными, опасаясь нарушения конфиденциальности и ставя под сомнение надёжность оказываемой им помощи.
- **Нормативно-правовые последствия**: организации здравоохранения могут столкнуться с административными штрафами за неспособность защитить данные пациентов и обеспечить безопасность медицинских устройств. Судебные иски также могут быть поданы пострадавшими пациентами или регулирующими органами.
- **Угрозы национальной безопасности**: в контексте обороны и военных операций скомпрометированные устройства Интернета вещей могут раскрывать конфиденциальную информацию, создавая риски для национальной безопасности.

E. Сторонние поставщики

Кибератаки на сторонних поставщиков в медицинском секторе могут иметь серьёзные последствия как для организаций здравоохранения, так и для пациентов, которых они обслуживают. Эти атаки представляют собой одну из самых серьёзных проблем в сфере кибер-рисков здравоохранения, поскольку больницы и системы здравоохранения подвергаются повышенному риску кибератак на третьи стороны, такие как деловые партнёры, поставщики медицинского оборудования и сторонние поставщики. Эти последствия включают:

- **Утечка данных**: сторонние поставщики часто имеют доступ к конфиденциальным данным, которые в случае взлома будут скомпрометированы, что приведёт к несанкционированному доступу к информации о пациенте.
- **Заражение вредоносными программами**: если система стороннего поставщика заражена вредоносным ПО, оно может распространиться на систему организации через этого него.
- **Атаки программ-вымогателей**: если у этих поставщиков отсутствуют надёжные меры безопасности и киберзащиты, они могут стать отправной точкой для атак программ-вымогателей.
- **Распределённые атаки типа "Отказ в обслуживании" (DDoS)**: организация может подвергаться DDoS-атакам через системы сторонних поставщиков.
- **Нарушения соответствия требованиям**: сторонние поставщики не всегда могут соблюдать те же правила, что и организации, с которыми они работают. Это может привести к нарушениям соответствия для организаций.
- **Ущерб репутации**: если сторонний поставщик будет взломан, это может нанести ущерб репутации организаций, с которыми он работает.
- **Влияние на медицинское оборудование**: кибератаки на сторонних поставщиков потенциально могут повлиять на медицинское оборудование, такое как аппараты компьютерной томографии и МРТ, которые обычно подключены к больничным сетям. Уязвимости в устаревшем программном обеспечении могут быть использованы атакующими, нарушающими работу цифровых записей пациентов и потенциально ставящими под угрозу здоровье пациентов

F. Медицинское программное обеспечение

Последствия атак на медицинское программное обеспечение выходят за рамки непосредственных финансовых потерь, создавая серьёзные риски для безопасности пациентов, целостности данных и общей эффективности оказания медицинской помощи, что подчёркивает важность приоритизации мер безопасности для защиты конфиденциальной медицинской информации и обеспечения непрерывности и качества медпомощи

- **Утечка данных**: может привести к несанкционированному доступу к конфиденциальным данным пациента, включая личную и финансовую информацию, медицинские записи и истории лечения. Это ставит под угрозу конфиденциальность пациентов и может привести к краже личных данных и финансовому мошенничеству.
- **Финансовые и юридические санкции**: организации здравоохранения могут столкнуться со значительными финансовыми потерями из-за штрафов и юридических санкций за неспособность должным образом защитить данные пациентов.
- **Проблемы с безопасностью пациентов**: могут нарушить работу медицинских служб и поставить под угрозу безопасность пациентов. Например, вмешательство в медицинские записи или диагностическое программное обеспечение может привести к неправильным диагнозам, неподходящему лечению или задержкам в оказании медицинской помощи.
- **Репутационный ущерб**: пациенты могут потерять уверенность в способности организации защитить их данные и обеспечить безопасное лечение, что нанесёт ущерб репутации организации и потенциально приведёт к потере бизнеса.
- **Снижение производительности**: может нарушить работу медицинских учреждений, что приведёт к задержкам процедур и анализов, более длительному пребыванию пациентов и общему снижению эффективности. Это приведёт к перегрузке ресурсов здравоохранения и скажется на уходе за пациентами.
- **Повышенные показатели смертности**: в некоторых случаях кибератаки были связаны с повышением показателей смертности пациентов.

Задержки в процедурах, тестах и оказании медицинской помощи из-за кибератак могут иметь серьёзные последствия.

- **Ограниченные инновации**: кибератаки могут затормозить инновации в секторе ввиду расходования средств на борьбу с возникающими проблемами вследствие этих атак

G. Медицинские радиочастотные помехи

Последствия радиочастотных помех в медицинской сфере могут быть серьёзными, поскольку они способны поставить под угрозу функциональность и безопасность медицинских устройств их использующих

- **Вмешательство в функциональность устройства**: может нарушить нормальную работу медицинских устройств, потенциально приводя к неправильным показаниям или неисправностям. Это имеет серьёзные последствия для ухода за пациентами, особенно в критических ситуациях, когда необходимы точные измерения и производительность устройства.
- **Утечка данных**: радиочастотные помехи потенциально могут быть использованы для получения несанкционированного доступа к конфиденциальным данным пациента, передаваемым по каналам связи. Это может привести к утечке данных, раскрытию личной и медицинской информации и поставить под угрозу конфиденциальность пациентов.
- **Вмешательство в работу устройства**: потенциально может манипулировать радиочастотными сигналами для отправки несанкционированных команд медицинским устройствам, таким как кардиостимуляторы или инсулиновые помпы, потенциально причиняя вред пациентам. Это может включать изменение настроек устройства, введение неправильных дозировок или даже полное отключение устройств.
- **Отказ в обслуживании**: возникает ситуации, когда устройства перестают отвечать на запросы, что нарушает уход за пациентами и формирует риск, в т.ч. в ситуации оказания немедленной медпомощи.
- **Потеря доверия:** успешные атаки на радиочастотные помехи могут подорвать доверие населения к медицинским устройствам и системе здравоохранения в целом, что потенциально приведёт к нежеланию пользоваться такими устройствами или обращаться за медпомощью.

H. Подключение к сети 5G

Последствия применения 5G в медицинской сфере существенны, учитывая решающую роль 5G в улучшении связи и передачи данных в системах здравоохранения:

- **Увеличенные площади атак**: расширение сетей 5G увеличивает количество потенциальных точек входа для кибер-атакующих, усложняя защиту сети от несанкционированного доступа и утечки данных.
- **Уязвимости в устройствах Интернета вещей**: медицинские устройства (с 5G подключением) являются частью Интернета медицинских вещей (IoMT). При возникновении ИБ-инцидентов приводят к компрометации данных пациента и функциональности устройства.
- **Риски протокола туннелирования GPRS**: использование протоколов туннелирования GPRS в сетях 5G может привести к появлению уязвимостей, потенциально позволяющих перехватывать передаваемые данные и манипулировать ими.
- **Устаревшие сетевые подключения**: сети 5G, подключённые к устаревшим системам, наследуют существующие уязвимости, что используется для получения доступа к конфиденциальным медицинским данным и системам.
- **Проблемы с пропускной способностью**: более высокая пропускная способность сетей 5G может ограничить текущие возможности мониторинга безопасности, затрудняя обнаружение угроз и реагирование на них в режиме реального времени.
- **Виртуализация сетевых функций**: зависимость от программного обеспечения и виртуализации в сетях 5G создаёт новые проблемы безопасности, поскольку каждый виртуальный компонент нуждается в мониторинге и защите для предотвращения потенциальных взломов.
- **Шифрование IMSI**: слабые места в шифровании IMSI могут привести к уязвимостям в конфиденциальности идентификационных данных абонентов, потенциально позволяя осуществлять атаки по принципу "один посередине" и несанкционированное отслеживание устройств.
- **Ботнеты и DDoS-атаки**: увеличившееся количество подключённых устройств в сети 5G может быть использовано злоумышленниками для создания ботнетов или запуска распределённых атак типа "отказ в обслуживании" (DDoS)
- **Нарушение работы важнейших служб здравоохранения**: кибератаки на сети 5G нарушают связь между медицинскими устройствами и поставщиками медуслуг, что приводит к задержкам в оказании неотложной помощи и потенциально поставит под угрозу жизни пациентов.
- **Последствия для регулирования и соблюдения требований**: организации здравоохранения могут столкнуться с контролем регулирующих органов и штрафными санкциями, если они не смогут защитить данные пациентов и обеспечить безопасность своих медицинских устройств и услуг с поддержкой 5G