ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56840— 2015/ IEC/TR 80001-2-3:2012

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 2-3

Руководство по беспроводным сетям

IEC/TR 80001-2-3:2012
Application of risk management for IT-networks incorporating medical devices — Part 2-3: Guidance for wireless networks
(IDT)

Издание официальное

Москва
Стандартинформ
2016

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Министерства здравоохранения Российской Федерации» (ЦНИИОИЗ Минздрава) и Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации «Фирма «ИНТЕРСТАНДАРТ» на основе собственного аутентичного перевода на русский язык международного документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздрава – постоянным представителем ISO ТС 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 28 декабря 2015 г. № 2228-ст

4 Настоящий стандарт идентичен международному документу IEC/TR 80001-2-3:2012 «Информатизация здоровья. Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 2-3. Руководство по беспроводным сетям» (IEC/TR 80001-2-3:2012 «Application of risk management for IT-networks incorporating medical devices — Part 2-3: Guidance for wireless networks»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (подраздел 3.5)

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0–2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

0.1 Предпосылка

Беспроводные коммуникации на протяжении десятилетий являлись ключевой технологией, обеспечивающей связь МЕДИЦИНСКИХ ПРИБОРОВ. Ранними примерами использования беспроводных технологий и МЕДИЦИНСКИХ ПРИБОРОВ являются амбулаторные системы кардиоконтроля в больницах и телеметрические системы, использующиеся через глобальные беспроводные сети. И хотя эти решения основывались на патентованных технологиях, появление готовых, основанных на стандартах, методов привело к растущему распространению беспроводных систем коммуникаций как внутри, так и вне помещений. Эти системы предоставляют и обеспечивают привлекательные и разнообразные варианты использования для целей соединения МЕДИЦИНСКИХ ПРИБОРОВ с информационными системами. Беспроводная технология обладает большими преимуществами, но, как и в любой технологии, при ее использовании возникают определенные РИСКИ, которые могут сказаться на трех ОСНОВНЫХ СВОЙСТВАХ: БЕЗОПАСНОСТИ, ЭФФЕКТИВНОСТИ и ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМ. В настоящем стандарте проведен обзор проблем, связанных с беспроводными технологиями, а также приведено руководство для обеспечения безопасного, эффективного и защищенного использования МЕДИЦИНСКИХ ПРИБОРОВ в беспроводной МЕДИЦИНСКОЙ ИТ-СЕТИ. Все это осуществляется в рамках общего подхода, согласованного с ПРОЦЕССОМ МЕНЕДЖМЕНТА РИСКА, как он определен в МЭК 80001–1.

Целевой аудиторией настоящего стандарта является ИТ отдел МО (медицинской организации), отделы биомедицинской и клинической инженерии, менеджеры по работе с рисками, а также люди, ответственные за проектирование и работу беспроводной ИТ сети.

В настоящем стандарте слово «следует» указывает на то, что среди нескольких возможностей соответствовать требованию, одна рекомендуется как наиболее подходящая, без упоминания других и не исключая другие. Оно также может указывать на то, что определенный план действий предпочтителен, но не является обязательным. Данное понятие не должно восприниматься как указание на требование.

0.2 Организация настоящего стандарта

Настоящий стандарт разделен на пять главных разделов, библиографию и два приложения. Раздел 4 содержит обзор беспроводной МЕДИЦИНСКОЙ ИТ СЕТИ и анализ различных типов беспроводных технологий, а также их применимость к здравоохранению. Следующие три раздела сосредоточены на высокоуровневых шагах, связанных с пониманием и определением сетевых технических характеристик, требований и связанных с ними мер по УПРАВЛЕНИЮ РИСКОМ в контексте создания МЕДИЦИНСКОЙ ИТ СЕТИ, а именно на:

а) планировании и проектировании;

б) внедрении и реализации; и

в) управлении работой.

Раздел 8 содержит общие меры по УПРАВЛЕНИЮ РИСКОМ, которые могут быть применимыми к уникальной МЕДИЦИНСКОЙ ИТ СЕТИ МО. И в завершение, в документе приведена библиография, содержащая перечень ссылочных документов для дальнейшего изучения. Приложение А содержит таблицу с вариантом сопоставления типов данных МЕДИЦИНСКОГО ПРИБОРА и связанных с ним сетевых приоритетов КАЧЕСТВА ОБСЛУЖИВАНИЯ Приложение В является анкетой контрольных вопросов для использования при выполнения АНАЛИЗА РИСКА.

0.3 Клиническая функциональность и вариант использования

Одной из фундаментальных концепций, на которой делается акцент в настоящем стандарте, является наличие сетевых характеристик МЕДИЦИНСКИХ ПРИБОРОВ, которые схожи с характеристиками других типов приборов и приложений общего назначения. Но в то же время, последствия неправильного проектирования и управления сетью для обеспечения выполнения СОГЛАШЕНИЯ об УРОВНЕ УСЛУГ (SLA) МЕДИЦИНСКИХ ПРИБОРОВ могут негативно сказаться на клинической функциональности. Это может повлечь за собой ошибочные диагнозы и/или пропущенное лечение, которое, в конечном счете, может сказаться на результате лечения пациента. В настоящем стандарте клиническая функциональность и клинический вариант использования являются взаимозаменяемыми. Эти понятия подразумевают средства, с помощью которых практикующий врач (медсестра, терапевт и т. д.) выполняют свои врачебные обязанности, используя беспроводную сеть, а также включают в себя компонент

ухода за пациентом и БЕЗОПАСНОСТЬ. Эти компоненты, как они представлены в совокупном контексте, который упоминается в пошаговом техническом отчете МЭК 80001-2-1, и данная информация необходимы для полного АНАЛИЗА РИСКА. Типичным примером служит медсестра, занимающаяся удаленным контролем пациента, осуществляющимся из центрального поста медицинской сестры посредством прибора контроля пациента, установленного у его постели и соединенного с беспроводной сетью. Клиническая функциональность это удаленный контроль здоровья пациента.

0.4 Руководство по беспроводным технологиям и МЕНЕДЖМЕНТ РИСКА

Беспроводной канал, установленный между пациентом и удаленным практикующим врачом, теперь является компонентом клинической функциональности и может влиять на ОСНОВНЫЕ СВОЙСТВА: БЕЗОПАСНОСТЬ и ЗАЩИЩЕННОСТЬ ДАННЫХ И СИСТЕМ. В то время как преимущества беспроводного доступа хорошо известны и представлены документально, как правило, беспроводной канал между МЕДИЦИНСКИМ ПРИБОРОМ и практикующим врачом более склонен, или обладает более высокой вероятностью потери связи, чем соединение посредством проводов. Эта проблема послужила толчком к созданию настоящего стандарта и является его главной темой.

Так как определения ОПАСНОСТИ, ОПАСНОЙ СИТУАЦИИ, ВРЕДА и причин зависит от варианта использования в каждой МО, настоящий стандарт следует использовать, как минимум, вместе с МЭК 80001–1 и МЭК/ТО 80001-2-1.

На рисунке 1 представлен обзор МЕНЕДЖМЕНТА РИСКА, который также рассмотрен в настоящем стандарте. Столбец прямоугольников, расположенный слева, представляет из себя обзор (для цели настоящего стандарта) 10 шагов МЕНЕДЖМЕНТА РИСКА, определенных в МЭК/ТО 80001-2-1. Прямоугольники, расположенные в центре, демонстрируют шаги ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА, которые находятся в центре внимания настоящего стандарта. В терминах ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА это следующие шаги:

- причина является событием, способным превратить ОПАСНОСТЬ в ОПАСНУЮ СИТУАЦИЮ. Примерами таких причин в беспроводных сетях могут быть радиопомехи, неправильная конфигурация беспроводной сети или отказ сетевого устройства;

- ОПАСНОСТЬЮ в контексте беспроводной связности является потеря или ухудшение связи в медицинской системе. Это нарушение связи может негативно сказаться на способности МЕДИЦИНСКОГО ПРИБОРА или клинической системы выполнять предназначенную ей функцию;

- ОПАСНАЯ СИТУАЦИЯ это обстоятельство, в котором МЕДИЦИНСКИЙ ПРИБОР или клиническая функциональность подвержены ОПАСНОСТИ. Например, практикующий врач ведет контроль пациента из поста медицинской сестры (клиническая функциональность в данном случае это удаленный контроль). Если по причине радиопомех беспроводная сеть отключается (ОПАСНОСТЬЮ в таком случае является потеря связи), то удаленный контроль пациента прекращается (ОПАСНАЯ СИТУАЦИЯ).

- Меры УПРАВЛЕНИЯ РИСКОМ в контексте настоящего стандарта представляют из себя шаги, которые выполняются для уменьшения вероятности возникновения ОПАСНОЙ СИТУАЦИИ (данная вероятность обозначается как P1 в МЭК/ТО 80001-2-1), или же шаги, которые выполняются для уменьшения вероятности причинения ВРЕДА после возникновения ОПАСНОЙ СИТУАЦИИ (P2 в МЭК/ТО 80001-2-1). Примером меры УПРАВЛЕНИЯ РИСКОМ для P1 может быть RF резервирование или процедуры управления изменениями в сети. Примером меры УПРАВЛЕНИЯ РИСКОМ для P2 может быть последовательность действий, которые предпримет медсестра при получении уведомления о потери связи между прибором контроля пациента и центральной станцией.

Большая часть настоящего стандарта посвящена проектированию и мерам по УПРАВЛЕНИЮ РИСКОМ, связанным с беспроводными технологиями. Тем не менее, и это является еще одним поводом для взаимодействия с практикующими врачами на ранних стадиях планирования, роль практикующих врачей в ослаблении нанесения ВРЕДА пациенту, должна быть внимательно рассмотрена. В представленном выше примере, использующем выделенные шаги, практикующий врач, в случае выхода сети из строя, может следовать документально установленной процедуре. Когда в сети происходит потеря связи, практикующий врач может следовать процедуре, в ходе которой ему необходимо работать непосредственно с пациентом.

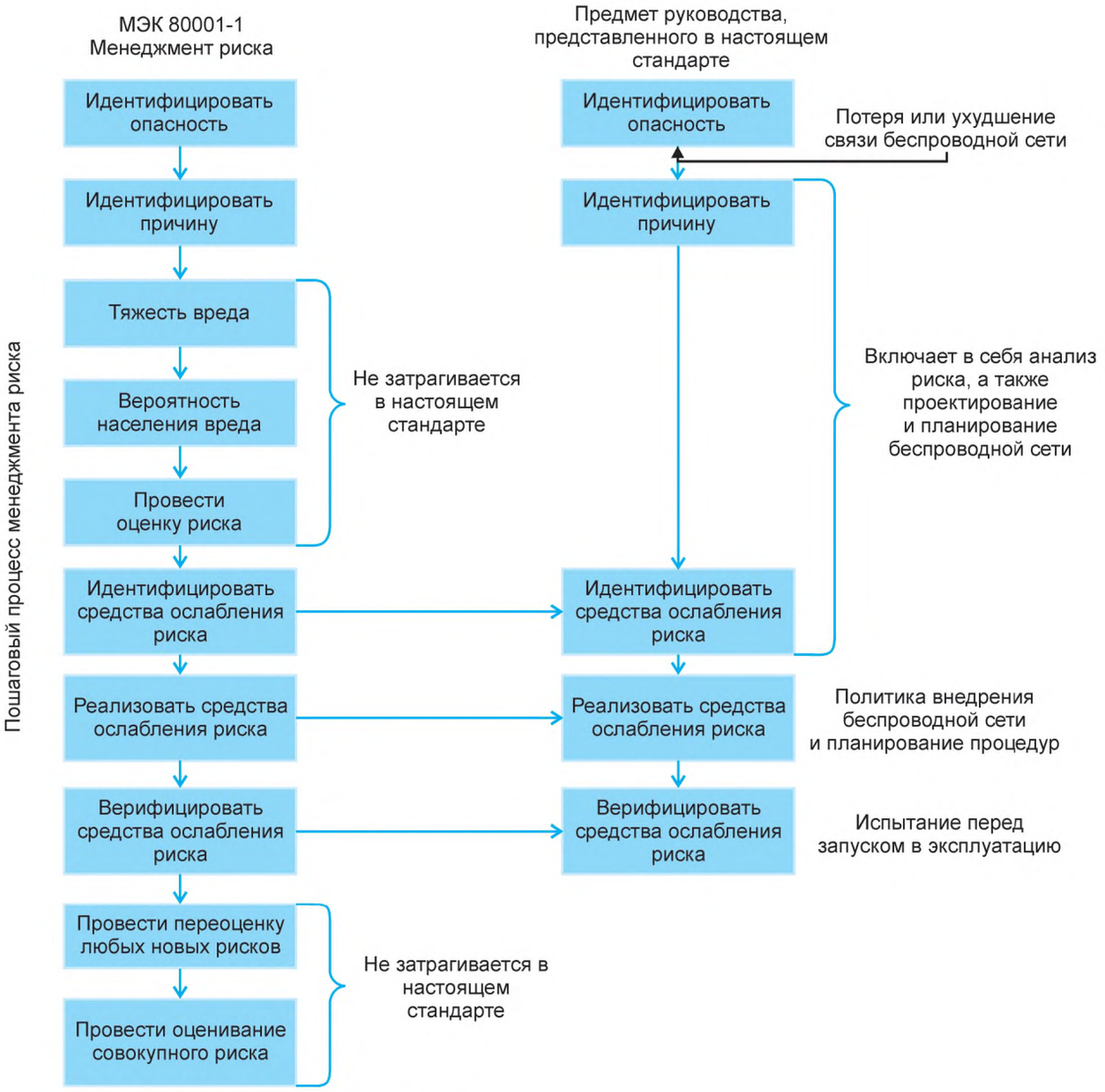

Рисунок 1 – Предмет настоящего стандарта

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 2-3

Руководство по беспроводным сетям

Health informatics. Risk management for IT-networks incorporating medical devices.
Part 2-3. Guidance for wireless networks

Дата введения — 2016—11—01

1 Область применения и цель

1.1 Область применения

Настоящий стандарт предназначен для поддержки медицинской организации (МО) в выполнении МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ ИТ СЕТИ, в которую входит один или несколько беспроводных каналов. В настоящем стандарте представлена техническая справочная информация, связанная с беспроводной технологией, а также примеры ОПАСНОСТЕЙ, которые следует учитывать при использовании беспроводной технологии в МЕДИЦИНСКИХ ИТ СЕТЯХ и предложены меры по УПРАВЛЕНИЮ РИСКОМ для снижения вероятности НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ.

1.2 Цель

Настоящий стандарт, будучи частью МЭК 80001, рассматривает использование МЕДИЦИНСКИХ ПРИБОРОВ, взаимодействующих в МЕДИЦИНСКОЙ ИТ СЕТИ посредством беспроводной технологии, а также предлагает практические методики подхода к уникальным требованиям МЕНЕДЖМЕНТА РИСКА, связанным с безопасной, защищенной и эффективной работой с МЕДИЦИНСКИМИ ПРИБОРАМИ, использующими беспроводную технологию.

Предметом настоящего стандарта являются беспроводные технологии, рассматриваемые с агностической точки зрения. Тем не менее, существуют определенные беспроводные технологии, преобладающие в МО (например, 802.11), которые рассматриваются в настоящем стандарте более подробно. При необходимости, эти различия между беспроводными технологиями отмечаются и оговариваются. Хотя настоящий стандарт не уделяет все внимание одной конкретной беспроводной технологии, но принято считать, что она связана с сетью с проводной инфраструктурой, и такой сетью является, основанная на Ethernet, IP сеть.

Целью настоящего стандарта не является предложение о регламентированном пошаговом ПРОЦЕССЕ для реализации беспроводной МЕДИЦИНСКОЙ ИТ СЕТИ или ослаблении РИСКА, связанного с определенной беспроводной технологией. Существует множество причин не выдвигать подобные предложения, и основными среди них являются следующие:

- Доступно множество различных беспроводных технологий, каждая из которых обладает своими физическими характеристиками (PHY), характеристиками управления доступом к среде (MAC) и характеристиками верхнего уровня с изменяющимися степенями управления, доступного для МО.
- Разработка многих беспроводных технологий находится на стадии совершенствования и потому такие технологии по-прежнему подвержены постоянным и значительным изменениям.
- Медицинские организации (МО), в зависимости от своих нужд, могут осваивать различные комбинации беспроводных технологий для обеспечения соответствия своим определенным требованиям. Для каждой технологии потребуется свой независимый АНАЛИЗ РИСКА и свои меры по УПРАВЛЕНИЮ РИСКОМ, ревизия которых должна осуществляться систематически (общий АНАЛИЗ РИСКОВ).

Издание официальное

- У каждой МО свой вариант клинического использования и своя топология сети, и каждая МО будет осуществлять свой уникальный АНАЛИЗ РИСКА и менеджмент, которые будут отличаться от других МО.

Вместо этого, настоящий стандарт признает обобщенный или высокоуровневый подход к пошаговому рассмотрению ПРОЦЕССА, который как по своей природе, так и специально рассматривает ОПАСНОСТИ, причины, влекущие за собой ОПАСНЫЕ СИТУАЦИИ, и меры по УПРАВЛЕНИЮ РИСКОМ. Общий подход, которому следует настоящий стандарт, осуществляется следующим образом:

a) ставится вопрос: требуется ли беспроводное подключение для данного варианта использования прибора? Это не тривиальный вопрос, но в настоящем стандарте предполагается считать, что ответ — «Да»;

b) определяются варианты клинического использования/функциональность, используя собрание практикующих врачей, персонала биомедицинской инженерии и кого-либо еще, кто может быть вовлечен в использование и поддержку МЕДИЦИНСКИХ ПРИБОРОВ;

c) выполняется анализ беспроводных спецификаций и функциональных возможностей МЕДИЦИНСКОГО ПРИБОРА(ОВ) и систем, и определяются базовые требования к производительности сети;

d) формируются клиническое SLA (СОГЛАШЕНИЕ об УРОВНЕ УСЛУГ) отобразив характеристики производительности сети на клиническую функциональность. См. таблицу А.1 в качестве примера подобного отображения;

e) требования МЕДИЦИНСКИХ ПРИБОРОВ и систем к производительности сети приводятся в соответствие с существующими функциональными возможностями ИТ СЕТИ общего назначения, и выявляются пробелы и несовместимости. Необходимо учесть конфигурации беспроводных сетей и требования к производительности сети всех существующих или запланированных беспроводных не-МЕДИЦИНСКИХ ПРИБОРОВ;

f) ПРОЦЕСС МЕНЕДЖМЕНТА РИСКА завершается идентификацией и реализацией мер УПРАВЛЕНИЯ РИСКОМ относящихся к ОСНОВНЫМ СВОЙСТВАМ. Многие из мер УПРАВЛЕНИЯ РИСКОМ очень похожи на «передовые методы проектирования», но документально оформляются, применяются и проходят ВЕРИФИКАЦИЮ, как часть ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА;

g) проектируется и конфигурируется сеть(и) для соответствия СОГЛАШЕНИЯМ об УРОВНЕ УСЛУГ (SLA) всех приборов (медицинских и немедицинских);

h) проводится испытание сети перед запуском в эксплуатацию для ВЕРИФИКАЦИИ того, что все приборы сосуществуют должным образом и в то же время поддерживают свое определенное SLA;

i) используются оперативные меры для контроля и управления действующей сетью с поддержанием постоянного соответствия SLA.

1.3 Масштабируемость МО

Область применения настоящего стандарта включает все МО независимо от размера сети. Большие сети могут сталкиваться с большим количеством приборов и сложными комбинациями приложений, использующими как проводные, так и беспроводные сети. В этих сетях могут как присутствовать, так и отсутствовать критически важные данные пациентов. Другие сети могут быть меньше по размеру, проще по количеству приборов и приложений, работающих в сети, но могут при этом содержать жизненно важные данные. Сложность сетей и аспект сетевого трафика, связанный с БЕЗОПАСНОСТЬЮ пациента, определяют масштаб требующихся анализа ОПАСНОСТЕЙ и МЕНЕДЖМЕНТА РИСКА. Аспект БЕЗОПАСНОСТИ пациента требует, чтобы план МЕНЕДЖМЕНТА РИСКА был завершен до того момента, пока еще сложность сети преобразуется в определенный уровень сложности мер по УПРАВЛЕНИЮ РИСКОМ.

Безусловно, можно поспорить с тем, что малая сеть (например, сеть кабинета терапевта), использующая беспроводную технологию, не нуждается в том же уровне АНАЛИЗА РИСКА, что и сеть всей больницы. Например, существуют небольшие катетеризационные лаборатории и небольшие методы косметической хирургии, сети которых могут быть небольшого размера, но при этом нести в себе данные пациентов. Все МО должны осуществлять управление защитой своих сетей и проводить оценку их клинической функциональности для профилактики возможных последствий, связанных с БЕЗОПАСНОСТЬЮ ПАЦИЕНТОВ. МО необходимо управлять применением беспроводных сетевых технологий, уделяя надлежащее и соответствующее масштабу внимание МЕНЕДЖМЕНТУ РИСКА.

И хотя предметом настоящего стандарта являются проблемы применения для сложных применений беспроводных сетей, руководящие указания, содержащееся в нем, могут применяться в множестве различных сетевых окружений, больших и малых.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты и документы. Для датированных ссылок следует использовать указанное издание. Для недатированных ссылок — последнее издание указанного документа, включая все поправки к нему.

МЭК 80001-1:2010, Применение менеджмента риска для ИТ СЕТЕЙ с медицинскими приборами. Часть 1: Роли, ответственности и действия (IEC 80001-1:2010, Application of risk management for IT–networks incorporating medical devices — Part 1: Roles, responsibilities and activities)

3 Термины и определения

В настоящем стандарте используются следующие термины и определения.

3.1 **ТОЧКА ДОСТУПА** (ACCESS POINT, AP): Мост между беспроводной и проводной средой.

3.2 **СОПРОВОДИТЕЛЬНЫЙ ДОКУМЕНТ** (ACCOMPANYING DOCUMENT): Документ, сопровождающий МЕДИЦИНСКИЙ ПРИБОР или вспомогательное оборудование и содержащий информацию, предназначенную для ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ или ОПЕРАТОРА, в частности, касающуюся БЕЗОПАСНОСТИ.

[МЭК 80001-1:2010, статья 2.1]

3.3 **УСОВЕРШЕНСТВОВАННЫЙ СТАНДАРТ ШИФРОВАНИЯ** (ADVANCED ENCRYPTION STANDARD, AES): Стандарт шифрования с помощью симметричного ключа.

Примечание — Один из способов использования настоящего стандарта предназначен для стандарта беспроводного шифрования WPA2.

3.4 **ИДЕНТИФИКАТОР ОСНОВНЫХ НАБОРОВ СЛУЖБ** (BASIC SERVICE SET IDENTIFIER, BSSID): Термин стандартов 802.11 для MAC-адреса ТОЧКИ ДОСТУПА (AP).

3.5 **ПРОТОКОЛ BOOTSTRAP** (BOOTSTRAP PROTOCOL, BOOTP): Сетевой протокол, который использует клиент сети для получения IP адреса от сервера конфигурации.

3.6 **ШИРОКОВЕЩАТЕЛЬНАЯ АДРЕСАЦИЯ** (BROADCAST ADDRESSING): Технология одновременной отправки сообщений всем абонентам сети.

3.7 **РАЗРЕШЕНИЕ на ИЗМЕНЕНИЕ** (CHANGE PERMIT): Результат ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ, представленный в виде документа, позволяющего реализовать сформированное изменение или тип изменения без дополнительных действий по МЕНЕДЖМЕНТУ РИСКОВ в рамках установленных ограничений.

[МЭК 80001-1:2010, статья 2.3]

3.8 **УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ** (CHANGE-RELEASE MANAGEMENT): Процесс, гарантирующий, что все изменения в ИТ СЕТИ оценены, приняты, выполнены и проанализированы контролируемым способом, а также, что изменения проведены, распространены и отслежены, что приводит к смене версии контролируемым способом с соответствующими входными и выходными данными для УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ.

[МЭК 80001-1:2010, статья 2.2]

3.9 **УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ** (CONFIGURATION MANAGEMENT): ПРОЦЕСС, гарантирующий, что информация о конфигурации компонентов и ИТ СЕТИ определена и поддерживается с надлежащей точностью и контролем, а также обеспечивает механизм для идентификации, управления и отслеживания версий ИТ СЕТИ.

[ИСТОЧНИК: МЭК 80001-1:2010, статья 2.4]

3.10 **ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ** (DATA AND SYSTEM SECUIRTY): Рабочее состояние МЕДИЦИНСКОЙ ИТ СЕТИ, в котором информационные ресурсы (данные и системы) обоснованно защищены от нарушения конфиденциальности, полноты и доступа.

[МЭК 80001-1:2010, статья 2.5 Определение является модифицированным. Два примечания из оригинального документа, неотъемлемые для понимания области применения определения, были удалены.]

3.11 **ЦИФРОВАЯ УСОВЕРШЕНСТВОВАННАЯ БЕСПРОВОДНАЯ СВЯЗЬ** (DIGITAL ENHANCED CORDLESS TELECOMMUNICATIONS, DECT): Стандарт цифровых коммуникаций, основным назначением которого является использование в создании беспроводных телефонных систем.

3.12 **РАСПРЕДЕЛЕННАЯ АНТЕННАЯ СИСТЕМА** (DISTRIBUTED ANTENNA SYSTEM, DAS): Антенная система, которая собирает сигналы и направляет их в централизованные месторасположения.

3.13 **ДИНАМИЧЕСКИЙ ВЫБОР ЧАСТОТЫ** (DYNAMIC FREQUENCY SELECTION, DFS): Механизм динамического выбора частот для обхода источников помех. Обычно используется совместно с системами, основанными на механизме 802.11a, использующимися для защиты от частот радиолокационных систем.

3.14 **ПРОТОКОЛ ДИНАМИЧЕСКОЙ КОНФИГУРАЦИИ СЕТЕВОГО УЗЛА** (DYNAMIC HOST CONFIGURATION PROTOCOL, DHCP): Метод присвоения IP адресов устройствам-клиентам по запросу клиента.

3.15 **ЭФФЕКТИВНОСТЬ** (EFFECTIVENESS): Способность достигать намеченных результатов по отношению к пациенту и ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ.

[МЭК 80001-1:2010, статья 2.6]

3.16 **ЭЛЕКТРОННАЯ МЕДИЦИНСКАЯ КАРТА** (ELECTRONIC MEDICAL RECORD, EMR): Компьютеризированная медицинская карта, создаваемая медицинской организацией (МО).

3.17 **СХЕМА КОДИРОВАНИЯ/ДЕКОДИРОВАНИЯ** (ENCODER/DECODER, CODEC): Модуль, способный кодировать и декодировать данные.

3.18 **УПРАВЛЕНИЕ СОБЫТИЕМ** (EVENT MANAGEMENT): ПРОЦЕСС, который гарантирует, что все события, негативно влияющие, или способные негативно повлиять на работу ИТ СЕТИ фиксируются, оцениваются и обрабатываются контролируемым способом.

[МЭК 80001-1:2010, статья 2.7]

3.19 **РАСШИРЕННЫЙ НАБОР СЛУЖБ ИДЕНТИФИКАЦИИ** (EXTENDED SERVICE SET IDENTIFIER, ESSID): Понятие, описывающее логическое группирование множества наборов BSSID.

Примечание — Данный термин часто заменяет SSID.

3.20 **РАСШИРЯЕМЫЙ ПРОТОКОЛ АУТЕНТИФИКАЦИИ** (EXTENSIBLE AUTHENTICATION PROTOCOL, EAP): Основа для аутентификации, часто использующаяся в беспроводных сетях и двухточечных соединениях.

Примечание — Данный термин определен в RFC 3748 и обновлен в RFC 5247.

3.21 **РАСШИРЯЕМЫЙ ПРОТОКОЛ АУТЕНТИФИКАЦИИ ЗАЩИТЫ ТРАНСПОРТНОГО УРОВНЯ** (EXTENSIBLE AUTHENTICATION PROTOCOL — TRANSPORT LAYER SECURITY, EAP-TLS): Специальный метод аутентификации, использующий метод аутентификации EAP (RFC 5216).

3.22 **ЗАПУСК В ЭКСПЛУАТАЦИЮ** (GO-LIVE): Момент, когда система переходит из стадии установки в стадии активного использования.

3.23 **ВРЕД** (HARM): Физическая травма или ущерб здоровью людей, или имуществу, или окружающей среде, а также снижение ЭФФЕКТИВНОСТИ или нарушение ЗАЩИЩЕННОСТИ СИСТЕМЫ И ДАННЫХ.

[МЭК 80001-1:2010, статья 2.8]

3.24 **ОПАСНОСТЬ** (HAZARD): Потенциальный источник ВРЕДА.

[МЭК 80001-1:2010, статья 2.9]

3.25 **ОПАСНАЯ СИТУАЦИЯ** (HAZARDOUS SITUATION): Обстоятельства, при которых люди, имущество или окружающая среда подвержены одной или нескольким ОПАСНОСТЯМ.

[МЭК 14971:2007, статья 2.4]

3.26 **ДАННЫЕ О ЗДОРОВЬЕ** (HEALTH DATA): ЛИЧНЫЕ ДАННЫЕ, указывающие на состояние физического или психического здоровья.

Примечание — Вышеописанное в общих чертах определяет в рамках настоящего стандарта личные данные и их подраздел ДАННЫЕ О ЗДОРОВЬЕ, что позволяет пользователям настоящего стандарта легко применять эти понятия к разным нормативным актам и регламентам о конфиденциальности данных. Например, в Европе, такие требования могут быть приняты, а термин может быть заменен на «Персональные данные» и «Уязвимые данные». В США термин ДАННЫЕ О ЗДОРОВЬЕ может быть заменен на «Защищенную информацию о здоровье (PHI)», а также, при необходимости, могут быть внесены поправки и в сам текст.

[МЭК/ТО 80001-2-2:2012, статья 3.7]

3.27 **МЕДИЦИНСКАЯ ОРГАНИЗАЦИЯ МО** (HEALTHCARE DELIVERY ORGANIZATION): Объект или предприятие, такое как клиника или больница, предоставляющее медицинские услуги.

3.28 **ЗАКОН О МОБИЛЬНОСТИ МЕДИЦИНСКОГО СТРАХОВАНИЯ И ОТСЛЕЖИВАЕМОСТИ ДАННЫХ** (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT, HIPAA): Законодательство, принятое в США, положения которого включают в себя, среди прочего, требования обеспечения защиты защищенных ДАННЫХ о ЗДОРОВЬЕ.

3.29 **ПРОМЫШЛЕННЫЙ, НАУЧНЫЙ И МЕДИЦИНСКИЙ ДИАПАЗОН** (INDUSTRIAL, SCIENTIFIC AND MEDICAL BAND, ISM): Радиодиапазоны, которые были первоначально предусмотрены (на международном уровне) для случаев использования РАДИОЧАСТОТНОЙ (RF) энергии в промышленных, научных и медицинских целях.

3.30 **ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ, ИТ** (INFORMATIONAL TECHNOLOGY): Технология (компьютерные системы, сети, программное обеспечение), использующаяся для реализации ПРОЦЕССА хранения, сбора и распространения информации.

3.31 **ИТ СЕТЬ** (INFORMATION TECHNOLOGY NETWORK, IT-NETWORK): Система или системы, состоящие из взаимодействующих узлов и каналов передачи данных, предназначенные для обеспечения проводной или беспроводной передачи данных между двумя или более установленными узлами коммуникации.

[МЭК 80001-1:2010, статья 2.12. Определение является модифицированным. Два примечания исходного определения не были сохранены.]

3.32 **ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ, ПРЕДНАЗНАЧЕНИЕ** (INTENDED USE INTENDED PURPOSE): Применение изделия, ПРОЦЕССА или службы в соответствии с техническими условиями, инструкциями и информацией, предоставленной производителем.

[МЭК 80001-1:2010, статья 2.10]

3.33 **ОТДЕЛЕНИЕ ИНТЕНСИВНОЙ ТЕРАПИИ** (INTENSIVE CARE UNIT, ICU): Участок больницы, на котором за ПАЦИЕНТОМ будет осуществляться строгий контроль, в связи с критическим состоянием его здоровья.

3.34 **ИНТЕРНЕТ ПРОТОКОЛ ГРУППОВОЙ МНОГОАДРЕСНОЙ ПЕРЕДАЧИ ДАННЫХ** (INTERNET GROUP MULTICAST PROTOCOL, IGMP): Протокол коммуникаций, использующийся хост-узлами и смежными маршрутизаторами в IP сетях для утверждения членства в группе МНОГОАДРЕСНОЙ ПЕРЕДАЧИ

3.35 **ИНТЕРОПЕРАБЕЛЬНОСТЬ** (INTEROPERABILITY): Свойство, позволяющее разнообразным системам и компонентам работать вместе для достижения установленной цели.

[МЭК 80001-1:2010, статья 2.11]

3.36 **СИСТЕМА ОБНАРУЖЕНИЯ ПРОНИКНОВЕНИЙ** (INTRUSION DETECTION SYSTEM, IDS): Система, осуществляющая контроль беспроводного окружения и обнаруживающая несанкционированные случаи использования, такие как «мошеннические» ТОЧКИ ДОСТУПА, вирусы, вирусы-черви и т. д.

3.37 **СИСТЕМА ПРЕДОТВРАЩЕНИЯ ПРОНИКНОВЕНИЙ** (INTRUSION PROTECTION SYSTEM, IPS): Система, включающая в себя IDS, старающаяся регулярно блокировать проникновения в систему.

3.38 **ОСНОВНЫЕ СВОЙСТВА** (KEY PROPERTIES): Три управляемые характеристики риска (БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ и ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ) МЕДИЦИНСКИХ ИТ СЕТЕЙ.

[МЭК 80001-1:2010, статья 2.13]

3.39 **ЛОКАЛЬНАЯ СЕТЬ** (LOCAL AREA NETWORK): Компьютерная сеть, охватывающая маленькую физическую область, такую как дом или офис, или же маленькую группу зданий, такую как школа или аэропорт.

Примечание — В терминологии 802.3 LAN — это набор устройств, реализующих ШИРОКОВЕЩАТЕЛЬНУЮ функцию.

3.40 **УПРАВЛЕНИЕ ДОСТУПОМ К СРЕДЕ** (MEDIA ACCESS CONTROL, MAC): Часть канального уровня в эталонной модели взаимодействия открытых систем.

3.41 **МЕДИЦИНСКИЙ ПРИБОР** (MEDICAL DEVICE): Любой инструмент, устройство, приспособление, машина, прибор, имплантат, реагент или калибратор в пробирке, программное обеспечение, материал или другие подобные, связанные с ними изделия:

a) предполагаемые производителем для применения к человеку, отдельно или в сочетании друг с другом для одной или более заданных целей, таких как:

- диагностика, профилактика, контроль, лечение или облегчение течения заболеваний,
- диагностика, контроль, лечение, облегчение травмы или компенсация последствий травмы,
- исследования, замещения, изменения или поддержка анатомического строения или физиологических процессов,
- поддержание и сохранение жизни,
- предупреждение беременности,
- дезинфекция медицинских приборов,
- предоставление информации для медицинских и диагностических целей, посредством исследований проб в пробирке, полученных из тела человека; и

b) не реализующие свое основное предназначение в или на теле человека с помощью фармакологических, иммунологических или метаболических средств, но чья основная функция может поддерживаться подобными мерами.

Примечания

1 Определение прибора для исследований в лабораторных условиях включает, например, реагенты, бужизмеритель, приборы забора и хранения образцов, контрольные материалы и связанные с этим инструменты и приспособления. Данные, полученные с помощью такого прибора диагностики в лабораторных условиях, могут использоваться в целях диагностики, контроля или сравнения. В некоторых юрисдикциях, отдельные приборы лабораторной диагностики, включая реагенты и подобные им, могут подчиняться отдельным правилам и положениям .

2 Изделия, которые, в некоторых юрисдикциях, могут быть приняты за медицинские приборы, но к которым еще не существует согласованного подхода, это:

- средства помощи инвалидам и людям с ограниченными возможностями;
- приборы для лечения/диагностики болезней и травм животных;
- аксессуары для медицинских приборов (см. примечание 3);
- дезинфицирующие вещества;
- приборы, использующие ткани животных и людей, которые могут соответствовать описанным выше определениям, но используются для других направлений.

3 Аксессуары, специально предназначенные производителями для использования совместно с медицинским прибором, для которого они были разработаны, для реализации цели медицинского прибора, должны подчиняться тем же процедурам GHT (Целевая группа глобальной гармонизации), которые применяются к самому медицинскому прибору. Например, аксессуар классифицируется так, как будто он является медицинским прибором. Это может привести к различию в классификациях аксессуара и прибора, для которого он был разработан.

4 Компоненты медицинских приборов в общих случаях контролируются через систему управления качеством производителя и процедуры оценки соответствия прибора. В некоторых юрисдикциях, компоненты включаются в определение «медицинского прибора».

[МЭК 80001-1:2010, статья 2.14]

3.42 **ПРОИЗВОДИТЕЛЬ МЕДИЦИНСКОГО ПРИБОРА**, ПМП (MEDICAL DEVICE MANUFACTURER): Производитель МЕДИЦИНСКИХ ПРИБОРОВ.

3.43 **ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МЕДИЦИНСКОГО ПРИБОРА** (MEDICAL DEVICE SOFTWARE): Система программного обеспечения, разработанная с целью включения в МЕДИЦИНСКИЙ ПРИБОР или предназначенная для использования как самостоятельный МЕДИЦИНСКИЙ ПРИБОР.

[МЭК 80001-1:2010, статья 2.15]

3.44 **МЕДИЦИНСКАЯ ИТ СЕТЬ** (MEDICAL IT-NETWORK): ИТ СЕТЬ, к который подключен хотя бы один МЕДИЦИНСКИЙ ПРИБОР.

[МЭК 80001-1:2010, статья 2.16]

3.45 **СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ СЕТИ (MEDICAL IT-NETWORK RISK MANAGER)**: Лицо, ответственное за МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ СЕТИ.

[МЭК 80001-1:2010, статья 2.17]

3.46 **МНОГОКАНАЛЬНЫЙ ВХОД МНОГОКАНАЛЬНЫЙ ВЫХОД** (MULTIPLE-IN MULTIPLE-OUT, MIMO): Использование нескольких антенн, установленных как на передатчике, так и на приемнике, для повышения производительности коммуникаций.

3.47 **ГРУППОВАЯ АДРЕСАЦИЯ** (MULTICAST ADDRESSING): Технология одновременной передачи сообщения группе абонентов сети.

3.48 **ОПЕРАТОР** (OPERATOR): Лицо, работающее с оборудованием.

[МЭК 80001-1:2010, статья 2.18]

3.49 **ПЕРСОНАЛЬНАЯ СЕТЬ** (PERSONAL AREA NETWORK, PAN): Компьютерная сеть, использующаяся для осуществления коммуникаций между компьютерными устройствами, включая телефоны и персональные цифровые помощники, находящиеся рядом с пользователем.

3.50 **ФИЗИЧЕСКИЙ ИНТЕРФЕЙС** (PHYSICAL INTERFACE, PHY): Уровень коммуникационного контроллера, взаимодействующий с физической средой.

3.51 **ПЕРЕНОСНОЙ ЦИФРОВОЙ ПОМОЩНИК** (PORTABLE DIGITAL ASSISTANT, PDA): Небольшое вычислительное устройство, предназначенное для таких задач, как ведение персонального дневника или контроля соблюдения графика.

3.52 **ПРЕДВАРИТЕЛЬНЫЙ КЛЮЧ** (PRE-SHARED KEY, PSK): Совместно используемый секретный ключ, который был предварительно выдан двум участвующим сторонам для шифрования данных, которыми они будут обмениваться.

3.53 **ЛИЧНЫЕ ДАННЫЕ** (PRIVATE DATA): Любая информация, связанная с идентифицированной личностью или личностью, доступной для идентификации.

[МЭК/ТО 80001-2-2:2012, статья 3.15]

3.54 **ПРОЦЕСС** (PROCESS): Совокупность взаимосвязанных и взаимодействующих действий, преобразующих входы в выходы.

[МЭК 80001-1:2010, статья 2.19]

3.55 **КАЧЕСТВО ОБСЛУЖИВАНИЯ** (QUALITY OF SERVICE, QoS): Возможность или средства обеспечения производительности сети на различных уровнях с помощью управления трафиком (задержкой, потерей, искажением пакета, скоростью передачи данных в бит/сек) различных потоков данных.

РАДИОЧАСТОТА RF (RADIO FREQUENCY): Частота, соответствующая области электромагнитного спектра, находящейся между областями звуковых частот и частот инфракрасного излучения. РАДИОЧАСТОТЫ используются при осуществлении радиопередач.

[МЭК 60601-1-2:2007, статья 3.25]

3.56 **РАДИОЧАСТОТНАЯ ИДЕНТИФИКАЦИЯ** (RADIO FREQUENCY IDENTIFICATION, RFID): Идентификация объектов или лиц посредством специальных меток, содержащих информацию (такую как демографические данные, серийный номер и т. д.), которая может быть считана устройствами считывания, работа которых основана на RF.

3.57 **ИНДИКАТОР УРОВНЯ ПРИНИМАЕМОГО СИГНАЛА** (RECEIVED SIGNAL STRENGTH INDICATOR, RSSI): Мера мощности, как правило в дБмВт, RF сигнала, обнаруженного приемником.

3.58 **ОСТАТОЧНЫЙ РИСК** (RESIDUAL RISK): РИСК, остающийся после выполнения мер по УПРАВЛЕНИЮ РИСКОМ.

[МЭК 80001–1:2010, статья 2.20]

3.59 **СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ** (RESPONSIBILITY AGREEMENT): Один или более документов, которые совместно определяют все ответственности для всех значимых заинтересованных сторон.

Примечание — Данное соглашение может быть юридическим документом, например, контрактом.

[МЭК 80001-1:2010, статья 2.21]

3.60 **ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ** (RESPONSIBILE ORGANIZATION): Юридическое или физическое лицо, ответственное за использование и обслуживание МЕДИЦИНСКОЙ ИТ СЕТИ.

Примечания

1 Ответственным лицом может быть, например, больница, частный врач или организация телемедицины.

2 Адаптировано из МЭК 60601-1:2005, подраздел 3.101.

[МЭК 80001-1:2010, статья 2.22]

3.61 **РИСК** (RISK): Комбинация вероятности причинения ВРЕДА и его тяжести.

[МЭК 80001-1:2010, статья 2.23]

3.62 **АНАЛИЗ РИСКА** (RISK ANALYSIS): Систематическое использование доступной информации для выявления ОПАСНОСТЕЙ и количественной оценки РИСКА.

[МЭК 80001-1:2010, статья 2.24]

3.63 **ОЦЕНКА РИСКА** (RISK ASSESSMENT): Общий процесс, включающий в себя АНАЛИЗ РИСКА и ОЦЕНИВАНИЕ РИСКА.

[МЭК 80001-1:2010, определение 2.25]

3.64 **УПРАВЛЕНИЕ РИСКОМ** (RISK CONTROL): ПРОЦЕСС принятия решений и выполнения мер по уменьшению рисков до установленных уровней или поддержания рисков внутри установленного диапазона.

[МЭК 80001-1:2010, статья 2.26]

3.65 **ОЦЕНИВАНИЕ РИСКА** (RISK EVALUATION): ПРОЦЕСС сравнения количественно оцененного РИСКА, с заданными критериями РИСКА для определения значимости РИСКА.

[МЭК 80001-1:2010, статья 2.27]

3.66 **МЕНЕДЖМЕНТ РИСКА** (RISK MANAGEMENT): Систематическое применение политик, процедур и практических методов менеджмента для решения задач анализа, оценивания, управления и контроля РИСКА.

[МЭК 80001-1:2010, статья 2.28]

3.67 **ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ** (RISK MANAGEMENT FILE): Совокупность записей и других документов, создаваемых в процессе МЕНЕДЖМЕНТА РИСКА.

[МЭК 80001-1:2010, статья 2.29]

3.68 **БЕЗОПАСНОСТЬ** (SAFETY): Отсутствие недопустимого РИСКА физической травмы или ущерба здоровью людей, или ущерба имуществу, или окружающей среде.

[МЭК 80001-1:2010, статья 2.30]

3.69 **СОГЛАШЕНИЕ об УРОВНЕ УСЛУГ** (SERVICE LEVEL AGREEMENT, SLA): Производительность сети, которая требуется прибору или классу приборов для того, чтобы работать должным образом.

Примечание — Типичные SLA сетевых услуг охватывают такие показатели как доступность, временная задержка и пропускная способность. Они могут также включать в себя спецификации среднего времени ответа, среднего времени ремонта и гарантии уведомления/оперативного решения проблемы. В беспроводных системах примерами могут служить скорость передачи данных, уровень сигнала, искажение пакета и временная задержка.

3.70 **ПРОСТОЙ ПРОТОКОЛ УПРАВЛЕНИЯ СЕТЬЮ** (SIMPLE NETWORK MANAGEMENT PROTOCOL, SNMP): Стандартный интернет-протокол для управления устройствами в IP сетях.

3.71 **ОТНОШЕНИЕ СИГНАЛ/ШУМ**, ОСШ (SIGNAL TO NOISE RATIO): Сравнение мощностей сигнала и шума.

3.72 **ИДЕНТИФИКАТОР НАБОРА СЛУЖБ** (SERVICE SET IDENTIFIER, SSID): Термин из 802.11, описывающий логическое объединение множества идентификаторов BSSID.

Примечание — В некоторых случаях именуется как ESSID или имя сети.

3.73 **ПРОТОКОЛ УПРАВЛЕНИЯ ПЕРЕДАЧЕЙ** (TCP): Один из основных протоколов в наборе протоколов Интернета.

Примечание — Отличается от UDP тем, что TCP является признанным протоколом, ориентированным на соединение.

3.74 **ПРОТОКОЛ ЦЕЛОСТНОСТИ ВРЕМЕННОГО КЛЮЧА** (TEMPORAL KEY INTEGRITY PROTOCOL, TKIP): Временное решение вопроса защиты, которое поддерживалось старым оборудованием, когда WEP был признан уязвимым.

Примечание — Также известен под торговым наименованием 802.11, как WPA.

3.75 **ВЫСШЕЕ РУКОВОДСТВО** (TOP MANAGEMENT): Лицо или группа лиц, реализующих направление(я) деятельности и управление ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ, отвечающих за МЕДИЦИНСКУЮ ИТ-СЕТЬ на самом высоком уровне.

[МЭК 80001-1:2010, статья 2.31]

3.76 **ИНДИВИДУАЛЬНАЯ АДРЕСАЦИЯ** (UNICAST ADDRESSING): Технология передачи сообщения одному абоненту в сети.

3.77 **НЕЛИЦЕНЗИРУЕМАЯ НАЦИОНАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА** (UNLICENSED NATIONAL INFORMATION INFRASTRUCTURE, U-NII): Нелицензированная область спектра в диапазоне 5 ГГц, использующаяся в приборах стандарта IEEE-802.11an и беспроводных ISP.

3.78 **ПРОТОКОЛ ПОЛЬЗОВАТЕЛЬСКИХ ДАТАГРАММ** (USER DATAGRAM PROTOCOL, UDP): Один из основных протоколов в наборе протоколов Интернета.

Примечание — Отличается от TCP тем, что UDP не является признанным протоколом и не ориентирован на соединение.

3.79 **ВЕРИФИКАЦИЯ** (VERIFICATION): Подтверждение на основе предоставления объективных свидетельств того, что установленные требования были выполнены.

[МЭК 80001-1:2010, статья 2.32. Определение является модифицированным. Три примечания к оригинальному определению не были сохранены.]

3.80 **ВИРТУАЛЬНАЯ LAN** (VLAN): Группа хост-узлов, взаимодействующих так, как если бы они были подсоединены к одному ШИРОКОВЕЩАТЕЛЬНОМУ домену, независимо от их физического месторасположения или физического подключения к одному сетевому коммутатору.

3.81 **ПЕРЕДАЧА ГОЛОСА ПО ИНТЕРНЕТ-ПРОТОКОЛУ** (VOICE OVER INTERNET PROTOCOL, VOIP): Технология, которая позволяет осуществлять телефонные звонки через компьютерные сети.

Примечание — Типичная СХЕМА КОДИРОВАНИЯ/ДЕКОДИРОВАНИЯ (CODEC) G.711 обрабатывает сетевой поток с пропускной способностью 64 кбит/с, который включает 50 пакетов в секунду.

3.82 **ГЛОБАЛЬНАЯ КОМПЬЮТЕРНАЯ СЕТЬ** (WIDE AREA NETWORK, WAN): Коммуникационная сеть, покрывающая большую географическую область, делая возможным обмен данными между городами, регионами и странами.

3.83 **ЭКВИВАЛЕНТ КОНФИДЕНЦИАЛЬНОСТИ ПРОВОДНЫХ СЕТЕЙ** (WIRED EQUIVALENT PRIVACY, WEP): Первоначальные механизмы защиты по стандарту 802.11, которые были заменены на TKIP (также известный как WPA) для устаревших устройств и на AES (также известный как WPA2) для всех устройств, сертифицированных в соответствии с 802.11, начиная с 2006 г.

3.84 **БЕСПРОВОДНОЕ КАЧЕСТВО** (WIRELESS FIDELITY Wi-Fi™): Торговая марка Wi-Fi Alliance.

3.85 **БЕСПРОВОДНАЯ ЛОКАЛЬНАЯ СЕТЬ** (WIRELESS LOCAL AREA NETWORK WLAN): ЛОКАЛЬНАЯ СЕТЬ, передающая и получающая данные посредством радиосигналов.

3.86 **БЕСПРОВОДНАЯ МЕДИЦИНСКАЯ ТЕЛЕМЕТРИЧЕСКАЯ СЛУЖБА** (WIRELESS MEDICAL TELEMETRY SERVICE, WMTS): Беспроводная служба (набор диапазонов радиочастот), специально утвержденная в США Федеральной Комиссией Связи (FCC) для передачи данных, связанных со здоровьем пациента (биотелеметрии).

3.87 **WI-FI МУЛЬТИМЕДИА** (WI-FI MULTI-MEDIA, WMM): Подраздел стандарта 802.11e, который предоставляет дифференцированное КАЧЕСТВО ОБСЛУЖИВАНИЯ для процесса доставки сообщений для некоторых классов трафика.

3.88 **ЗАЩИЩЕННЫЙ ДОСТУП WI-FI (WI-FI PROTECTED ACCESS**, WPA): Временное решение вопроса защиты, которое исправило многие из недостатков алгоритма WEP и может быть реализовано на старом оборудовании, спроектированном для реализации WEP.

3.89 **ЗАЩИЩЕННЫЙ ДОСТУП WI-FI 2** (WI-FI PROTECTED ACCESS 2, WPA2): Долгосрочное решение вопроса защиты, принятое для замены WEP и WPA.

Примечание — WPA2 использует УСОВЕРШЕНСТВОВАННЫЙ СТАНДАРТ ШИФРОВАНИЯ с добавлением функций защиты, таких как, проверка целостности сообщения.

4 Беспроводные МЕДИЦИНСКИЕ ИТ СЕТИ. Введение

4.1 Базовые понятия

Общее представление проблем, связанных с возможностью беспроводного подключения к МЕДИЦИНСКИМ ПРИБОРАМ, является критически важным для успешной работы МЕДИЦИНСКОЙ ИТ СЕТИ. Ниже описаны некоторые из высокоуровневых проблем, встречающихся при реализации беспроводной медицинской ИТ сети:

- использование смартфонов (интеллектуальных телефонов) и планшетных устройств из социальных сетей в качестве кардиологических устройств наблюдения;
- отсутствие у персонала отделов ИТ, биомедицины и клинической инженерии навыков работы в области беспроводных и RF технологий;
- использование перегруженного нелицензионного диапазона;
- запатентованные функции в дополнение к стандартам (например, таким как, 802.11);
- обеспечение защиты данных, как на беспроводных устройствах, так и при передаче;
- формальное организационное взаимодействие между персоналом отделов ИТ, биомедицины и клинической инженерии.

Как правило, эти трудности разрешаются с помощью применения концепции «наилучших практик» в процессе проектирования и управления беспроводной сетью. Многие из наилучших практик, обычно использующихся для решения этих трудностей, относят к категории мер по УПРАВЛЕНИЮ РИСКОМ согласно профессиональному языку МЭК 80001-1:2010. В настоящем стандарте предлагается осуществить интеграцию этих и других наилучших практик в ПРОЦЕСС применения МЕНЕДЖМЕНТА РИСКА к разработке МЕДИЦИНСКОЙ ИТ СЕТИ.

Трудности, связанные с выполнением требований SLA для множества разных приборов усугубляются еще и тем фактом, что у одного МЕДИЦИНСКОГО ПРИБОРА может быть множество уровней РИСКА. В настоящем стандарте будет подчеркнуто, что один и тот же вид трафика в клиническом приборе может обладать различной клинической важностью, зависящей от варианта клинического использования или функциональности. Например физиологические данные, как правило, не требуется передавать в EMR (электронную медицинскую карту) в реальном времени. Тем не менее, если такие данные направляются практикующему врачу и содержат информацию о текущем состоянии пациента в реальном времени, то задержка доставки все тех же данных теперь имеет повышенную степень тяжести ОПАСНОСТИ и для ее устранения могут потребоваться более мощные средства УПРАВЛЕНИЯ РИСКОМ. Таким образом, при проектировании и конфигурировании сети недостаточно использовать только характеристики производительности МЕДИЦИНСКОГО ПРИБОРА, клинические аспекты использования и поддержки прибора, необходимо также включать в проектное решение сети.

4.2 Корпоративная МЕДИЦИНСКАЯ ИТ СЕТЬ

Проектирование больничных сетей в беспроводном окружении является очень трудной задачей из-за сложного физического окружения и того, как оно влияет на прохождение радиочастотных сигналов (RF сигналов), а также в связи с большим числом близкорасположенных устройств, функционирующих в сети.

Сложности в радиочастотной среде, как правило, связаны с мобильным металлическим оборудованием (например, металлический поднос для еды или лекарственных препаратов), стенами из строительных материалов с варьирующимися характеристиками прохождения радиочастотных сигналов и планировкой этажей, меняющейся от отделения к отделению. Типы приборов, подключенных к здравоохранительной сети, включают в себя множество типов приборов общего назначения, не МЕДИЦИНСКИХ, также как и МЕДИЦИНСКИХ ПРИБОРОВ. Такими приборами могут быть устройства гостевого доступа, рабочие станции на колесах, на которых установлены разнообразные приложения, инфузионные насосы, карманные устройства ввода данных, такие как PDA устройства или планшетные персональные компьютеры, коммуникационные устройства VOIP, метки радиочастотной идентификации (RFID-метки) и приборы контроля пациента. Каждое из этих устройств обладает своими собственными характеристиками данных и трафика, использующими различные протоколы связи (TCP, UDP и т.д.), и своими собственными требованиями к производительности сети (которые могут варьироваться в случае клинической функциональности, как, например, в результатах лабораторных испытаний, упомянутых выше). Прибор может обладать множеством клинических функций, таких как мобильность пациента; передача больших файлов изображений, клинические аварийные сигналы и сигналы тревоги в режиме реального времени, и передача физиологических данных в EMR. Данные клинические функции, вместе с требованиями к производительности сети прибора и профилями трафика данных определяют клиническое СОГЛАШЕНИЕ об УРОВНЕ ОБСЛУЖИВАНИЯ (SLA). Там где необходимо добиться мобильности, защищенности, низкой задержки, высокого уровня доступности и других показателей производительности сети, клиническая функциональность отображается в соответствующие варианты сетевого использования. Коротко говоря, разница между выполнением требований к производительности сети в случае беспроводных устройств общего назначения и в случае МЕДИЦИНСКИХ ПРИБОРОВ заключается в том, что несоответствие уровню SLA для компьютера общего назначения влечет за собой только неудобство работы с медленным сетевым соединением. ОПАСНОСТЬ, вызванная невыполнением требований SLA для МЕДИЦИНСКОГО ПРИБОРА, может привести к ОПАСНОЙ СИТУАЦИИ и возможному причинению ВРЕДА пациенту.

На диаграмме на рисунке 2 показан упрощенный пример проводной и беспроводной МЕДИЦИНСКОЙ ИТ СЕТИ с трафиком, как и от МЕДИЦИНСКИХ ПРИБОРОВ, так и от приборов общего назначения.

Использование VLAN для логического разделения типов трафика является распространенным методом в проводных технологиях построения сетей и может расширяться до беспроводных технологий на периметре сети с помощью различных средств (например, SSID идентификаторы часто назначаются определенной VLAN сети). В дополнение к множеству типов трафика и связанных с ними уровней SLA, в МЕДИЦИНСКОЙ ИТ СЕТИ может также существовать множество разных коммуникационных путей, установленных между МЕДИЦИНСКИМИ ПРИБОРАМИ, центральными постами медсестры или ведущих через центр сбора и обработки данных в помещение для централизованного контроля.

4.3 Использование сетей VLAN и идентификаторов SSID

Использование ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ (VLAN) распространено в проводных сетях, но каждая дополнительная VLAN и сопутствующие ей SSID привносит определенные дополнительные расходы ШИРОКОВЕЩАТЕЛЬНОГО/МНОГОАДРЕСНОГО трафика, что может негативно повлиять на доступную емкость беспроводного канала. Следует проявлять осторожность при обычном использовании VLAN сетей и SSID идентификаторов для сегментирования трафика. Следует также рассмотреть другие механизмы логического разделения трафика, чтобы минимизировать дополнительные расходы ШИРОКОВЕЩАТЕЛЬНОГО/МНОГОАДРЕСНОГО трафика, связанные с использованием нескольких VLAN сетей. Другие возможности по разделению трафика могут включать в себя использование нескольких частот или диапазонов частот с различающимися SSID и запатентованные механизмы, предоставленные оператором инфраструктуры WLAN. Разделение устройств посредством уникальных VLAN и ESSID не считается наилучшей практикой, особенно если группа устройств, которую необходимо разделить, растет по причине того, что каждый дополнительный ESSID или VLAN привносят дополнительные расходы ресурсов беспроводного канала.

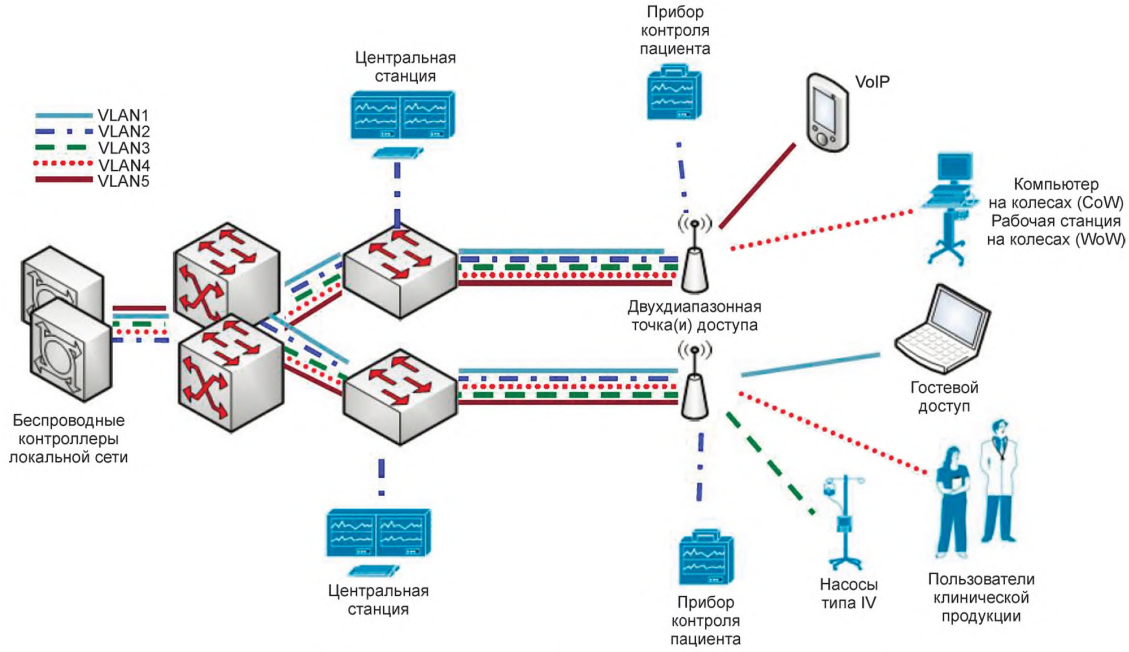

Рисунок 2 — МЕДИЦИНСКАЯ ИТ СЕТЬ медицинской организации

4.4 Глобальная МЕДИЦИНСКАЯ ИТ СЕТЬ

На рисунке 3 показана модель, в которой МЕДИЦИНСКИЕ ПРИБОРЫ взаимодействуют в рамках ГЛОБАЛЬНЫХ СЕТЕЙ, как проводных, так и беспроводных, обеспечивая доставку медицинского трафика для предоставления удаленного доступа к клинической информации. Это можно осуществлять через сборку данных от пациентов на дому, за которыми осуществляется удаленный контроль, или с помощью более продвинутых функциональных возможностей, в которых источники видеосигналов дают терапевту интерактивный доступ в режиме реального времени к данным о пациенте, находящемся у себя дома. Многие из промежуточных сетей в глобальном варианте использования имеют компоненты, принадлежащие разным административным территориям, что усложняет обеспечение целостных SLA соглашений. В связи с этим, подобные компоненты больших сетей усложняют обеспечение производительности, которая необходима для аварийных сигналов пациентов в режиме реального времени и сопутствующих ответных действий в случаях, когда БЕЗОПАСНОСТЬ пациента зависит от совокупной производительности сети.

Следует оценить пользу от использования определенной инфраструктуры, например сотовой, с учетом РИСКОВ. Например, для пациентов, находящихся не в больнице, получение клинической экспертной помощи через беспроводную WAN сеть, такую как сотовую сеть, будет выгодно даже в том случае, если терапевт будет периодически недоступен из-за отключения сети.

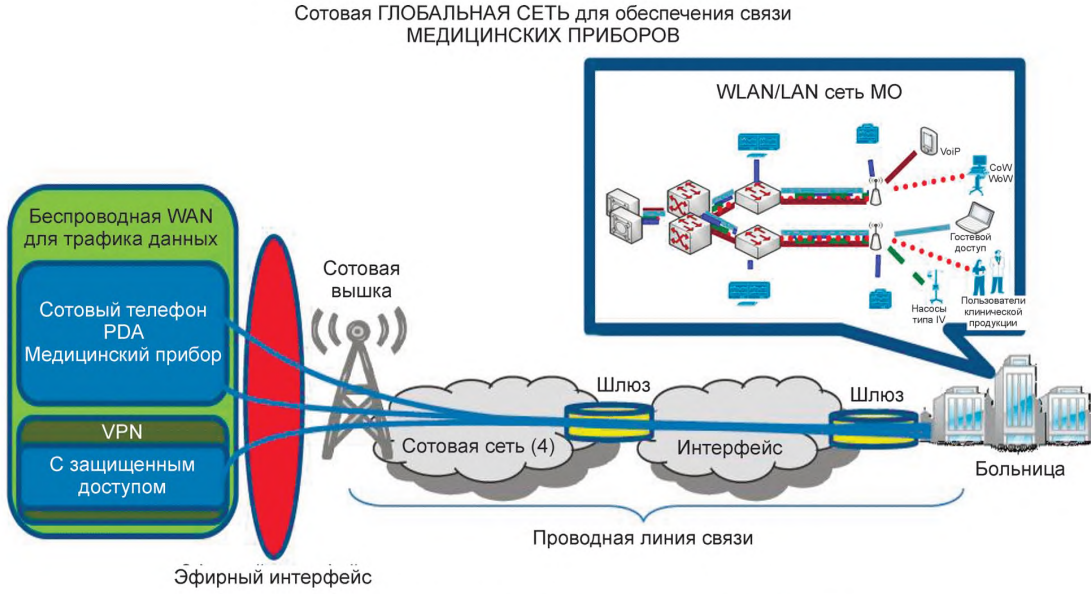

Рисунок 3 — Возможные подключения беспроводной сети WAN

4.5 Приложения смартфонов (интеллектуальных телефонов)

4.5.1 Общие положения

Все более распространяющееся использование служб передачи голоса, видео и данных смартфонов привело к появлению значительного числа разработок приложений для этих устройств. Некоторые из таких приложений предназначаются или будут предназначаться для здравоохранения. Использование подобных устройств и их медицинских приложений достигнет как больниц, так и врачебных пунктов, клиник и жилых домов. Как и для любого другого МЕДИЦИНСКОГО ПРИБОРА, в АНАЛИЗЕ РИСКА данных устройств необходимо учитывать клиническое использование приложений так же, как и ожидаемые рабочие характеристики сети(ей), через которые проходят медицинские данные.

4.5.2 Клиническая функциональность приложения

В то время как аппаратная составляющая смартфона, как правило, не эксплуатируется как МЕДИЦИНСКИЙ ПРИБОР, использование медицинских приложений и их предусмотренной клинической функциональности определяет оправданность применения мер по УПРАВЛЕНИЮ РИСКОМ. Трудность для ИТ отдела МО заключается в том, что сеть может быть WAN сетью, которая конфигурируется и управляется ИТ администрацией МО. Это не означает, что применение мер по УПРАВЛЕНИЮ РИСКОМ невозможно, а только то, что производительность внешней сети необходимо рассмотреть и определить в терминах клинической функциональности и ожиданий пользователя. Важно, чтобы конечный пользователь, будь он терапевтом или пациентом, понимал рабочие возможности, лежащие в основе сети, и то, что некоторыми мерами по УПРАВЛЕНИЮ РИСКОМ должен управлять на приборе сам пользователь.

Например, надежность сотовых или беспроводных широкополосных сетей может быть допустимой для варианта использования, в котором терапевт занимается удаленным анализом медицинских карт пациентов при помощи смартфона. Как бы там ни было, терапевту нужно быть готовым к тому обстоятельству, что беспроводное соединение с данными может оказаться недоступным в определенное время и в определенном месте.

4.5.3 Сотовые сети

Появление сетей 4G (сетей четвертого поколения) и сопутствующих им устройств со значительно более высокой скоростью передачи данных, введение фемто-ячеек для локализованного беспроводного развертывания и продолжающаяся эволюция и усовершенствование смартфонов окажут влияние на медицинские организации (МО) и их способности безопасно управлять сетью. С целью удовлетворения растущих требований к пропускной способности со стороны как медицинских, так и немедицинских приложений и устройств, необходимо рассмотреть использование всех сетей. Например, смартфон, который включает как 802.11, так и 3G/4G радиоприемники, часто по умолчанию выбирает сеть 802.11. Это

может создавать излишнюю нагрузку для беспроводной локальной сети 802.11. В таком случае сотовая ГЛОБАЛЬНАЯ СЕТЬ для обеспечения медицинской связи, вынуждающая устройство к работе в 3G/4G сети, будет примером меры по УПРАВЛЕНИЮ РИСКОМ.

4.5.4 Сосуществование смартфонов

Смартфоны, как правило, включают в себя радиоприемник 802.11 (в дополнение к сотовой связи), который используется для получения широкополосного доступа, когда это возможно. Если в МО используется множество смартфонов, с взыскательными требованиями к доступу к широкополосной сети (например, возможность беспроводной трансляции видео, передачи голоса и т. д.), то эти устройства могут перегружать емкость сети и вызывать выходы из строя сети, которые влияют на все устройства, подключенные к WLAN 802.11. Несмотря на то что смартфоны могут как использоваться, так и не использоваться для медицинских целей, они по-прежнему будут влиять на защиту и производительность всех устройств в сети, если та не обеспечивается должным образом. Надлежащее обеспечение сети, осуществляющееся таким образом, что смартфоны, независимо от их использования, не перегружают сеть, является мерой по УПРАВЛЕНИЮ РИСКОМ на этапе конфигурации и проектирования, которую следует применять. См. 6.4 для общего руководства по мерам УПРАВЛЕНИЯ РИСКОМ.

4.5.5 Защита данных в беспроводных сетях

Передача ДАННЫХ о ЗДОРОВЬЕ пациента требует наличия сильных механизмов для защиты этих данных. Меры по УПРАВЛЕНИЮ РИСКОМ для предотвращения потери или кражи ЛИЧНЫХ ДАННЫХ или ДАННЫХ о ЗДОРОВЬЕ включают в себя технологии, предотвращающие хранение ЛИЧНЫХ ДАННЫХ или ДАННЫХ о ЗДОРОВЬЕ и/или удаленное стирание/разрушение данных на самом устройстве. Меры защиты, связанные с шифрованием и авторизацией пользователей в сетях, рассмотрены в остальных разделах настоящего стандарта. Дополнительная информация может быть найдена в документе о защите (см. «Библиографию»).

4.6 РАСПРЕДЕЛЕННЫЕ АНТЕННЫЕ СИСТЕМЫ

Некоторые МО применяют РАСПРЕДЕЛЕННЫЕ АНТЕННЫЕ СИСТЕМЫ (DAS) для распространения сотовых, пейджинговых, сигналов общественной БЕЗОПАСНОСТИ и других радиочастотных сигналов (RF сигналов) в здании через разделенную антенную инфраструктуру. Такая инфраструктура может использовать активные и пассивные технологии, а многие инфраструктуры включают также их совместное использование. Пассивная система использует ADSL-фильтры (сплиттеры), соединительные устройства и коаксиальные кабели для передачи радиочастотных сигналов на излучатели/антенны, которые распространяют сигнал на необходимой территории. Активная система передает цифровые данные удаленному электронному оборудованию, которое конвертирует цифровой сигнал в/из радиочастотного сигнала и усиливает как принятые, так и переданные радиочастотные сигналы. Гибридная волоконно-оптическая/коаксиальная система добавляет пассивное распространение после удаленного электронного оборудования.

При правильном проектировании, развертывании, обеспечении и проведении подтверждения на соответствие DAS может предоставить эксплуатационные выгоды в отличие от развертывания отдельной системы антенн внутри здания для каждого поставщика услуг беспроводной связи (WSP), так как одна DAS может обеспечить для каждого WSP охват всего здания корпорации. Это в особенности актуально для случаев использования сотовых сигналов в корпорациях. МО следует учитывать, что широкий охват ведет к тому, что каждое устройство WSP принимает шум из всей территории охвата, а это сказывается на ОСШ (соотношении сигнала и шума) системы. Аналогично преимущество увеличения зоны охвата DAS, в свою очередь, увеличивает число пользователей, поддерживаемых конкретным элементом оборудования WSP, а это, в свою очередь, увеличивает нагрузку пользователей, которую следует учитывать при развертывании системы DAS.

Важно понимать проблемы и их решения при использовании технологий 802.11 для DAS. Некоторые поставщики DAS поддерживают интеграцию 802.11 в DAS, другие же — нет. На данный момент поставщики инфраструктуры 802.11 не сертифицируют свое оборудование, соединенное с DAS. Многие из дополнительных функций, рекламируемых и распространяемых поставщиками технологий 802.11, такие как IDS, IPS, службы определения местоположения и согласованное использование многолучевого распространения для улучшения производительности RF системы проектируются для использования с отдельной WLAN архитектурой и могут быть совместимы, хотя, как правило, поставщики AP не гарантируют производительность RF системы при использовании антенн, которые они не испытывали и не рекомендовали. Использование технологий 802.11n с MIMO создает дополнительные трудности

для развертываний DAS систем, так как каждый поток входа/выхода требует дополнительную антенну для того, чтобы функционировать в соответствии своему проекту. Некоторые свойства 802.11n, такие как формирование луча, потребуют дополнительную перестройку DAS системы. Консультирование как с поставщиком DAS, производителем устройства, так и с поставщиком инфраструктуры 802.11 критически важно осуществлять до развертывания 802.11 в DAS.

5 Беспроводные МЕДИЦИНСКИЕ ИТ СЕТИ. Планирование и проектирование

5.1 Клинические системы и их влияние на беспроводную сеть

Клинические системы и их влияние на беспроводную сеть определяются на ранних этапах планирования и проектирования МЕДИЦИНСКОЙ ИТ СЕТИ. С точки зрения отдела ИТ, практикующие врачи могут рассматриваться как новые клиенты сети WLAN, которые приносят в сеть клинические системы и МЕДИЦИНСКИЕ ПРИБОРЫ, обладающие уникальными и изменяющимися требованиями к производительности сети.

5.1.1 Определение клинического СОГЛАШЕНИЯ об УРОВНЕ УСЛУГ (SLA)

Понимание того, как практикующие врачи будут использовать МЕДИЦИНСКИЕ ПРИБОРЫ в своем рабочем процессе, того, что в настоящем стандарте определено как клиническая функциональность, является первым шагом на ранних стадиях планирования применения МЕНЕДЖМЕНТА РИСКА к беспроводным сетям. Поддержка и управление многочисленными SLA, некоторые из которых будут обладать жизненно важными аспектами, в МЕДИЦИНСКОЙ ИТ СЕТИ является трудной задачей. От гостевого доступа к интернету общего назначения до критически важных для миссии бизнес-приложений и до приборов контроля пациента — требования к производительности таких сетей различны и разнообразны.

Клиническое СОГЛАШЕНИЕ об УРОВНЕ УСЛУГ (SLA) состоит как из требований к производительности сети на уровне прибора, так и из систем клинической поддержки типа Helpdesk (службы технической поддержки) и процедурных систем. Ниже приведен список типичных компонентов клинического SLA:

- требования к производительности сети на уровне прибора (потеря пакетов данных, задержка и т. д.);
- время реакции службы технической поддержки (helpdesk'a);
- время безотказной работы или доступность сети;
- области действия беспроводной сети, уровни сигнала и доступность полосы пропускания;
- система защиты;
- поддержка и конфигурация коммуникационного протокола (протокола связи);
- регламент восстановления после аварий;
- составление графика технического обслуживания устройства.

Компиляция и документация базового клинического SLA является основным показателем результативности в планировании и проектировании МЕДИЦИНСКОЙ ИТ СЕТИ. Данное соглашение достигается взаимодействием с практикующими врачами и персоналом отдела биомедицинской инженерии на этапе планирования и проектирования, с целью понимания ПРОЦЕССА и клинической функциональности, связанной с работающими в сети приборами.

5.1.2 Создание партнерских отношений

С введением МЕДИЦИНСКИХ ПРИБОРОВ и клинических систем в беспроводную ИТ сеть общего назначения одной из первоначальных задач является участие практикующих врачей, биомедицинских инженеров и команды ИТ инженерии в ПРОЦЕССЕ планирования. Проектировщик сети получает представление о требованиях к производительности сети, полученных для клинической системы, в результате анализа того, как и где будет использоваться каждый МЕДИЦИНСКИЙ ПРИБОР, проводимого совместно с практикующими врачами и поддерживающим персоналом. Без понимания этих требований невозможно определить клиническое SLA для МЕДИЦИНСКИХ ПРИБОРОВ или систем.

В таблице приложения А представлен пример анализа МЕДИЦИНСКИХ ПРИБОРОВ и их клинических требований, а также требований к сетевому трафику. Таблица приложении А демонстрирует различные типы данных, с которыми можно столкнуться при использовании беспроводных МЕДИЦИНСКИХ ПРИБОРОВ и связанных с ними их сетевых профилей. В приложении В представлен список вопросов, с которыми следует ознакомиться при определении требований к производительности сети МЕДИЦИНСКИХ ПРИБОРОВ, размещенных в беспроводной сети.

5.1.3 Географическое месторасположение

Информация для определения клинической функциональности включает в себя идентификацию географической области, в которой практикующие врачи будут использовать МЕДИЦИНСКИЕ ПРИБОРЫ, приложения и системы. Приборам, которые могут быть мобильными в пределах всей корпорации, может потребоваться как внутренняя, так и внешняя поддержка передачи обслуживания абонентов, предоставляемая в пределах беспроводных сетей. Приборы, которые используются на определенной территории (например, в отделении интенсивной терапии или ICU), лучше всего поддерживаются с помощью изолированной беспроводной инфраструктуры, предназначенной специально для МЕДИЦИНСКИХ ПРИБОРОВ. На этапе планирования следует провести оценку всех вышеперечисленных вариантов, чтобы выбрать подходящую беспроводную технологию.

5.1.4 Вариант клинического использования

Спрашивая у практикующих врачей, как они собираются использовать приборы, можно установить сетевой приоритет, закрепленный за прибором и/или клинической системой. Например, включает ли применение прибора архивацию данных или поддерживается ли режим реального времени, включающий в себя жизненно важную информацию, такую как аварийные сигналы от пациентов. Необходимо взаимодействовать с инженерами биомедицины, которые занимаются поддержкой клинических систем, чтобы понять, как они осуществляют свою деятельность. Узнавать, каковы их планы по техническому обслуживанию, включая усовершенствование приборов, и стремиться к установлению партнерства там, где над ПРОЦЕССАМИ и процедурами осуществляется совместное руководство, когда дело касается сети. Необходимо также установить, как конфигурируются устройства для доступа к сети. Итогом этих усилий станет четкое понимание сетевого приоритета, который необходимо назначить МЕДИЦИНСКОМУ ПРИБОРУ и системам, а также совместно установленные правила взаимодействия по отношению к управлению приборами и моделям клинической поддержки, связанной с сетью.

5.2 Беспроводные возможности МЕДИЦИНСКОГО ПРИБОРА

Исследование клинической функциональности сопряжено с необходимостью понять беспроводные возможности и характеристики производительности МЕДИЦИНСКИХ ПРИБОРОВ, приложений и систем. Взаимодействие с ПМП (производителем медицинских приборов) для полного понимания функциональных возможностей МЕДИЦИНСКОГО ПРИБОРА, связанных с беспроводной производительностью, является важным ранним шагом в проектировании и конфигурировании беспроводной сети. Комбинация понимания клинической функциональности вместе с характеристиками производительности беспроводной сети на уровне приборов позволяет установить базовые требования для проекта построения беспроводной сети.

5.3 Возможности МЕДИЦИНСКОГО ПРИБОРА и профиль сетевого трафика

Беспроводная технология определяет характеристики сети, которые устанавливают рамки для производительности МЕДИЦИНСКОГО ПРИБОРА в условиях беспроводной связи. Примерами могут служить:

- PHY (физический радиоинтерфейс): спецификации рабочих характеристик приемника, поддерживаемые типы модуляции и кодирования, скорость передачи данных, частоты и уровни мощности передачи;
- MAC (компонент канального уровня): детерминированный сетевой доступ против недетерминированного, функциональные возможности QoS, защита, передача обслуживания AP для автоматической настройки на местную сеть связи (роуминга) и механизмы экономии энергии;
- сеть (IP уровень): DHCP или BOOTP, подсеть или роуминг 3-го уровня, использование типов данных ШИРОКОВЕЩАТЕЛЬНОЙ И МНОГОАДРЕСНОЙ передачи;
- протокол транспортного уровня: TCP (ориентированный на соединение), UDP (без соединения);
- уровень приложения/прибора: типы трафика (в режиме реального времени, не в режиме реального времени), пропускная способность сети, механизмы экономии энергии, подтверждения более высокого уровня.

После того, как было установлено понимание функциональных возможностей и профилей трафика для МЕДИЦИНСКИХ ПРИБОРОВ, систем и/или типов приложений для применения беспроводной технологии, проектировщик сети может приступить к проектированию и конфигурированию проводной и беспроводной сети для надлежащей поддержки МЕДИЦИНСКИХ ПРИБОРОВ и систем.

5.4 Требования к производительности сети

МЕДИЦИНСКАЯ ИТ-СЕТЬ должна поддерживать требования к производительности, выставляемые системами МЕДИЦИНСКИХ ПРИБОРОВ, которые были установлены в процессе планирования и проектирования, если клиническая система стремится быть безопасной, защищенной и эффективной. После установления требований к производительности сети всех приборов их необходимо документально оформить, чтобы обеспечить основание для проведения испытаний до и после установки, и в случаях внесения изменения, которые могут повлиять на производительность системы. Изменения, которые могут повлиять на производительность прибора, включают в себя изменения фактической сетевой конфигурации, модификации RF среды и добавления приборов в сеть. Требования к производительности сети каждого прибора должны учитывать топологию сети и ее конфигурацию. Сеть должна проектироваться таким образом, чтобы удовлетворять требованиям к производительности сети наиболее чувствительного к производительности приложения/прибора в сети при придельной нагрузке сети. Список некоторых требований к производительности, которые следует учесть, включен в приложение В.

Проверенным методом является определение требований к производительности МЕДИЦИНСКОГО ПРИБОРА по спецификации прибора, отмечая самые строгие требования к производительности. Эти требования необходимо сопоставить с рабочими характеристиками (установленными и измеренными) сети (беспроводной и проводной). В качестве примера, допустим, что один производитель установил предельную нагрузку на сеть и предельное число пользователей на ТОЧКЕ ДОСТУПА (AP). Чтобы не достигать этих предельных значений, МО решает добавить дополнительные AP на местности, где будут использоваться приборы. Такая мера по УПРАВЛЕНИЮ РИСКОМ также, как правило, приводит к более высокоуровневому сигналу (и более высокому ОСШ (отношению шума и сигнала) — см. рисунок 4), так как AP располагаются ближе к клиентам. По причине уменьшения числа конфликтов, связанных с временем передачи, пропускной способностью, задержкой, потерей пакетов, все требования к производительности передатчика смягчаются за счет проектного решения. Использование средств контроля сети для контроля характеристик производительности сети, с генерацией сигналов тревоги в случаях, когда условия ухудшаются, является дополнительной мерой по УПРАВЛЕНИЮ РИСКОМ, предназначенной для поддержания SLA соглашений конкретных устройств.

5.5 Механизмы обеспечения КАЧЕСТВА ОБСЛУЖИВАНИЯ (QoS)

Механизмы КАЧЕСТВА ОБСЛУЖИВАНИЯ (QoS) предоставляют привилегированный доступ к сети в рамках технологии. Эти механизмы могут помочь в обеспечении способности сети соответствовать клиническим SLA, которые требуют клиенты с высоким приоритетом, что осуществляется предоставлением этим клиентам преимущественного доступа к сети в противовес клиентам низкого приоритета. Беспроводные технологии используют различные методы предоставления QoS, и поставщики, поддерживающие те же стандарты, могут по-разному реализовывать механизмы обеспечения QoS. Например, в сети 802.11, WI-FI МУЛЬТМЕДИА (WMM) предоставляет 4 класса обслуживания в качестве своей стандартной опции. В дополнение к этому некоторые поставщики обеспечивают формирование трафика (управление пропускной способностью) и/или запасное время передачи, используя собственные схемы. МО следует ВЕРИФИЦИРОВАТЬ наличие у беспроводной сети и ее клиентов (беспроводных клиентов) совместимых и последовательных решений обеспечения QoS. Более того, необходимо обеспечить эффективное применение политики QoS во всей сети. Это включает в себя все отображения QoS между проводными и беспроводными сетями.

Примером может служить МО, которая принимает решение предоставить гостевой доступ к беспроводной сети и желает получить гарантии того, что гостевой доступ в WLAN не затрагивает данные пациентов. МО уже использует QoS по 802.11e для сегментирования трафика в WLAN сети. Голосовые устройства и МЕДИЦИНСКИЕ ПРИБОРЫ находятся в одной голосовой категории QoS, в то время как видеотрафику назначается видеокатегория. SSID гостевого доступа и связанные с ним приборы попадают в категорию «best effort» и поэтому обладают более низким приоритетом доступа к WLAN. соединение типа

Если прибор или группа приборов не поддерживают QoS, то МО сегментирует неподдерживаемые приборы в отдельный диапазон или подгруппу каналов для обеспечения разделения на физическом уровне.

5.6 Функциональные возможности приемника

ОСШ принятого сигнала представляет собой соотношение мощности принятого сигнала и мощности RF шума на приемнике (см. рисунок 4). Минимальным значением ОСШ прибора, передающего

данные с определенной скоростью, является наименьшее значение ОСШ, позволяющее прием и декодирование принятого пакета при установленном или максимально возможном коэффициенте пакетных ошибок. Многие факторы влияют на определение требований прибора к ОСШ, но, при прочих равных условиях, чем ниже требования прибора к ОСШ, тем лучше прибор функционирует в условиях ухудшения RF сигнала. Минимальный уровень принимаемого сигнала является показателем мощности принимаемого сигнала, необходимой для того, чтобы прибор мог надлежащим образом декодировать сигнал при установленном коэффициенте пакетных ошибок. В случае ОСШ этим уровнем будет «С» (требуемый уровень сигнала) в ОСШ. На рисунке 4 точка доступа АР1 принимает сигнал с уровнем – 65 дБмВт и имеет значение ОСШ, равное 30 дБ. АР2 принимает сигнал с уровнем – 55 дБмВт и имеет значение ОСШ, равное 40 дБ.

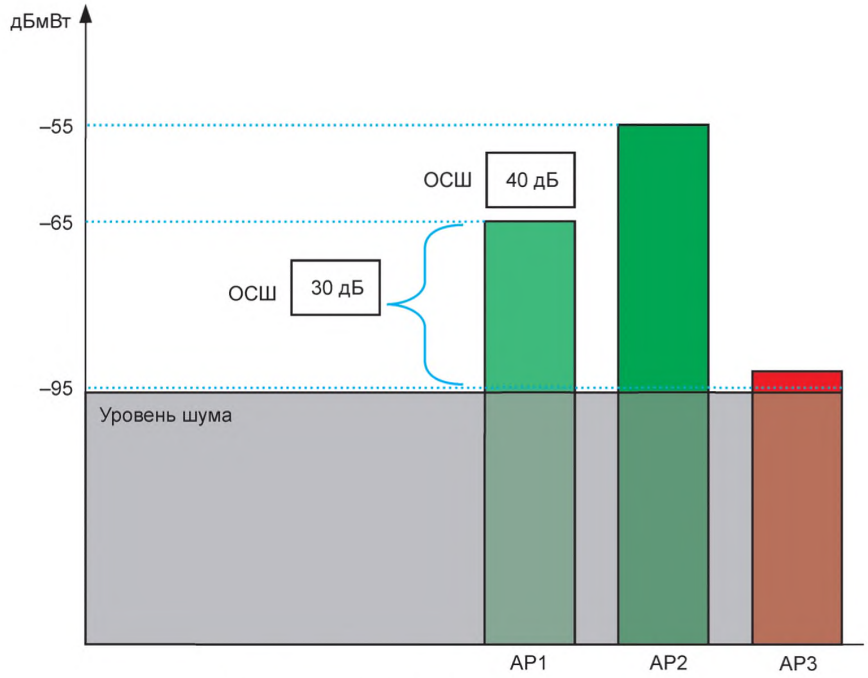

Рисунок 4 — ОТНОШЕНИЕ СИГНАЛ/ШУМ

5.7 Уровень принимаемого сигнала и ОСШ в сравнении со скоростью передачи данных

По мере того как уровень принимаемого сигнала (RSSI) и сопутствующее ему ОСШ уменьшается, максимальная скорость передачи данных, при которой приемник может успешно декодировать сигнал, также понижается. ОСШ — это величина или граница уровня сигнала, находящаяся над порогом чувствительности приемника или порогом шума (в зависимости от того, который находится выше). Принимая значения порога шума и чувствительности приемника равным – 88 дБмВт для 802.11 и значение RSSI равным – 65 дБмВт и получая результирующее ОСШ, равное 23 дБ (88 – 65 = 23), можно получить скорость передачи данных, равную 36 Мбит/с. При RSSI, равном – 82 дБмВт, и такой же чувствительности приемника (– 88 дБмВт) результирующее ОСШ, равное 6, означает, что приемник может поддерживать скорость передачи данных, только равную 6 Мбайт/с. Как бы там ни было, канал с низкой скоростью передачи данных может успешно принимать данные при более слабом сигнале на более далеких расстояниях от АР. Подобным же образом высокое скопление приборов, в особенности тех, что требуют высокой скорости передачи данных или очень низкой частоты возникновения ошибок, требует более высокого ОСШ. Поэтому приложения или приборы, которые существенно нагружают пропускную способность (видеопотоки) или для которых требуются низкие коэффициенты пакетных ошибок (трафик реального времени, такой как VOIP или потоковая передача данных пациентов, содержащих аналоговые сигналы), должны внедряться в среде с высоким ОСШ. Меры УПРАВЛЕНИЯ РИСКОМ по предоставлению избыточной емкости сети согласуются с концепцией предоставления ОСШ,

требующегося для наиболее эффективной возможной скорости передачи данных, в то же время они минимизируют влияние высоких уровней сигналов АР на общий фоновый RF шум.

МЕДИЦИНСКИЕ ПРИБОРЫ поддерживают разнообразные коммуникационные протоколы, в зависимости от своей конструкции и предназначения. Некоторые из протоколов общего уровня, которые можно встретить при работе с МЕДИЦИНСКИМ ПРИБОРОМ, это IP, TCP, UDP и протоколы более низкого уровня MAC. Типы трафика, которые могут влиять на производительность и требования беспроводной сети, являются различными вариантами использованиями ОДНОАДРЕСНОЙ, МНОГОАДРЕСНОЙ и ШИРОКОВЕЩАТЕЛЬНОЙ адресации. МЕДИЦИНСКИЙ ПРИБОР может использовать множество типов протоколов, типов трафика и других сетевых функций трафика в одном приборе. Например, сеть, осуществляющая контроль за пациентом, может использовать ШИРОКОВЕЩАТЕЛЬНЫЙ трафик для установления связи, ОДНОАДРЕСНЫЙ трафик для взаимодействия приборов и МНОГОАДРЕСНЫЙ трафик для взаимодействия множества приборов. Некоторые поставщики предоставляют ШИРОКОВЕЩАТЕЛЬНЫЙ/МНОГОАДРЕСНЫЙ трафик в виде множества ОДНОАДРЕСНЫХ сообщений (каждое для каждого связанного клиента) на АР. Такой тип взаимодействия может потребовать большую полосу пропускания беспроводной сети. Поставщики могут также улучшить доставку ОДНОАДРЕСНЫХ сообщений только тем клиентам, которым необходимо получить это сообщения, тем самым ограничивая использующуюся полосу пропускания беспроводного канала, в то же время получая надежную доставку подобных сообщений. С другой стороны, по умолчанию, ШИРОКОВЕЩАТЕЛЬНЫЕ и ОДНОАДРЕСНЫЕ сообщения не подтверждаются, поэтому доставка сообщения не подтверждается. Важно понимать и проектировать сеть для поддержания всех типов трафика, требующегося для МЕДИЦИНСКОГО ПРИБОРА, в то же время обеспечивая сосуществование медицинского трафика с сетевым трафиком других сетевых приборов. В проекте должны учитываться все типы данных и их коммуникационные протоколы.

Например, в сети 802.11 определенному МЕДИЦИНСКОМУ ПРИБОРУ требуется использование МНОГОАДРЕСНОЙ передачи, в то же время МЕДИЦИНСКИЙ ПРИБОР другого типа требует минимизации МНОГОАДРЕСНОГО трафика. Когда требуется МНОГОАДРЕСНЫЙ трафик, например, если какие-то приборы или приложения используют МНОГОАДРЕСНЫЙ трафик, то проектировщик сети должен понимать это требование, включить соответствующие версии IGMP и обеспечить поддержку на всем сетевом пути. Часто эти приборы имеют различные требования к МНОГОАДРЕСНОЙ передаче, поэтому конструкцией сети должно быть предусмотрена логическая изоляция приборов соответствующими методами. Как упоминалось ранее, сегментирование трафика с помощью SSID/VLAN считается наилучшей практикой лишь для небольшого количества приборов и SSID идентификаторов. Следует рассмотреть и другие, зависящие от поставщика, механизмы изоляции трафика в беспроводном канале.

5.8 Сравнение емкости, зоны покрытия и плотности расположения АР

Емкость, зона покрытия и плотность расположения являются взаимосвязанными факторами, которые необходимо учитывать при проектировании беспроводной сети:

- емкость связывает доступную полосу пропусканию с определенной географической местностью. На емкость влияет не только плотность расположения беспроводных ТОЧЕК ДОСТУПА, но и уровень сигнала, который напрямую связан со скоростью передачи данных;
- зона покрытия, как правило, указывает на возможности подключения беспроводного устройства к беспроводной сети, без каких-либо дополнений на доступную полосу пропускания;
- плотность развертывания АР связана как с емкостью, так и с зоной покрытия, так как чем более плотно развернута сеть, тем больше должна быть доступная емкость (не принимая во внимание зависимость от планирования каналов) и зона покрытия RF сигнала.

Установление уровня сигнала для заданной зоны покрытия больше не является достаточной мерой при проектировании сети. Требования емкости для этой области необходимо учесть и выполнить посредством обеспечения требующейся плотности расположения ТОЧЕК ДОСТУПА. Например, пункт медсестры может иметь множество беспроводных пользователей, собранных на маленькой физической территории. Если данные пользователи и связанными с ними приложения требуют совокупную пропускную способность сети в 45 Мбайт/с и одна АР сети 802.11 может предоставить практическую пропускную способность, равную приблизительно 15 Мбайт/с, то для поддержки приложения в данной физической области, не учитывая потребность избыточного обеспечения допустимой емкости, потребуется минимум три ТОЧКИ ДОСТУПА.

Примером сравнения зоны покрытия с емкостью является РАСПРЕДЕЛЕННАЯ АНТЕННАЯ СИСТЕМА, подключенная к АР 802.11 таким образом, что она предоставляет расширенную зону покрытия на целом этаже. Если это осуществляется посредством множества антенн и/или излучающего

коаксиального кабеля, то АР может стать открытой для большого количества приборов и пользователей. В данном примере высока вероятность того, что емкость данной АР будет превышена. Независимо от того, используется ли система DAS или рекомендованные производителем АР антенны, важно обеспечивать область правильным числом АР для достижения надлежащего распределения нагрузки. Иначе можно просто установить ТОЧКИ ДОСТУПА в стандартном отдельном развертывании, независимом от DAS.

Для случая сопоставления сотовой зоны покрытия и емкости поставщик сотовых услуг должен определить количество приборов, которые будут работать на предприятии, и соответствующим образом распланировать установку(и) микро- и пикоячеек. МО должен содействовать поставщику сотовых услуг в анализе типов приборов и приложений, которые будут действовать в сети, для обеспечения достаточной емкости для случаев пиковой нагрузки на сеть.

5.9 Сравнение детерминированных и недетерминированных беспроводных протоколов доступа

Детерминированный доступ работает таким образом, что приборам заранее предоставляется доступ к сети в предопределенные временные интервалы (т. е. распределенные специально предназначенные доли общей емкости). Недетерминированный доступ означает, что устройствам приходится соперничать и доступ в сеть не является гарантированной. Детерминированный протокол использует закрепленные временные интервалы, делая их неизменными в отношении сроков, так что пакету данных приходится ожидать своего собственного временного интервала для передачи, даже если никакие другие устройства не используют средства передачи данных.

Собственные протоколы имеют преимущество готового решения, которое выполняется поставщиком, но это также может быть и недостатком, так как МО может быть привязано к определенному поставщику. Протоколы, основанные на стандартах, как правило, могут выбирать из множества поставщиков, но требуют высокой степени компетенции МО при проектировании, развертывании и управлении сетью. Выбор между детерминированными и недетерминированными протоколами, основанными на стандартах и собственными или другими уникальными атрибутами протоколов, зависит как от доступных беспроводных технологий, так и от требований прибора. Детерминированное решение может предоставить более высокий уровень обеспечения доставки пакетов, но обладает менее эффективным использованием времени. В недетерминированной системе требуется избыточное обеспечение сети емкостью.

5.10 Сводная информация о планировании и проектировании

Определение требований МЕДИЦИНСКОГО ПРИБОРА к производительности сети, связанных с его использованием практикующим врачом, и отображение этих требований на функциональные возможности доступных беспроводных технологий являются основными выходными результатами этапа планирования. Соблюдение руководящих принципов, рассмотренных в данном разделе, создает прочную основу для мер по УПРАВЛЕНИЮ РИСКОМ, предназначенных для фактического проектирования беспроводной МЕДИЦИНСКОЙ ИТ СЕТИ.

6 Беспроводные МЕДИЦИНСКИЕ ИТ СЕТИ. Развертывание и конфигурирование

6.1 Сравнение РИСКОВ и преимуществ беспроводных коммуникационных систем

Необходимо рассмотреть РИСКИ, связанные с беспроводными коммуникационными системами, с учетом преимуществ, таких как повышенная мобильность пациентов, приборов и практикующих врачей с более быстрым доступом к данным. Многие РИСКИ не зависят от используемого беспроводного решения, скорее даже все беспроводные системы несут в себе внутренний РИСК, связанный с тем, что эти системы полагаются на среду, не ограниченную физически.

Например, хотя аутентификация пользователей требуется как для проводных, так и для беспроводных систем, невозможность гарантировать недоступность данных в беспроводных сетях для несанкционированного пользователя требует технического подхода, отличного от того, к которому можно прибегнуть в проводной LAN. Расположенные поблизости строительные площадки и другие электронные устройства, как правило, не влияют на соединения в проводной LAN, в то время как недавно возведенные стены могут блокировать сигналы для беспроводных соединений с LAN, а другие беспроводные устройства создают помехи.

Следует учитывать, что помимо беспроводных LAN существуют другие беспроводные технологии. Они включают в себя WAN, PAN и собственные технологии, каждая из которых демонстрирует свои характеристики, которые предприятие может пожелать задействовать в МЕДИЦИНСКИХ ПРИБОРАХ, подключенных к сети.

6.2 Лицензированный и нелицензированный спектр

Лицензированный спектр регулируется административными органами, которые устанавливают законы, диктующие, что или кто может использовать определенный диапазон или спектр. Сотовые системы действуют в рамках лицензированного спектра и им разрешено действовать с относительным отсутствием помех от других источников. Нелицензированный спектр подчиняется специальному регламенту, посвященному излучателям непреднамеренных помех, но спектр не ограничивается конкретными устройствами или беспроводными технологиями. Приборы, работающие в нелицензированном спектре, должны уметь сосуществовать с другими типами приборов и признавать определенный порог помех. Все возможные диапазоны спектра, рассматриваемые для использования, независимо от того, являются ли они лицензированными или нет, должны подвергаться оценке на месте расположения МО для определения уровней помех от всех источников. В дополнение к этому способность приборов работать при наличии помех следует рассматривать при АНАЛИЗЕ РИСКА беспроводной сети.

6.3 Источники помех

Применительно к использованию как лицензированного, так и нелицензированного спектра, выявление источников помех (например, микроволновых печей, приемопередатчиков, соседствующих WLAN) является трудной задачей и критически важным фактором для производительности беспроводной сети. Трудность заключается в том, что выявление и управление источником помех в лучшем случае является сложной задачей, но является критически важной, так как эти создающие помехи источники могут повлечь за собой отказ части всей беспроводной сети на неопределенное время. В общем, использование нелицензированного спектра имеет более высокую вероятность возникновения помех. И хотя источники помех наиболее вероятны в нелицензированном спектре, лицензированный спектр не защищен от помех. Распространенным источником помех в диапазоне 2.4 ГГц являются микроволновые печи. Политика оценки размещения микроволновых печей рядом с клиническими областями, на которых действуют МЕДИЦИНСКИЕ ПРИБОРЫ, является мерой по УПРАВЛЕНИЮ РИСКОМ. Данная оценка включает в себя испытание при наличии помех и использование новой модели микроволновых печей с пониженным RF излучением. В более общем случае источники помех на территории МО и за ее пределами должны быть известны и должны рассматриваться при АНАЛИЗЕ РИСКА беспроводной сети.

6.4 Использование и распределение спектра

6.4.1 Совместная работа приборов в общем спектре

Если приборы совместно работают в общем спектре, но использует разные беспроводные технологии, то системам следует иметь внутренние механизмы для защиты от радиочастотных конфликтов (например, использование обнаружения RF излучения и методы предотвращения влияния). Предпочтительной является способность разделять несовместимые беспроводные технологии, разделяющие общий спектр, посредством физического размещения. Приборы могут сосуществовать в одном физическом пространстве, работая в различных частях спектра (например, WMTS диапазоны сотовой связи и нелицензированные диапазоны). Как бы там ни было, во многих случаях это является непрактичным, так как многие приборы способны работать в одном спектральном диапазоне.

Если от приборов требуется совместная работа в общем физическом пространстве и в общем спектральном диапазоне (например, в U-NII диапазонах), то для выполнения надлежащего развертывания следует проводить оценку доступности и использования спектра. Это может как потребовать, так и не потребовать наличия раздельных инфраструктур. Для случая совместной работы в одной инфраструктуре разделение частот посредством грамотного планирования канала является средством обеспечения большей емкости без помех. Надлежащее планирование частот или управление каналом является незаменимым для увеличения емкости сети в физическом пространстве. Расширенные функции, такие как MIMO, формирования луча и умные антенны, могут обеспечить более эффективное повторное использование спектра и более низкий уровень помех, и если такие функции доступны, то следует провести оценку в контексте требований определенной физической области развертывания.

Следует обратиться к поставщику беспроводной сети и производителям прибора для получения информации о том, проводилось ли подтверждение на соответствие для подобных решений.

6.4.2 Управление спектром

Грамотное использование доступного спектра является краеугольным камнем успешного развертывания беспроводной МЕДИЦИНСКОЙ ИТ СЕТИ. Предпочтительно, чтобы распределение спектра основывалось на приоритете сетевого доступа и критичности клинических требований прибора. Например, если два приложения в сети ухудшают RF производительность друг друга, то МО следует подумать о том, чтобы отдать спектральное предпочтение приложению с более высоким приоритетом. Примером может служить развертывание приборов по 802.11. Использование U-NII диапазонов (5,150 — 5,875 ГГц) в дополнение к использованию 2,4 ГГц диапазонов и согласованное распределение приборов по этим диапазонам в зависимости от приоритета и вариантов клинического использования, является правильным механизмом для развертывания на всем доступном спектре.

Управление спектром требует понимания того, какие беспроводные технологии доступны и каковы их характеристики. Оно также требует понимания, какие из этих беспроводных технологий используются внутри здания МО и вокруг него. Обладая подобным пониманием, МО может грамотно определить места, где могут возникать помехи. Используя эту информацию, физическое разделение клинических приборов и/или разделение приборов по частотам может применяться для профилактики РИСКА RF помех. Если от приборов требуется совместная работа в общем физическом пространстве и в общих спектральных диапазонах, то должно осуществляться грамотное развертывание спектра и выделение каналов для обеспечения надлежащей производительности, необходимой для соответствия ПРЕДНАЗНАЧЕННОМУ ИСПОЛЬЗОВАНИЮ.

Иногда использование различных частей спектра вокруг здания МО, в особенности теми, кто не подчиняется администрации МО, может со временем изменяться. Адаптация к подобным изменениям при использовании спектра требует постоянного контроля RF среды и принятия корректирующих мер при необходимости для сохранения неиспользованных или менее использованных частей спектра для критически важных приложений МО.

6.4.3 Управление емкостью сети

Беспроводной спектр является конечным ресурсом, который необходимо распределять между приборами. Так как каждый прибор использует спектр и время передачи и получения информации, другим приборам приходится ждать своей очереди. Целью управления емкостью является обеспечение доступа к беспроводной структуре для всех приборов посредством их SLA. Некоторыми примерами методов достижения требующейся емкости сети является установка достаточного числа беспроводных ТОЧЕК ДОСТУПА и повторное использование частоты посредством грамотного планирования канала.

Управление и учет времени передачи (эфирного времени) для доступа к каналу на различных классах трафика является другим методом для управления емкостью и обеспечения соблюдения SLA соглашений. Изучение этих типов возможностей (некоторые из которых являются собственными) с поставщиком беспроводной сети является важной частью этапа планирования и проектирования.

6.5 Конфигурация беспроводной сети (для 802.11)

6.5.1 Общие положения

Конфигурация компонентов беспроводной LAN определяет способность сети обеспечивать безопасные и эффективные коммуникации.

6.5.2 VLAN и SSID

Логическое разделение приборов посредством VLAN сетей может обеспечить изоляцию в проводном сегменте сети. VLAN сети отображаются в беспроводную сеть посредством назначения SSID идентификаторов для расширения логической изоляции беспроводных приборов. Такая концепция является распространенной практикой для МЕДИЦИНСКИХ ПРИБОРОВ, предназначенной для ослабления нежелательного и потенциально несовместимого сетевого трафика и для предотвращения излишнего потребления энергии клиентами, которое может стать результатом получения нежелательного МНОГОАДРЕСНОГО или ШИРОКОВЕЩАТЕЛЬНОГО трафика.

Использование SSID для логического разделения приборов является мерой предоставления уникальных услуг (например, политики защиты) группам приборов, но не несет никаких других последствий, которые необходимо учитывать во время проектирования сети. Число возможных SSID идентификаторов ограничено, в особенности если сравнить его с числом возможных VLAN сетей. Увеличение числа SSID идентификаторов в той же физической инфраструктуре увеличивает простои

(увеличением количества отправляемых сигналов и т. д.) на беспроводных каналах, уменьшая доступную емкость, предназначенную для критически важных данных, и усложняя управление WLAN сетью.

Как было упомянуто ранее, VLAN не увеличивают стоимость для проводных сетей, но несут дополнительные издержки для беспроводных каналов при отображении VLAN в беспроводную сеть и поэтому требуют назначения уникального SSID для каждой WLAN в беспроводном канале. Каждый SSID привносит дополнительную загрузку сети в форме рассылки сигналов. Лучшая практика предполагает минимизацию и VLAN сетей, и SSID идентификаторов, и использование других методов разделения трафика, таких как назначение специальных спектральных диапазонов сетям WLAN (например, U-NII и ISM).

шифрование с использованием временных ключей

6.5.3 Аутентификация и шифрование

Система защиты беспроводной сети обеспечивает защиту от прослушивания (перехвата информации) и несанкционированного доступа к сети. Необходимо обеспечить поддержку минимально допустимого уровня защиты с помощью беспроводной технологии и реализовать наиболее высокий допустимый уровень защиты. Например, по причине числа известных уязвимостей, не рекомендуется использовать WEP в качестве механизма защиты для передачи данных о пациенте в сети типа 802.11. ПРОТОКОЛ ЦЕЛОСТНОСТИ ВРЕМЕННОГО КЛЮЧА (TKIP) — это механизм, задействованный протоколом ЗАЩИЩЕННОГО ДОСТУПА Wi-FI (WPA) и направленный на исправление недостатков, которые были у WEP, тем не менее, на сегодняшний день уже доступны более новые и предпочтительные методы. Сейчас Wi-Fi Alliance (объединение крупнейших производителей компьютерной техники и беспроводных устройств Wi-Fi) рекомендует WPA2 / 802.11i, который использует УСОВЕРШЕНСТВОВАННЫЙ СТАНДАРТ ШИФРОВАНИЯ (AES)[1)] в качестве функциональной возможности обеспечения минимума защиты. WPA2-Personal, который использует ПРЕДВАРИТЕЛЬНЫЙ КЛЮЧ (PSK), требует использования всеми пользователями одного общего ключа, что может ограничивать возможности и создавать технические трудности. WPA2-Enterprise, напротив, предоставляет множество разнообразных гибких механизмов аутентификации, основанных на РАСШИРЯЕМОМ ПРОТОКОЛЕ АУТЕНТИФИКАЦИИ (EAP) 802.1X, который может быть разным для каждого пользователя прибора. Для целей развертывания 802.11, WPA2-Enterprise предоставляет более высокий уровень защиты и управления доступом, чем WPA2-PSK. Существует большое количество специальных типов EAP, которые могут быть реализованы на различных устройствах, также как и поддерживаться в сети. Использование EAP решения, которое поддерживает двунаправленные (на сторону сервера и клиента) сертификаты, такие как EAP-TLS, считается более мощным, чем использование имени пользователя/пароля только для аутентификации стороны клиента, но в то же время представляет собой потенциально трудную задачу, связанную с генерацией и поддержанием большого числа сертификатов стороны клиента. Для того, чтобы установить необходимость дополнительного усложнения в виде реализации двунаправленных сертификатов, необходимо провести АНАЛИЗ РИСКА.

6.5.4 Собственные расширения поставщика

Многие, основанные на стандартах, беспроводные технологии, такие как 802.11, имеют собственные компоненты. Подобные собственные функции могут быть не совместимы с некоторыми устройствами и могут как положительно, так и отрицательно влиять на производительность МЕДИЦИНСКИХ ПРИБОРОВ. Важно понимать, как осуществляется управление данными функциями, так как это влияет на характеристики сетевой производительности МЕДИЦИНСКОГО ПРИБОРА. Примерами могут быть механизмы поддержки отслеживания активов и алгоритмы для настройки канала AP и передачи энергии. Необходимо взаимодействовать с поставщиком беспроводной сети для понимания влияния этих собственных функций, чтобы позволить конфигурации сети оптимально использовать такие собственные расширения.

6.5.5 Сотовые и собственные сети

Сотовые и собственные беспроводные сети либо управляются поставщиками услуг, либо предварительно конфигурируются, когда требуется минимум надзора со стороны МО или же он не требуется вообще. Это включает в себя управление конфигурацией и техническими характеристиками проводных сетевых устройств, таких как коммутаторы (центральные, распределительные и граничные), маршрутизаторы (направляющие пакеты данных между сетями LAN, или в сеть WAN, или в Интернет, и/или в сотовую сеть), управление уровнем защиты в пределах сети и некоторым числом МЕДИЦИНСКИХ ПРИБОРОВ, являющихся частью проводной сети. Настоящий стандарт не рассматривает непосредственно РИСК проводных сетей, но он имеет отношение к теме настоящего стандарта, так как большинство

[1)] http://www.wi-fi.org/files/kc/WPA-WPA2_Implementation_2-27-05v2.pdf.

беспроводных МЕДИЦИНСКИХ ПРИБОРОВ, так или иначе, подсоединяются к проводной сети для доступа к серверу, у которого, как правило, проводное соединение с сетью. Поэтому проводная сеть является частью всей медицинской сетевой системы и должна полностью учитываться в совокупном планировании и проектировании сети для обеспечения поддержки сетью клинических SLA МЕДИЦИНСКИХ ПРИБОРОВ.

Хотя МО не может нести ответственности за полное проектирование, реализацию и управление сотовыми и собственными беспроводными сетями, ей следует взаимодействовать с поставщиком услуг для определения и обеспечения соответствия сети требованиям подходящего SLA.

6.5.6 Доступность сети

Если доступность данных является критически важной, то сеть должна быть спроектирована с расчетом на быстрое восстановление после отказов компонентов. Построение сети с расчетом на избыточность и устойчивость для повышения доступности сети предотвращает остановку потока данных по причине отказов, связанных с одиночной неисправностью. Например, в критически важном приложении для непрерывного контроля пациента, если маршрутизатор или контроллер WLAN отказывает, должен существовать альтернативный путь для направления потока данных от пациента, практикующему врачу. В связи с разными уровнями РИСКА требование скорости восстановления для жизненно важных данных может отличаться от требования для данных общего назначения. Время восстановления для различных решений резервного копирования может колебаться от нескольких секунд до нескольких минут. Выбор лучшего решения резервного копирования зависит от стоимости реализации и вероятности возникновения ОПАСНОЙ СИТУАЦИИ (например, у пациента случается аритмия сердца в то время, которое необходимо для восстановления сети). АНАЛИЗ РИСКА применяется для того, чтобы определить, стоит ли устанавливать более быстрое и более дорогое решение резервного копирования.

В беспроводном пространстве или пространстве RF, использование перекрытия зон обслуживания предоставляет механизм обеспечения высокой доступности сети. Как обсуждалось в 6.4, грамотное использование RF каналов позволяет использовать RF избыточность. Например, ISM ДИАПАЗОН 2,4 ГГц имеет спектр 83 МГц, в то время как U-NII диапазоны 5 ГГц предоставляют спектр в 555 МГц. В случае 802.11 в США это означает наличие трех доступных неперекрывающихся каналов в спектре 2,4 ГГц и до 24 неперекрывающихся каналов в спектре U-NII. Из-за небольшого числа различающихся каналов в диапазоне 2,4 ГГц перекрытие зон обслуживания в большом физическом пространстве, где требуется большая емкость сети, не представляется оправданным при использовании 2,4 ГГц. Большее число доступных каналов в U-NII диапазонах 5 ГГц позволяет перекрытие зоны обслуживания RF и таким образом обеспечивает RF избыточность, что означает высокую степень доступности беспроводной сети.

6.6 Испытание для ВЕРИФИКАЦИИ

6.6.1 Общие положения

Использование испытания сети для ВЕРИФИКАЦИИ является лучшей практикой в индустрии, которая напрямую применима к успешному развертыванию и управлению беспроводной сетью. Испытание сети обнаруживает ошибки не только в 1) сетевом оборудовании и встроенном программном обеспечении или 2) ИНТЕРОПЕРАБЕЛЬНОСТИ между прибором и инфраструктурой, но также и в 3) конструкции, топологии и конфигурации сети, являющейся собственностью проектировщика/эксплуатационщика. Различая между разными сетями будут существовать всегда, и ни ПМП, ни производитель ИТ оборудования не обладают полным пониманием конструкции и повседневной эксплуатации, уникальной для больницы сети. В контексте конструкции, развертывания и конфигурации беспроводной МЕДИЦИНСКОЙ ИТ СЕТИ испытание для ВЕРИФИКАЦИИ является необходимой задачей.

Многие МО не имеют помещений и аппаратуры для создания лабораторной сети для проведения испытаний для ВЕРИФИКАЦИИ. Сегментирование части действующей сети для проведения на ней испытаний без подсоединения приборов к настоящим пациентам может служить подходящей альтернативой. Важным является предоставление полного доступа команде реализации (специалистам ИТ, биомедицины, практикующим врачам и т. д.) во время испытания для ВЕРИФИКАЦИИ, а возможность испытывать приборы и системы в фактической сети является довольно дорогой.

6.6.2 Испытание для ВЕРИФИКАЦИИ перед запуском в эксплуатацию

Использование лабораторной среды для имитации и ВЕРИФИКАЦИИ работы как МЕДИЦИНСКИХ, так и НЕМЕДИЦИНСКИХ ПРИБОРОВ в сети WLAN является важным компонентом мер по УПРАВЛЕНИЮ РИСКОМ. И хотя лабораторное испытание является хорошим показателем общей производительности, оно не может заменить испытание, проводимое в среде самой МЕДИЦИНСКОЙ ИТ СЕТИ,

так как лабораторная среда является лишь приближенной версией настоящего окружения. В дополнение к этому, ВЕРИФИКАЦИЯ должна также включать испытания для подтверждения предусмотренной конструкцией доступности сети в случае отключения от сети индивидуальных сетевых компонентов.

6.6.3 Испытание для ВЕРИФИКАЦИИ во время эксплуатации

После проведения автономного испытания для ВЕРИФИКАЦИИ изменения сети испытываются в реальных условиях эксплуатации. Подготовка к испытаниям включает создание плана установки для перехода на новое решение, который включает в себя план поддержки персонала (например, наличие дополнительных сотрудников) на случай, если усовершенствования не удастся осуществить, или включает время простоя сети[2)]. Это в свою очередь включает поддержку со стороны ИТ специалистов, практикующих врачей и инженеров биомедицины для испытания МЕДИЦИНСКИХ ПРИБОРОВ в действующей сети. Конфигурация приборов и сети, ожидаемое время простоя, персонал дополнительной поддержки и фактическое использование испытуемых приборов и сети врачами — все это следует включить в план установки испытания для ВЕРИФИКАЦИИ ВО ВРЕМЯ ЭКСПЛУАТАЦИИ. Для крупных развертываний, после успешно проведенных испытаний, может быть оправданным осуществление поэтапного введения в эксплуатацию. Например, система, занимающая множество этажей, может развертываться этаж за этажом.

7 Беспроводные МЕДИЦИНСКИЕ ИТ СЕТИ. Управление и поддержка

7.1 Общие положения

Данный раздел предоставляет обзор мер по УПРАВЛЕНИЮ РИСКОМ и лучших практик, связанных с управлением МЕДИЦИНСКОЙ ИТ СЕТЬЮ после развертывания и конфигурирования.

7.2 Сеть и управление приложениями

После того как планирование, развертывание и ВЕРИФИКАЦИЯ МЕДИЦИНСКОЙ ИТ СЕТИ были осуществлены, необходимо использовать инструменты управления сетью и приложениями для контроля и ослабления событий, ухудшающих производительность, и выходов сети из строя. Для определения требующейся области применения и масштаба инструментов и функциональных возможностей контроля сети необходимо провести АНАЛИЗ РИСКА. Следует рассматривать от простых мер по УПРАВЛЕНИЮ РИСКОМ, таких как SNMP ловушки, до крупномасштабных корпоративных инструментов сторонней организации. Целью следует сделать идентификацию ухудшения производительности до того момента, как оно предстанет в виде ОПАСНОЙ СИТУАЦИИ или ВРЕДА.

Использование контроля сети, как в беспроводных, так и в проводных инфраструктурах, объединенное с контролем на уровне приложений, может дать понимание работы сети в реальном времени. Контроль может также предупредить о снижении емкости сети или других проблемах, которые могут отрицательно сказаться на способности сети соответствовать требованиям SLA соглашений.

7.3 Правила и процедуры

Необходимо установить, документально оформить и распространить строгие правила и процедуры, касающиеся использования как беспроводной сети, так и RF среды. Правила должны уделять основное внимание ограничению использования (например, в зависимости от местности) беспроводных или других устройств, которые могут создавать помехи для устройств в беспроводной сети МО.

Примерами могут быть:

- местность, на которой могут использоваться личные устройства связи, такие как сотовые телефоны, Bluetooth наушники, DECT устройства или другие беспроводные телефоны;
- запрет индивидуального или группового использования мошеннических беспроводных сетевых устройств, таких как AP точки 802.11;
- выбор физического месторасположения и/или смены местоположения (например, для моделей, которые генерируют низкие уровни RF излучения/помех) имущества МО, которое может быть источником помех. Это, например, микроволновые печи, оборудование электрохирургии и т. д.

Необходимо документально оформить процедуры, которые описывают в общих чертах ПРОЦЕСС принятия соединения беспроводного устройства с сетью. Правилом должно быть установлено требование, согласно которому любые закупки беспроводных устройств, перед тем как покупка была

[2)] 10-шаговый процесс АНАЛИЗА РИСКА, описанный в МЭК/ТО 80001-2-1:2012, предоставляет шаблон, который можно использовать для установления ролей и ответственностей во время усовершенствования сети.

совершена, проверялись бы ИТ персоналом ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ. Правила должны быть как наглядно размещены для гостевых пользователей, так и распространены внутри компании.

7.4 Управление изменениями

Осведомленность и понимание возможного влияния изменений в МЕДИЦИНСКОЙ ИТ СЕТИ на производительность МЕДИЦИНСКИХ ПРИБОРОВ позволяет применять МЕНЕДЖМЕНТ РИСКА к ПРОЦЕССУ управления изменением. Примерами таких изменений могут служить изменения: версия программного обеспечения беспроводного контроллера, установка пакетов исправлений для программного обеспечения или изменение конфигурации сетевого компонента (следует отметить, что некоторые системы управления беспроводной сетью могут автоматически менять сетевые параметры устройств). Например, обновление встроенного микропрограммного обеспечения контроллера беспроводной сети для поддержания пакета исправлений защиты может исправить проблему в защите, но вызвать проблемы в другом месте сети в результате внесения дефекта программного обеспечения в новое программное обеспечение контроллера. Примером для аппаратных средств (оборудования) может служить усовершенствование АР до 802.11abgn от 802.11abg. Во всех этих случаях рекомендуется использование испытания для ВЕРИФИКАЦИИ перед ЗАПУСКОМ В ЭКСПЛУАТАЦИЮ в качестве части ПРОЦЕССА управления изменениями, как описано в 6.6.

Не рекомендуется усовершенствование до нового выпуска оборудования или программного обеспечения инфраструктуры сети без консультации с ПМП. Более ранние версии программного обеспечения имеют более высокую вероятность возникновения проблем производительности. Рекомендуется уточнить у ПМП, были ли завершены испытания для ВЕРИФИКАЦИИ рассматриваемых версий их приборов и программного обеспечения беспроводной инфраструктуры. Важно понимать, что с ростом количества оборудования и доступных версий программного обеспечения, предоставляемых как поставщиками сетевой инфраструктуры, так и ПМП, существует вероятность того, что не все комбинации будут подвергнуты испытаниям до развертывания конкретной комбинации в МО. Если желаемая комбинация еще не испытывалась, МО следует провести свою собственную ВЕРИФИКАЦИЮ.

Так как выпуск некоторых обновлений оборудования и программного обеспечения (в том числе и внутреннего) поставщиками беспроводных сетей, как правило, не привязан к конкретному графику (например, для обновлений системы защиты), может оказаться, что ПМП не смогут завершить подтверждение соответствия в сроки, затребованные МО. В своем АНАЛИЗЕ РИСКА МО следует учесть РИСК использования беспроводного сетевого программного обеспечения, которое не прошло испытания ПРОИЗВОДИТЕЛЕЙ МЕДИЦИНСКИХ ПРИБОРОВ на ИНТЕРОПЕРАБЕЛЬНОСТЬ. Если ни одну из этих ситуаций нельзя допускать, то МО следует завершить испытание для ВЕРИФИКАЦИИ самостоятельно.

Изменения в физическом окружении могут сказаться на зоне RF покрытия. Анализ и посещение объекта или использование инструментов управления RF для подтверждения соответствия зоны RF покрытия после любых изменений в окружении являются основными мерами УПРАВЛЕНИЯ РИСКОМ. Примеры включают реставрацию помещений или планировки этажей, на которых используются беспроводные сети с МЕДИЦИНСКИМИ ПРИБОРАМИ.

Добавление новых приложений, медицинских или немедицинских, может сказаться на производительности существующих сетевых устройств в разделяемом беспроводном окружении с ограниченной доступной пропускной способностью сети. Примерами могут служить включение гостевого доступа к WLAN и добавление устройств отслеживания/определения местоположения оборудования.

8 Общие меры УПРАВЛЕНИЯ РИСКАМИ

8.1 Общие положения

В предыдущих разделах рассмотрен ПРОЦЕСС, посредством которого может осуществляться планирование, проектирование, развертывание и управление беспроводной МЕДИЦИНСКОЙ ИТ СЕТЬЮ. Очевидно, что каждая сеть отлична от других, включая использование различных технологий и решений поставщиков. В данном разделе будет проведен обзор некоторых мер УПРАВЛЕНИЯ РИСКАМИ, которые можно применять к определенным технологиями или МО. Здесь также приведена сводка некоторых внутренних наилучших практик проектирования, рассмотренных в предыдущих разделах. При определении списка уникальных причин, уникальных для МО, следует рассмотреть список мер УПРАВЛЕНИЯ РИСКАМИ, представленный в настоящем разделе, на возможность его применения, а также может ли он помочь в заполнении пробелов АНАЛИЗА РИСКА.

8.2 Определение базовой производительности сети

Понимание характеристик производительности беспроводной технологии и их соответствия требованиям сетевых устройств к производительности сети является жизненно важным для обеспечения надлежащего развертывания МЕДИЦИНСКИХ ПРИБОРОВ в беспроводной инфраструктуре.

При группировании приборов все приборы разделяют общие функциональные возможности и требования к производительности сети. Разбиение каждой группы требований к производительности на конкретные характеристики беспроводной производительности, включая конфигурации WLAN, является рекомендованным методом для определения каждой группы. Следует проектировать беспроводную сеть с расчетом на соответствие требованиям наиболее строгих характеристик производительности прибора в каждой группе, тем самым неизбежно выполняя SLA менее требовательных к производительности сети устройств.

8.3 Учет уровня сигнала зоны покрытия при проектировании

Проверенным методом является использование беспроводных технологий, таких как 802.11, для развертывания беспроводной инфраструктуры таким образом, что минимум ее RSSI и ОСШ в предназначенной зоне покрытия будет выше установленной чувствительности приемника МЕДИЦИНСКОГО ПРИБОРА и ОСШ для наивысшей скорости передачи данных, поддерживаемой прибором. RF сигналы в реальных условиях, таких как больница, могут иметь уровни сигнала, отличающиеся друг от друга на 10 дБ в устойчивом состоянии, и испытывать замирание (снижение сигнала из-за эффекта многолучевого распространения волн) на 20 дБ или больше. Таким образом, если чувствительность приемника прибора для наивысшей возможной скорости передачи данных равна – 75 дБмВт (или 20 дБ ОСШ, если уровень шума равен – 95 дБмВт), то проект беспроводной сети должен обеспечивать зону покрытия – 65 дБмВт.

Другим способом является измерение уровня RF шума в области беспроводного покрытия в течение промежутка времени для идентификации наиболее неблагоприятных ситуаций и уменьшения мощности передачи беспроводных AP, и /или размещение AP ближе друг к другу так, чтобы уровень получаемого сигнала МЕДИЦИНСКОГО ПРИБОРА превышал чувствительность приемника с наивысшей скоростью передачи данных хотя бы на 10 дБ. На рисунке 4 демонстрируется графическое представление ОСШ.

8.4 Разделение трафика и типов данных

Типичной лучшей практикой является логическое сегментирование сети для ограничения (например, использование VLAN сетей) ШИРОКОВЕЩАТЕЛЬНОГО трафика до значения, предназначенного ему предметной областью или подсетью. Также эта лучшая практика, если типы трафика могут быть четко идентифицированы, может применяться для разделения жизненно важных данных и ИТ трафика общего назначения. После идентификации клинического использования МЕДИЦИНСКОГО ПРИБОРА и связанного с ней трафика (например, архивации данных и т. д.) необходимо установить поддерживаемые МЕДИЦИНСКИМ ПРИБОРОМ коммуникационные протоколы, режимы адресации (ОДНОАДРЕСНЫЙ, МНОГОАДРЕСНЫЙ, ШИРОКОВЕЩАТЕЛЬНЫЙ) и другую информацию по использованию протоколов. Необходимо также создать VLAN на проводном канале сети для различных классов МЕДИЦИНСКИХ ПРИБОРОВ и клинических данных, а затем отобразить МЕДИЦИНСКИЕ ПРИБОРЫ в беспроводной сети на соответствующую VLAN (например, в случае WI-FI идентификатор SSID отображается на конкретную VLAN).

8.5 Физические изменения и изменения в среде

Физические изменения в беспроводной среде (например, изменение планировки этажа) будут оказывать влияние на производительность RF системы беспроводных устройств. Блокирование или изменение пути RF сигнала может значительно сказаться на производительности беспроводного канала устройства. Возможной мерой по УПРАВЛЕНИЮ РИСКОМ для такого случая будет оценка всех физических изменений структуры в окружении МЕДИЦИНСКОЙ ИТ СЕТИ с целью получения надлежащего RSSI и ОСШ и проведение испытаний после любых изменений. Также следует передвигать или устанавливать дополнительную беспроводную инфраструктуру (например, точки AP) в соответствии с результатами исследования RF объекта или использовать другие средства.

8.6 Поддержание RF среды в «чистоте»

Для МО поддерживание RF среды в «чистоте» для существующей и управляющейся беспроводной сети(ей) является трудной задачей. Внешние помехи от соседствующих сетей, микроволновые печи, другие пользователи нелицензированного спектра (Bluetooth, DECT телефоны, Zigbee и т. д.) могут периодически появляться в управляемом МО RF пространстве. Периодические исследования физической зоны покрытия сети с использованием инструментов спектрального анализа для сканирования и идентификации источников помех являются одним из способов ослабления неизвестных и неуправляемых источников помех. Необходимо установить и документально отразить политику, которая запрещает использование источников помех или способствует их удалению (в зависимости от местоположения, если это возможно). Другим возможным способом ослабления помех является закрепление наименее нагруженных каналов за МЕДИЦИНСКИМИ ПРИБОРАМИ, независимо от того, находятся ли они в лицензированных или нелицензированных диапазонах.

8.7 Планирование емкости сети

8.7.1 Общие положения

Проектирование беспроводной сети, которая всегда поддерживает конкретную величину емкости, превышающую нагрузку пользователей, является трудной задачей, так как количественно определить загрузку сети большим количеством разнородных устройств за продолжительный промежуток времени практически невозможно. С вероятностной точки зрения загрузка, как правило, является случайным ПРОЦЕССОМ, распределенным по закону Пуассона, и может также включать в себя пространственно-временной разброс. Сложность количественно точного определения нагрузки является частью причины значительного ограничения на емкость сети (например, проектирование емкости, превышающей на 50 % требующуюся емкость, для предполагаемого использования). Если сеть является собственной разработкой, то управление емкостью может быть встроено в сеть (например, как в телеметрической системе, передающей информацию по беспроводному каналу).

Мера УПРАВЛЕНИЯ РИСКОМ для предотвращения перегрузки сети заключается в проведении испытания и ВЕРИФИКАЦИИ фактического влияния изменений в сетевом оборудовании и у клиентов сети. Для понимания соотношения требований приборов и приложений к емкости сети с емкостью зоны покрытия необходимо собрать спецификации рабочих характеристик как от ПМП, так и от поставщика беспроводной инфраструктуры. Одним из способов оценить емкость зоны покрытия сети является представление доступной полосы пропускания (в Мбит/с), приходящейся на единицу площади этажа. В качестве примера рассмотрим этаж больницы площадью 1000 кв. м. На этапе планирования и проектирования установлено, что объединенная требующаяся для всех приборов (как медицинских, так и немедицинских) пиковая емкость сети составляет 100 Мбит/с или 100 (Кбит/с)/кв. м (100 Мбит/с, распространяющиеся на весь этаж, равносильны 100 Кбит/с, приходящимся на каждый квадратный метр). Также установлено, что пункт медсестры потребляет наибольшую емкость на единицу площади и что для пункта медсестры потребуется пиковая емкость в 130 Кбайт/с на 1 квадратный метр. Во время планирования выбор беспроводной технологии сети 802.11 и двухдиапазонной AP сети 802.11 должен обеспечить реальную емкость 20 Мбит/с в U-NII диапазонах 5 ГГц сети 802.11a и 6 Мбит/с в ISM ДИАПАЗОНЕ 2,4 ГГц сети 802.11bg. Проектировщик сети решает установить достаточное число AP точек на всем этаже, чтобы выполнить требования к емкости, представленные пунктом медсестры (альтернативой данному решению может быть добавление AP только на площади пункта медсестры). Если расширить требования к емкости до 130 Кбит/с на 1 кв. м для всего этажа и проектировать WLAN с 50 %-ным запасом емкости, то получаем проект зоны действия WLAN, для которой требуется совокупная емкость 260 Кбит/с на 1 кв. м или 260 Мбит/с. Для удовлетворения этого требования при развертывании используется 10 точек AP (200 Мбит/с для сети 802.11a и 60 Мбит/с для сети 802.11bg). Если принять, что развертывание и конфигурация (например, назначение каналов и т. д.) приборов проведены с расчетом на эффективное использование обоих диапазонов и зона RF покрытия AP точек подтверждена посредством инструментов исследования объекта, то проект развертывания является подходящим для данного случая и готов к испытаниям и ВЕРИФИКАЦИИ.

8.7.2 ГГц и ДИНАМИЧЕСКИЙ ВЫБОР ЧАСТОТЫ (DFS)

В каждой стране установлены свои правила и регламент, касающиеся использования нелицензированного спектра. Доступные каналы и повторное использование спектра могут варьироваться от страны к стране. Например, некоторые каналы 5 ГГц запрещены на тех территориях, где они могут создавать помехи для радарных систем, для которых предназначен данный диапазон. МО может провести

расследование совместно с местными органами власти, чтобы установить наличие радиолокационных станций рядом со зданием организации. В дополнение к этому инфраструктурное устройство, такое как AP 802.11, которое использует DFS канал, должно осуществлять поиск радаров и предотвращать помехи в случае обнаружения их источников. Большинство AP точек и сетей WLAN оповещают об этом и представляют отчеты, содержащие информацию об обнаружении радара и активации DFS системы. Если стало известно, что поблизости находятся радиолокационные станции, то подверженные их влиянию каналы 802.11 может потребоваться отключить вручную. Это необходимо по той причине, что DFS останавливает работу AP точки на канале, подверженном помехам, и любые клиенты, соединенные с этой AP, могут потерять соединение с сетью и возможность подключения к ней на длительный период времени (может длиться как секунды, так и минуты, в зависимости от действий клиента). Это будет происходить до тех пор, пока они не смогут переподключиться к той же AP или к соседствующей с ней и работающей на канале, не затронутом помехами.

8.7.3 Меры обеспечения защиты и планирование

Дополнительную информацию по обеспечению защиты беспроводных коммуникаций можно найти в стандартах по ОЦЕНКЕ РИСКА системы защиты, таких как ИСО/МЭК 27001:2005, ИСО/МЭК 27002:2005, ИСО/МЭК 15408-2:2008 и т. д. Беспроводные коммуникационные технологии включают множество технических средств управления защитой, поэтому следует ознакомиться со спецификациями каждой технологии (например, 802.11, Bluetooth и т. д.). Руководство по РИСКАМ защиты при присоединении МЕДИЦИНСКИХ ПРИБОРОВ к ИТ СЕТЯМ можно найти в МЭК/ТО 80001-2-2, содержащем описание нужд системы защиты МЕДИЦИНСКОГО ПРИБОРА, РИСКОВ и средств управления ими.

Защита уже была важным и приоритетным предметом для ИТ СЕТЕЙ еще до появления МЕДИЦИНСКИХ ПРИБОРОВ. Защищаемая информация о здоровье в любой сети требует серьезных мер обеспечения защиты. Это в особенности актуально для беспроводных сетей. Оценка каждого канала в цепи коммуникаций для обнаружения дефектов в системе защиты и определение соответствующих ответных мер должны быть частью процесса проектирования и планирования сети WLAN. Необходимо использовать состоятельные механизмы шифрования и аутентификации, такие как AES и 802.1X. В дополнение к этому, использование IDS/IPS может быть оправдано для обнаружения многих механизмов беспроводного проникновения в сеть и защиты от них. Если устаревшие устройства, поддерживающие более низкие уровни шифрования, необходимо включить в состав сети, то проект сети должен предусматривать ограничение сетевого доступа для таких устройств. Например, инфузионным насосам, имеющим слабые механизмы защиты, следует предоставлять доступ только к одному серверу обновления справочника, ограничивая место возникновения РИСКА нарушения в защите сети одним сервером.

8.8 Использование RF спектра

Несмотря на то что доступный спектр является ограниченным и ценным ресурсом, грамотное планирование и использование RF спектра в МО часто пренебрегается. В АНАЛИЗЕ РИСКА следует рассматривать весь спектр и все связанные с ним беспроводные технологии, доступные для МО. Следует изучить природу помех и вероятность их возникновения, продумать поддержку для пиковой нагрузки трафика и способность технологии выполнять свою работу при наличии ожидаемых источников помех. На большинстве территорий лицензированный спектр обладает меньшей вероятностью возникновения помех, чем нелицензированный. Как бы там ни было, некоторые поставщики лицензированного спектра (например, сотовой связи) проектируют с расчетом на средние нагрузки, но не пиковые нагрузки. В случае нелицензированного спектра, рекомендуется использование менее нагруженного спектра или спектра с большей пропускной способностью.

Например, анализ емкости сети может указать на использование U-NII диапазона (5 ГГц) с пропускной способностью 555 МГц вместо использования ISM диапазона 2,4 ГГц и пропускной способности всего лишь 83 МГц. Каждый диапазон спектра имеет свои «за» и «против», которые следует тщательно проверять на соответствие RF требованиям.

Например, МО следует проанализировать необходимость использования DFS каналов U-NII диапазона, так как помехи от радаров могут привести к временной потере связи и другим нарушениям работы сети, связанным с нарушениями во вторичной сети, происходящими, когда AP точки, подверженные помехам, неожиданно сменяют каналы.

8.9 Классификация приборов и приложений

Когда в одной сети сосуществуют сильно отличающиеся друг от друга устройства с различающимися требованиями к производительности, классификация, основанная на политике защиты и требова-

ниях к производительности, является полезным инструментом управления сетевым доступом. В случае МЕДИЦИНСКИХ ПРИБОРОВ, для которых производительность и доступность сети могут быть связаны с осложнениями, влияющими на БЕЗОПАСНОСТЬ, способность классифицировать беспроводные МЕДИЦИНСКИЕ ПРИБОРЫ как приборы более высокого сетевого приоритета доступа является даже более важной и жизненно важной задачей. Следует рассмотреть выбор беспроводных технологий и решений инфраструктуры, которые могут различать передачи пакетов данных разных приоритетов и управлять ими. Подобные механизмы обеспечения КАЧЕСТВА ОБСЛУЖИВАНИЯ (QoS) следует изучать на стадии планирования и проектирования и реализовывать во всей сети.

Также следует рассмотреть механизмы, которые позволяют обнаруживать и предотвращать неправильное использование меток QoS для получения недозволенного доступа к беспроводной полосе пропускания. Например, пакет данных с низким приоритетом помечается как пакет данных высокого приоритета и получает привилегии, которые ему не полагаются. Это может сказаться на SLA соглашениях для трафика с высоким приоритетом. Обнаружение и предотвращение подобного неправильного использования QoS помогает выполнять SLA соглашения. Чтобы разобраться с подобными типами функциональных возможностей, необходимо обратиться к поставщику беспроводной инфраструктуры сети.

8.10 Гостевой доступ или доступ с помощью смартфонов

Большинство корпоративных сетей 802.11 применяют ту или иную функциональную возможность для обеспечения соблюдения распределения пропускной способности. Например, полоса пропускания для пользователей-гостей должна быть минимальна, сохраняя большую часть полосы пропускания для приложений, имеющих значение для жизни и миссии. Даже в случае МЕДИЦИНСКИХ ПРИБОРОВ или медицинских приложений смартфонов клиническая функциональность того, «как» используется приложение, должна учитываться при проектировании на уровне системы. Если терапевт хочет воспользоваться своим смартфоном для немедицинских целей, находясь в здании МО, то трафик от его/ее устройства должен быть изолирован либо с помощью SSID гостевого доступа, либо отдельного SSID, предназначенного для приложений смартфонов. Независимо от этого необходимо понимать клиническую функциональность устройств, принадлежащих этому SSID, и учитывать эти устройства в АНАЛИЗЕ РИСКА и при проектировании. При ограничении использования пропускной полосы до одного прибора или приложения должна учитываться клиническая функциональность, а не предпочтения пользователя, касающиеся широковещательного доступа. Если требуются более высокие уровни широковещательного доступа для поддержания гостевого доступа и приложений смартфонов, то могут потребоваться другие средства УПРАВЛЕНИЯ РИСКОМ. Примеры подобных средств рассматривались в настоящем стандарте, например увеличение числа AP точек и расширенное использование спектра 5 ГГц.

8.11 Конфигурация инфраструктуры WLAN

Администратору МЕДИЦИНСКОЙ ИТ СЕТИ МО следует ожидать, что ему может потребоваться внести некоторые изменения или создать некоторый уровень настройки конфигурации беспроводной инфраструктуры. Большинство решений беспроводной инфраструктуры сопровождается подробными руководствами и наборами лучших практик. Чтобы изучить функциональные возможности беспроводной сети и способы грамотной конфигурации системы с расчетом на максимальную производительность и доступность, соответствующий персонал должен пройти необходимое обучение. После того как понимание конфигураций достигнуто, для них можно сформировать соответствующие требования приборов МЕДИЦИНСКОЙ ИТ СЕТИ к производительности сети. Эти требования включает в себя характеристики производительности сети, такие как задержка и потеря пакетов данных, положение о защите и любую конфигурацию, требующуюся для обеспечения совместимости МЕДИЦИНСКИХ ПРИБОРОВ и беспроводной сети. Выполнение SLA соглашений всех приборов является задачей, которая потребует нахождения компромисса между клиническим приоритетом, ресурсами и бюджетом, и все это должно учитываться в ПРОЦЕССЕ МЕНЕДЖМЕНТА РИСКА.

8.12 Внешние партнерские отношения как с производителем МЕДИЦИНСКОГО ПРИБОРА, так и с производителем сетевых устройств

Развитие отношений с ПМП, так же как и с поставщиком МЕДИЦИНСКОЙ ИТ СЕТИ, на сегодняшний день является важным аспектом проектирования и сопровождения МЕДИЦИНСКОЙ ИТ СЕТИ. Необходимо взаимодействовать как с поставщиком беспроводной сети, так и с ПМП для получения понимания инфраструктуры и требований, и функциональных возможностей на уровне устройств, а также

для совместного со всеми заинтересованными сторонами анализа конфигураций устройств и WLAN сети. В идеальной ситуации параметры формализуются в СОГЛАШЕНИЯХ об ОТВЕТСТВЕННОСТИ. После анализа и принятия предложенной конфигурации всеми ответственными сторонами неотъемлемой частью ПРОЦЕССА АНАЛИЗА РИСКА является проведение испытаний сети WLAN и конфигураций приборов в лабораторных условиях для оценки совместимости и измерения производительности.

Необходимо отметить, что это дополняет внутренние партнерские отношения, необходимые для МО, включая партнерство между инженерами биомедицины, сотрудниками службы безопасности, практикующими врачами и менеджерами риска.

8.13 Резервирование

Резервирование является наилучшей практикой, применяющейся в проводных и беспроводных сетях. Развертывание беспроводной сети таким образом, чтобы каждая область покрывалась хотя бы двумя приемопередатчиками, работающими на разных каналах, обеспечивает резервирование сети. Подобная стратегия развертывания возможна только при наличии достаточного числа каналов. Более того, если подобные приемопередатчики подсоединены к разным матрицам сетевого коммутатора, то единичный отказ коммутатора не приведет к потере работоспособности всей беспроводной сети.

Например, при использовании сети 802.11, работающей в ISM ДИАПАЗОНЕ 2,4 ГГц, имеется, в лучшем случае, в зависимости от регулятивного домена[3)] три раздельных доступных частотных канала в 802.11. В физическом пространстве с большим числом областей с перекрытием зон обслуживания AP недостаток раздельных каналов может привести к более частому появлению межканальных помех. Применение RF резервирования в таком случае приведет к уменьшению совокупной емкости сети. Метод ослабления негативных последствий в таком случае заключается в перемещении критически важного трафика в диапазоны U-NII 5 ГГц, где доступно до 24 раздельных каналов типа 802.11. Вместе с этим большим числом раздельных каналов при грамотном развертывании сети физически перекрывающиеся зоны обслуживания AP обеспечивают увеличенную емкость, так же как и резервирование RF. С добавлением большего числа AP мощность передатчика AP и клиента так же может быть уменьшена для поддержания достаточно плотного развертывания AP.

[3)] Страны, совместно использующие общий регламент радиосвязи, определенный одним из регулятивных органов (основные регулятивные органы: FCC, ETSI, TELEC).

Приложение А
(справочное)

Варианты клинического использования и профили сетевого трафика

Таблица, приведенная ниже, содержит примеры вариантов клинического использования и демонстрирует их отображение на профили сетевого трафика. Данная таблица рассматривается в качестве общего подхода, с помощью которого ИТ специалисты смогут установить конкретные варианты клинического использования, соответствующие их МО, и отобразить их в своем общем плане проектирования и реализации сети. Важно понимать, что фактический вариант клинического использования может значительно поменять степень тяжести отказов, показанных в нижеприведенных примерах, что в свою очередь может сказаться на профиле сетевого трафика. Например, телефон VOIP, использующийся для коммуникаций общего назначения не требует приоритета выше среднего, но если этот телефон используется для передачи сигналов тревоги или аварийных сигналов о состоянии пациента и опасных событиях, то его приоритет становится высоким.

Таблица А.1 представлена исключительно в справочных целях, так как МЕДИЦИНСКИЙ ПРИБОР может обладать множеством разных клинических и сетевых профилей. Так же не предполагается, что в данной таблице представлены все варианты использования МЕДИЦИНСКОГО ПРИБОРА.

Важно обратить внимание на то, что более детальные характеристики трафика (например, размер пакета данных и определение временных соотношений) по сравнению со средней нагрузкой на прибор или реализуемым приложением, также является критически важными факторами в определении требований к производительности сети. Например, устройство VOIP, использующее CODEC G.711 располагает пропускной способностью 64 Кбайт/с, что близко к «низкой» категории пропускной способности. В то же время, по причине того, что оно использует скорость передачи пакетов равную 50 пакетам в секунду, влияние на совокупную пропускную способность сети гораздо более значительно. Таким образом, для некоторых случаев, таких как трафик VOIP устройства, понимание и планирование с расчетом на требования более высокой пропускной способности сети, вызванные высокой скоростью передачи пакетов, должно учитываться при проектировании сети в процессе обеспечения ее производительности.

Т а б л и ц а А.1 — Примеры вариантов клинического использования и профилей трафика

Пример медицинских приборов	**Тип данных**	**Вариант клинического использования**	**Уровень РИСКА (например, установленный в ходе пошагового ПРОЦЕССА). Использовать обозначения: высокий, умеренный и низкий**	**Профиль сетевого трафика**			
	***Тип данных + вариант клинического использования* определяют уровень РИСКА**			Пропускная способность	Допустимая задержка	Тип	TCP/ UDP
Прибор контроля пациента, устройство проверки на месте	Сигналы тревоги и аварийные сигналы	ЧДД, пульс/сердцебиение, давление, температура, SpO2, дефибриллятор/системы поддержания жизни/ оборудование поддержания жизни	Высокий	Низкая	Низкая	ОДНОАДРЕС./М. АДРЕС/ ШИРОКОВЕЩ.	TCP/ UDP
	Формы сигналов	Анализ на центральной станции, отслеживание тенденций, ведение записей	Умеренный	Низкая	Средняя	ОДНОАДРЕС./М. АДРЕС/ ШИРОКОВЕЩ.	TCP/ UDP
	Данные пациента	Наблюдение пациентов (удаленно в больнице)	Умеренный	Низкая	Средняя	ОДНОАДРЕС./М. АДРЕС/ ШИРОКОВЕЩ.	TCP/ UDP
		Наблюдение пациентов (на дому), контролирующееся для отчетности		Низкая	Высокая	ОДНОАДРЕС./М. АДРЕС/ ШИРОКОВЕЩ.	TCP/ UDP

Расшифровка обозначений параметров сетевого профиля представлена в таблице А.2.

Т а б л и ц а А.2 — Параметры сетевого профиля

	Низкая	Средняя	Высокая
Пропускная способность (кбит/с)	<50	>200	>1000
Задержка (с)	<1	1<X<10	>10

Приложение В
(справочное)

Вопросы к рассмотрению

В настоящем приложении приведен список вопросов, которые должна рассмотреть медицинская организация (МО) и которые являются исходными для формирования дополнительных вопросов, ориентированных на конкретных заказчиков, необходимых для выполнения АНАЛИЗА РИСКОВ МО. Настоящее приложение следует рассматривать в качестве руководства по составлению набора параметрических данных, которые могут использоваться для определения ПРОЦЕССА АНАЛИЗА РИСКА.

Сеть

1) МО предпочитает создание отдельной сети для каждого приложения или одной сети, которая поддерживает множество приложений?

a) Если на одну сеть приходится одно приложение, как будет осуществляться управление множеством сетей?

b) Если имеется одна сложносоставная сеть, то какое технологическое решение поддерживает большинство приложений в рамках данной сети? Как будут разрешаться конфликты использования одной сети для разных интересов?

2) Как будет обеспечена требующаяся доступность к сети (например, поддерживает ли топология сети средства ослабления последствий в случае отказов от одиночного сбоя как для проводных, так и для беспроводных LAN сегментов)?

3) Как топология сети поддерживает масштабируемость и как она влияет на мобильность устройств; например, имеются ли разные подсети для разных этажей или зданий?

4) С какой совокупной нагрузкой сталкивается каждое устройство для подключения к сети и достаточна ли емкость восходящего/нисходящего каналов связи?

5) Какие применимые лабораторные и клинические испытания были проведены?

6) Какова задержка в сети и соответствует ли она требованиям устройств и приложений?

7) Каковы искажения сети и соответствует ли они требованиям устройств и приложений?

8) Какие решения применяются для обеспечения QoS?

9) Какой уровень надежности (достоверности) данных будет поддерживать установленная сеть?

10) Какое максимальное число устройств, максимальное число передаваемых пакетов данных в секунду и максимальная пропускная способность, которую может поддерживать индивидуальная AP, и для какой скорости передачи данных установлены эти максимальные значения?

11) Какое максимальное число устройств, максимальное число пакетов данных в секунду, и максимальная пропускная способность, рекомендованные поставщиком, которые индивидуальная AP должна поддерживать при худшей скорости передачи данных в МО? Для всей системы в целом? Обратите внимание, что различные поставщики WLAN и различные ПМП могут рекомендовать различные максимальные ограничения. Предпочтительно, предоставление ПМП и поставщиками WLAN логического обоснования для этих ограничений, такого как «максимальная нагрузка определена как надежная». Если у каждого из поставщиков есть свои собственные рекомендации, связанные с максимальной нагрузкой, то следует придерживаться минимальной из них.

12) Какую максимальную пропускную способность должна поддерживать индивидуальная AP для ожидаемого типа и числа клиентов, связанных с данной AP? Для системы в целом?

13) Вопросы, связанные с физическим использованием МЕДИЦИНСКИХ ПРИБОРОВ:

a) Где физически будут применяться приборы? На всей площади предприятия или в определенном отделении?

b) Где в клиническом пространстве будут использоваться приборы? Будут ли они отключаться от энергопитания, передвигаться или находиться вблизи другого оборудования?

c) Данные, поступающие от медицинских приборов, считаются жизненно важными?

d) Будет ли прибор передвинут в результате выполнения технического обслуживания?

14) Каков реальный резерв емкости для принятой в МО нагрузки на беспроводную сеть?

15) Как много AP точек требуется для поддержания необходимой нагрузки на каждом отдельном участке больницы, учитывая:

a) число клиентов;

b) пиковую скорость передачи данных;

c) среднюю скорость передачи данных;

d) зону RF покрытия (минимальный допустимый уровень сигнала).

16) Требуется ли избыточное RF покрытие? Включено ли размещение дополнительных точек доступа в проект областей с высокой плотностью расположения устройств и областей критически важной зоны покрытия для обеспечения запаса безопасности?

17) Какие инструменты для обнаружения проблем в сети и тенденций ухудшения производительности доступны?

a) Как долго хранятся записи данных?

b) Позволяют ли хранящиеся данные осуществлять отладку системы для устранения проблем?

c) Какие оповещения доступны?

18) Были ли установлены соответствующие инструменты для измерений и контроля емкости беспроводной сети, осуществляемых как систематически, так и для каждой отдельной АР?

19) Каким образом осуществляется сбор и анализ показателей производительности беспроводной сети?

20) Планируется ли установка каких-либо АР контроля сети?

21) Каким образом устанавливаются и поддерживаются требования к RF покрытию?

22) Как устанавливаются пороговые значения; каким образом осуществляется доставка оповещений о сбоях и кому доставляются подобные оповещения; каково время ответных действий? Каким образом оно документируется?

23) Каким образом документально оформляется обследование объекта (площадки, на которой будет производиться развертывание сети)? Как оно может быть сопоставлено с RF покрытием в будущем?

24) Каким образом может осуществляться контроль изменений производительности RF сети в течение продолжительного периода времени и насколько устойчива беспроводная сеть в управлении изменения в среде? Принимают ли конечные устройства активное участие в адаптации механизмов адаптации сети?

25) Какое обучение доступно? Предоставили ли поставщики надлежащее обучение для грамотного управления, конфигурирования и использования беспроводной сети?

26) Существуют ли приложения, динамически влияющие на работу АР, например, использующие АР как сетевой анализатор пакетов, применяющие АР для отслеживания различных средств, внеканального сканирования?

27) Какие каналы будут использоваться и как распределяется набор каналов между АР?

28) Какая мощность передачи АР используется для типичного использования и для случая обследования объекта?

29) Достаточна ли мощность передачи АР для всего предназначенного диапазона частот и физических режимов передачи данных (скорость передачи данных, тип кодирования и модуляции, пропускная способность канала)?

30) Какова чувствительность приемника АР для предназначенных физических режимов передачи данных (скорость передачи данных, тип кодирования и модуляции, пропускная способность канала)?

31) Устойчивы ли к другим сигналам в спектре используемые физические и MAC (например, QoS) режимы передачи данных и их настройки?

32) Осуществляет ли система управления мощностью передачи с целью минимизации помех?

33) Если решение (технология) предоставляет гостевой доступ, то может ли осуществляться управление пропускной способностью и на каком уровне (АР/системы/пользователя)?

34) Позволяет ли решение конфигурировать параметры WLAN (например, DTIM интервал, поддержку 802.11h, аутентификацию/шифрование, RADIUS-сервер, и т. д.) для каждого SSID?

35) Требует ли инфраструктура различные ESSID для каждого типа аутентификации/шифрования?

36) Как регулируется число приборов для обеспечения достаточной емкости сети? Может ли это число регулироваться на основании типа прибора, таком как ограничение числа VoIP звонков?

37) Как осуществляется управление контролем доступа к очередям высокого QoS?

38) Как решение позволяет МО соответствовать требованиям HIPAA?

a) Какие решения защиты данных поддерживаются?

b) Какие решения защиты сети поддерживаются?

c) Поставщик использует подтвержденное, стандартизированное решение для аутентификации и шифрования?

d) Какие решения доступны для защиты сети в случаях, когда устройства с меньшими функциональными возможностями защиты должны быть допущены в сеть?

39) Какая конфигурация сети необходима для поддержания МНОГОАДРЕСНОЙ/ШИРОКОВЕЩАТЕЛЬНОЙ передачи пакетов различными устройствами?

40) Каким образом на конечных устройствах используется или воспринимается широковещательный/многоадресный трафик и как он обрабатывается в беспроводном канале? Была ли проведена оценка влияния использования широковещательного, многоадресного и одноадресного трафика на общую емкость беспроводного канала?

41) Какая конфигурация сети необходима для обеспечения защиты соединений с непрерывными данными в реальном времени от прерываний другими системными операциями сети? Как эта конфигурация сети сказывается на других системных операциях и на поддержке других клиентов?

42) Кто отвечает за техническое обслуживание сети?

43) Документируется ли процесс управления изменениями в беспроводной сети?

44) Как различные отделения разрешают конфликты, связанные с их приоритетами сетевых обновлений?

45) Каким образом устанавливается новое встроенное программное обеспечения для сетевых компонентов и осуществляется резервное копирование существующего встроенного ПО?

46) Каким образом изменяется конфигурации сетевых компонентов и осуществляется резервное копирование существующей конфигурации?

47) Как можно восстановить предыдущую конфигурацию сети или предыдущую версию встроенного ПО?

48) Как много времени занимает установка усовершенствований для внутреннего ПО на каждой АР и контроллере?

49) Какие аспекты решения основаны на стандартах, а какие являются собственными, и каким образом было проведено подтверждение соответствия для правильного функционирования данных решений? Например, алгоритмы, которые управляют каналами АР и мощностью передачи, могут быть собственными.

Приборы

1) Какие приборы будут работать в сети на разных участках больницы?

2) Какова критическая важность каждого приложения?

3) Какова допустимая потеря данных?

4) Какие SLA и сетевые требования указаны ПРОИЗВОДИТЕЛЕМ МЕДИЦИНСКОГО ПРИБОРА для каждого прибора (и, быть может, для каждого приложения, работающего на каждом приборе)? Примерами могут быть:

a) пропускная способность, пиковая и средняя в битах в секунду;

b) число пакетов в секунду (ОДНОАДРЕСНАЯ/МНОГОАДРЕСНАЯ/ШИРОКОВЕЩАТЕЛЬНАЯ передача);

c) уникальный SSID/VLAN;

d) конфигурации QoS;

e) поддерживаемый ФИЗИЧЕСКИЙ ИНТЕРФЕЙС, например 802.11 a/b/g/n;

f) допуск задержки;

g) допуск на искажения.

5) Какова географическая плотность размещения приборов, то есть, как много приборов каждого типа необходимо поддерживать на заданном участке здания предприятия?

6) Какие *конкретные* методы защиты (аутентификации и шифрования) поддерживаются устройством, например, в случае WPA2-Enterprise, какие *конкретные* EAP режимы поддерживаются?

7) Какова мощность передачи устройства на всех предназначенных каналах и физические режимы передачи данных (скорость передачи данных, тип кодирования и модуляции, пропускная способность канала)?

8) Какие физические режимы (скорость передачи данных, тип кодирования и модуляции, пропускная способность канала) поддерживает устройство?

9) Какова чувствительность приемника на разных предназначенных каналах и при разных физических режимах (скорость передачи данных, тип кодирования и модуляции, пропускная способность канала)?

10) Использует ли прибор МНОГОАДРЕСНЫЙ или ШИРОКОВЕЩАТЕЛЬНЫЙ трафик? Как часто отправляются пакеты данных МНОГОАДРЕСНОЙ/ШИРОКОВЕЩАТЕЛЬНОЙ передачи и насколько они большие?

11) Регулирует ли прибор мощность передачи, возможно, посредством реализации *Регулировки Мощности Передачи* 802.11h, для минимизации помех? Для решений 802.11, поддерживается ли прибором регулирование отдаваемой мощности как функция элемента AP для ограничения мощности?

12) Какое обучение доступно и как много отладочной информации можно получить из прибора?

Среда (окружение)

1) Какие другие устройства и системы используют тот же RF диапазон и находятся рядом с объектом? Какие мощности передачи имеют эти устройства и системы и какие методы модуляции они используют?

2) Каков уровень фонового шума/помех, вызванных как преднамеренными, так и непреднамеренными излучателями в выбранном RF диапазоне?

3) Какие типы конструкций использовались при создании здания и как каждый их них влияет на прохождение RF сигналов в предназначенных диапазонах?

4) Требуется ли включение лифтов и пожарных лестниц в зону покрытия?

5) Находится ли здание предприятия рядом с местом расположения действующей радиолокационной станции? (военной базы, аэропорта, метеостанции)?

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 80001-1:2010	—	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта (документа). Перевод данного международного стандарта (документа) находится в Федеральном информационном фонде технических регламентов и стандартов.		

Библиография

Примечание — Объединенная рабочая группа не подтверждает содержание каких-либо технических справочных документов, перечисленных ниже. Они предлагаются в качестве дополнительной информации, связанной с руководством по применению требований стандарта МЭК 80001-1 к беспроводной МЕДИЦИНСКОЙ ИТ СЕТИ.

[1] IEC 80001-2-1:2012 Application of risk management for IT-networks incorporating medical devices — Part 2-1: Step-by-step risk management of medical IT-networks — Practical applications and examples

[2] IEC 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices — Part 2-2: Guidance for the communication of medical device security needs, risks and controls

[3] ISO 14971:2007 Medical devices — Application of risk management to medical devices

[4] ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[5] ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements

[6] ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management

[7] AAMI TIR-18 Guidance on electromagnetic compatibility of medical devices for clinical/biomedical engineers — Part 1: Radiated radio-frequency electromagnetic energy, Association for the Advancement of Medical Instrumentation, 1110 N. Glebe Road, Suite 220, Arlington, VA 22201-5762

[8] ANSI C63.18 Recommended Practice for an On-Site, Ad Hoc Test Method for Estimating Radiated Electromagnetic Immunity of Medical Devices to Specific Radio-Frequency Transmitters, American National Standards Institute/ The Institute of Electrical and Electronics Engineers, Inc., 345 East 47th Street, New York, NY 10017-2394, USA

[9] IEEE Std 473-1985 IEEE Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 GHz), The Institute of Electrical and Electronics Engineers, Inc., 345 East 47th Street, New York, NY 10017-2394, USA

[10] IEEE Std 11073-00101-2008 Healthcare informatics — PoC medical device communication: Part 00101: Guide – Guidelines for the use of RF wireless technology, The Institute of Electrical and Electronics Engineers, Inc., 345 East 47th Street, New York, NY 10017-2394, USA

[11] FDA Guidance Document: Draft Guidance for Industry and FDA Staff — Radio-Frequency Wireless Technology in Medical Devices [cited 2012-06-08]. Available from Internet: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077210.htm

[12] Failure mode and effects analysis in health care: proactive risk reduction. Chicago (IL): Joint Commission Resources, Inc.; 2002. p.8

[13] Alarm Interventions During Medical Telemetry Monitoring: A Failure Mode and Effects Analysis, Pennsylvania Patient Safety Authority [cited 2012-06-08]. Available from Internet:http://patientsafetyauthority.org/ADVISORIES/AdvisoryLibrary/2008/mar5(suppl _rev)/Pages/mar5(supplrev).aspx

[14] Patient Safety: Achieving a New Standard for Care. Institute of Medicine, Washington D.C.: The National Academies Press 2004

[15] The Quality System Compendium, GMP Requirements & Industry Practice, Association for the Advancement of Medical Instrumentation, 1998.

[16] United States Code of Federal Regulations § 820

[17] ITU-T; An overview of the impairments and quality attributes of wireless applications [cited 2012-06-08]. Available from Internet :http://www.itu.int/rec/T-REC/

[18] BAKER, Steven D. and Hoglund, David H. Medical-Grade, Mission-Critical Wireless Networks. IEEE Engineering in Medicine and Biology Magazine, March/April 2008, pp 86—95

[19] FDA Guidance for Industry — Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software [cited 2012-06-08]. Available from Internet: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm)

[20] ISO/IEC Joint Technical Committee — Health informatics — Use of mobile wireless communication and computing technology in healthcare facilities

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, информационная безопасность, менеджмент рисков, информационно-вычислительные сети, медицинские приборы

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *В.Е. Нестерова*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 19.05.2016. Подписано в печать 02.06.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,70. Тираж 29 экз. Зак. 1397.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru