А.П. СТОЛБОВ,
д.т.н., профессор Высшей школы управления здравоохранением,
Первый Московский государственный медицинский университет им. И.М. Сеченова,
г. Москва, Россия, ap100Lbov@mail.ru

ОБ ОПРЕДЕЛЕНИИ КЛАССОВ КИБЕРБЕЗОПАСНОСТИ МЕДИЦИНСКОЙ ТЕХНИКИ

УДК 61:656.251+615:47+004.056.53

Столбов А.П. ***Об определении классов кибербезопасности медицинской техники*** *(Первый Московский государственный медицинский университет им. И.М. Сеченова, г. Москва, Россия)*

Аннотация. Рассмотрены проблемы кибербезопасности (КБ) цифровой медицинской техники (МТ). Перечислены основные угрозы, связанные с несанкционированным внешним кибервоздействием (НСВ) на МТ для безопасности пациента. Предложена классификация МТ в зависимости от уровня исходной защищенности от НСВ. Описаны правила идентификации классов КБ медицинской техники.

Ключевые слова: *информационная безопасность, медицинская техника, классификация рисков применения медицинской техники, классы кибербезопасности медицинской техники.*

UDC 61:656.251+615:47+004.056.53

Stolbov A.P. ***About the definition of the classes of Cybersecurity of Medical devices*** *(The First Sechenov Moscow State Medical University, Moscow, Russia)*

Abstract. The paper discusses problems of Cybersecurity (CS) digital medical devices (MD). Lists the main threats associated with unauthorized external cybervandalism (CV) MD for patient safety. The classification of MD depending on the level of initial security from CV. The rules identify classes of CS medical devices.

Keywords: *information security, medical devices, classification of risks of the use of medical devices, the classes of cybersecurity medical devices.*

Одной из наиболее значимых сегодня тенденций в развитии здравоохранения является «цифровизация» медицинских технологий. При этом в условиях всеобщей «интернетизации» все более актуальными становятся проблемы обеспечения кибербезопасности (КБ)[1] [1, 16–22] информационных и технологических систем. В последнее время заметно возросло количество инцидентов, связанных с несанкционированным внешним воздействием (НСВ)[2] на

[1] Кибербезопасность – обеспечение защиты (защищенность) от несанкционированного внешнего воздействия на компьютерную систему, информационные ресурсы и программное обеспечение через телекоммуникационные сети или машинные носители данных, результатами которого могут быть нарушение работоспособности системы, утечка, искажение и (или) потеря данных (информации).

[2] В специальной литературе, нормативных и методических документах используется также термин «несанкционированный доступ к информации» (НСД), под которым понимается доступ к информации, нарушающий установленные правила разграничения доступа, а под доступом к информации понимается ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации. Далее термины НСВ и НСД будем считать синонимами.

медицинские информационные системы (МИС) и цифровую медицинскую технику (МТ)[3], в состав которой входит программное обеспечение (ПО) и/или микропрограммный блок управления (контроллер, процессор), например, на томографы, лабораторные анализаторы, кардиостимуляторы и инсулиновые помпы [25–27]. Результатами реализации указанных киберугроз в общем случае могут быть: отказ – потеря работоспособности МИС и/или МТ, несанкционированное изменение режима и параметров функционирования МТ; частичная или полная потеря или искажение результатов измерения физиологических параметров, исследования биоматериала, записей в электронной медицинской карте пациента (ЭМК), в хранилище (архиве) медицинских изображений и т.п.; утечка персональных данных пациента – несанкционированный доступ к конфиденциальной информации, в том числе к сведениям, составляющим врачебную тайну.

Заметим, что в США, начиная с 2013 г., FDA (www.fda.gov) осуществляется мониторинг инцидентов, связанных с кибервоздействием на цифровую медицинскую технику.

Очевидно, что нарушение работоспособности цифровой МТ, вызванное несанкционированным внешним кибервоздействием, может иметь самые серьезные последствия для здоровья пациента и/или персонала. При этом неправильная работа МТ может привести даже к более тяжелым последствиям, чем явный «отказ», особенно, если признаки неправильной работы не заметны для пользователя. Во многих случаях, не связанных с явным отказом МИС и МТ, для обнаружения признаков НСВ необходимо предпринимать особые усилия и применять специальные средства обнаружения кибервторжений[4].

Таким образом, при анализе и оценке рисков применения медицинских технологий[5], использующих МТ, необходимо учитывать также угрозы внешнего кибервоздействия, случайного или преднамеренного.

Разработчик цифровой МТ должен изначально, еще на этапе проектирования иметь возможность априорно идентифицировать и оценить потенциальные риски ее применения, связанные с возможным кибервоздействием, в том числе для того, чтобы предусмотреть при необходимости включение в состав МТ встроенных или внешних (как обязательные принадлежности) средств защиты информации, контроля работоспособности и т.д., и определения требований к мерам и средствам защиты в процессе эксплуатации техники.

Потребитель, покупатель цифровой МТ также должен заранее знать, какие ресурсы, организационно-технические меры и средства защиты от кибервоздействия необходимы для обеспечения нормальной, устойчивой и безопасной работы медицинской техники при ее использовании в условиях конкретного медицинского учреждения.

Вместе с тем, вопросы кибербезопасности цифровой МТ и её классификации по уровню исходной защищенности от НСВ сегодня недостаточно рассмотрены в отечественных научных публикациях и практически не отражены в нормативно-методических документах Минздрава России, регламентирующих обращение медицинских изделий. Большинство из принятых в последнее время международных стандартов по менеджменту рисков в компьютерных сетях с медицинской техникой [16–22] имеет «рамочный» характер – в них описываются только самые общие подходы и требования к обеспечению защиты МТ от кибервоздействия. Нужны специальные методические руководства по их практическому применению в медицинских организациях, в том числе с учетом классифика-

[3] Изделие медицинской техники – ГОСТ 207980. Здесь и далее под МТ будем понимать также и ПО, которое используется для применения медицинской техники по назначению.

[4] См. приказ ФСТЭК России от 06.12.2011 г. № 638.

[5] См. ГОСТ Р 56044.

ций и требований к информационной безопасности, установленных документами, принятыми в Российской Федерации.

Целью настоящей работы является идентификация классов кибербезопасности цифровой медицинской техники, на основе которых могут быть определены требования к составу мер и средств защиты МТ от НСВ, в том числе, с учетом требований к информационной безопасности, установленных нормативными документами Правительства Российской Федерации, Федеральной службы по техническому и экспортному контролю (ФСТЭК) и Федеральной службы безопасности (ФСБ) России. При этом, как показал проведенный анализ, непосредственное «один к одному», прямое применение для цифровой МТ классификаций защищенности от несанкционированного доступа (НСД), установленных руководящими документами ФСТЭК для средств вычислительной техники и автоматизированных систем [3–6], в общем случае нецелесообразно и невозможно, поскольку в указанных документах акценты сделаны на гриф секретности (категорию) защищаемой информации и принципы разграничения доступа субъектов к объектам защиты в соответствии с установленными полномочиями, что в нашем случае, очевидно, не является столь актуальным.

Далее под **классом кибербезопасности** цифровой медицинской техники будем понимать комплексный показатель, характеризующий уровень исходной (проектной) защищенности изделия медицинской техники от несанкционированного (неконтролируемого пользователем) внешнего воздействия на программное обеспечение и/или цифровой блок управления, и определяющий требования, выполнение которых обеспечивает нейтрализацию угроз указанного воздействия.

Термин «исходная защищенность» в данном случае характеризует устойчивость данного типа МТ по отношению к несанкционированному кибервоздействию, независимо от того, в составе какой технологической системы она используется, в том числе независимо от защищенности от НСВ других элементов, входящих в состав этой системы. Иными словами, термин «исходная защищенность» характеризует данный тип МТ как отдельный, самостоятельный элемент системы, независимо от ее состава, структуры, режима использования, квалификации пользователей, используемых средств защиты информации, состава организационно-технических мероприятий по обеспечению информационной безопасности и т.д.

При определении классов кибербезопасности цифровой медицинской техники будем исходить из того, что:

– риск, угроза НСВ на цифровую медицинскую технику является одной из составляющих риска безопасности ее применения – потенциальный риск применения цифровой МТ должен оцениваться и классифицироваться в зависимости от последствий для здоровья пациента, к которым может привести неправильная работа МТ, в том числе в результате несанкционированного внешнего кибервоздействия на «цифровые» компоненты МТ и программное обеспечение;

– цифровая медицинская техника эксплуатируется в среде определенной организационно-технической системы – лечебно-профилактического учреждения, безопасность (в том числе кибербезопасность) и результативность работы которой в значительной степени зависят от «человеческого фактора» и качества управления (менеджмента), а не только от работоспособности и характеристик техники и информационной системы учреждения.

Классификация медицинской техники по уровню исходной защищенности осуществляется на основе следующих положений:

– при определении класса кибербезопасности цифровая МТ рассматривается исключительно как техническое устройство – объект защиты от НСВ, безотносительно к его «медицинскому» назначению (функции);

– при определении классов кибербезопасности анализируется и оценивается только вероятность НСВ, безотносительно к характеру возможных последствий и проявлений НСВ – явный отказ, неявное изменение режима или алгоритма работы, утечка, искажение или удаление данных и т.д.;

– класс кибербезопасности цифровой МТ должен соотноситься с вероятностью и результативностью НСВ исходя из принципа «враждебного окружения» – полагается, что воздействие осуществляет высококвалифицированный внешний нарушитель, имеющий возможность использовать средства для обхода «штатной» системы защиты «стандартной» операционной среды (системы).

Определение классов кибербезопасности (уровней защищенности) цифровой медицинской техники (ККБ) предлагается осущетвлять с помощью метода анализа и оценки рисков по качественным признакам по следующей лингвистической шкале:

– высокий уровень – класс «В», когда для защиты МТ от НСВ не требуется применение специальных дополнительных мер – режим использования МТ, а также встроенные средства защиты от НСВ обеспечивают высокую исходную защищенность МТ; успешное (результативное) несанкционированное внешнее воздействие маловероятно;

– средний уровень – класс «С», когда необходимый уровень защиты МТ от НСВ обеспечивается применением общих организационных и технических мер и средств обеспечения информационной безопасности медицинского учреждения, в соответствии с предусмотренными технической документацией режимами использования МТ, в том числе, возможно, совместно с определенным внешним ПО в составе МИС; дополнительных мер для защиты данного медицинского изделия от НСВ не требуется; успешное (результативное) НСВ возможно, но его вероятность невелика;

– низкий уровень – класс «Н», когда предусмотренный технической документацией режим использования МТ и встроенные средства защиты от НСВ не обеспечивают необходимого уровня защиты МТ от НСВ и безопасности пациента – требуется применение специальных дополнительных мер защиты от случайного или преднамеренного кибервоздействия; вероятность успешного (результативного) НСВ достаточно высока.

В качестве критериев при определении класса кибербезопасности определенного типа цифровой медицинской техники предлагается использовать следующие структурно-функциональные характеристики:

1) тип используемой операционной системы (ОС)[6]:

СтС – «стандартная» ОС, для которой известны основные уязвимости и способы «взлома» штатной системы защиты в ОС, имеются программные «вирусы» и т.д.; заметим, что заражение МТ «вирусами» может осуществляться как преднамеренно, так и случайно;

СпС – специальная ОС, разработанная для данного типа МТ (семейства изделий МТ, см. ГОСТ 34.003), для которой практически ничего неизвестно об уязвимостях, способах «взлома» системы защиты, а появление «вирусов» маловероятно;

2) необходимость использования внешних машинных носителей данных (ВН) в процессе применения по назначению/эксплуатации медицинской техники, например, для обмена данными, обновления программного обеспечения и т.д.:

МН – используются «стандартные» внешние носители данных, которые могут использоваться с обычным, персональным компьютером;

БН – использование «стандартных» внешних носителей невозможно либо запрещено, либо допускается использование только

[6] Здесь и далее указаны условные буквенные обозначения соответствующих характеристик.

«доверенных» стандартных носителей, либо применяются специальные «нестандартные» внешние носители данных, которые не могут использоваться с обычными компьютерами;

3) режим работы / применения МТ по назначению – автономный (АР) либо в составе вычислительной сети информационно-технологической системы; автономным в данном случае считается также режим, когда при эксплуатации МТ используются специальные, «нестандартные» внешние машинные носители данных;

4) необходимость подключения к телекоммуникационной сети и/или использование беспроводных технологий, постоянно или периодически, например, для дистанционного управления работой МТ, передачи измерительной информации, в том числе при выполнении телемедицинских услуг (дистанционный мониторинг состояния здоровья пациента и т.д.), технического обслуживания МТ, обновления ПО и т.д. (КС):

ЗК – используются только защищенные каналы передачи данных для взаимодействия с внешними «доверенными» информационными системами (серверами);

ОК – используются открытые, незащищенные каналы передачи данных общего пользования для взаимодействия с внешними «открытыми» ИС либо необходим выход в Интернет;

5) наличие встроенных средств защиты от НСВ и проверки работоспособности медицинской техники (СК); например, средств доверенной загрузки программного обеспечения, выполнения контрольных задач и т.д.; сюда же относятся случаи, когда внесение изменений в программный код цифрового блока управления МТ («перепрошивка») возможно только с помощью специального оборудования («в заводских условиях»).

Правила определения класса кибербезопасности МТ в формализованном виде могут быть представлены в виде путей в классификационном графе[7] – ориентированном гиперграфе (см. рисунок), состоящем из начальной вершины МТ и гипервершин двух видов:

– классов кибербезопасности (ККБ), включающей вершины классов – уровней исходной защищенности изделия медицинской техники: Н – низкая, С – средняя, В – высокая;

– классификационных характеристик МТ– три гипервершины: КС – каналы передачи данных, ВН – внешние носители данных, ОС – операционная система (далее – Х-вершины), вершины в которых соответствуют перечисленным выше структурно-функциональным характеристикам изделия медицинской техники.

Каждому правилу соответствует определенный простой путь в графе из начальной вершины МТ в одну из ККБ-вершин, проходящий через Х-вершины.

Например, путь (МТ–ОК–СтС–Н) означает, что если в процессе эксплуатации МТ необходимо использовать открытый канал связи (ОК) и при этом работа осуществляется в среде «стандартной» операционной системы (СтС), то МТ имеет низкий класс кибербезопасности (Н); путь (МТ–АР–В) – если изделие МТ работает в автономном режиме (АР), то оно имеет высокий класс кибербезопасности (В) и т.д.

Пути в графе – правила определения класса кибербезопасности ККБ изделия медицинской техники – могут быть описаны в виде следующих логических выражений:

П1: ОК $\wedge$ СтС $\Rightarrow$ ККБ = Н;
(соответствует пути (МТ–ОК–СтС–Н) на графе)
П2: МН $\wedge$ СтС $\Rightarrow$ ККБ = Н;
П3: ОК $\wedge$ СпС $\Rightarrow$ ККБ = С;
П4: МН $\wedge$ СпС $\Rightarrow$ ККБ = С;
П5: ЗК $\wedge$ БН $\Rightarrow$ ККБ = В;
П6: АР $\Rightarrow$ ККБ = В;
П7: СК $\Rightarrow$ ККБ = В;

где символ $\wedge$ – это знак логической операции «И» (конъюнкция), символ $\Rightarrow$ – знак логиче-

[7] В классификационном графе не может быть циклов и изолированных вершин.

ского следствия (импликации) «ЕСЛИ ..., ТО ...» (по ГОСТ Р 54521).

Алгоритм определения класса кибербезопасности может быть представлен также в виде дерева решений, которое описывается следующими логическими выражениями:

А1: Если АР ∨ СК ∨ ЗК ∧ БН, то ККБ = В и «Стоп»; иначе перейти к А2;

А2: Если СпС, то ККБ = С и «Стоп»; иначе ККБ = Н и «Стоп»;

где символ ∨ – это знак логической операции «ИЛИ» (дизъюнкция).

Выражение А1 означает, что если изделие медицинской техники эксплуатируется в автономном режиме (АР) и/или имеет встроенные средства контроля (СК) либо в процессе его эксплуатации используются только защищенные каналы связи (ЗК) и при этом не используются «стандартные» внешние машинные носители (БН), то оно имеет высокий класс кибербезопасности (ККБ = В). «Стоп» означает, что дальнейшие проверки для определения класса можно не выполнять. Выражение А2 здесь означает, что если в «неавтономном» изделии МТ, не имеющем встроенных средств защиты, применяется специальная операционная система (СпС), и при этом в процессе эксплуатации используются открытые каналы связи и/или «стандартные» внешние носители данных, то МТ имеет средний уровень исходной защищенности от кибервоздействия (ККБ = С); в остальных случаях, то есть когда используется «стандартная» ОС, открытые каналы связи и/или «стандартные» носители – изделие медицинской техники имеет низкий класс кибербезопасности (ККБ = Н).

Следует отметить, что описанные выше правила классификации по уровням кибербезопасности относятся только к изделиям цифровой медицинской техники и в общем случае не применимы к программным медицинским изделиям (Software as a Medical Device – SaMD, см. [8, 28, 29]).

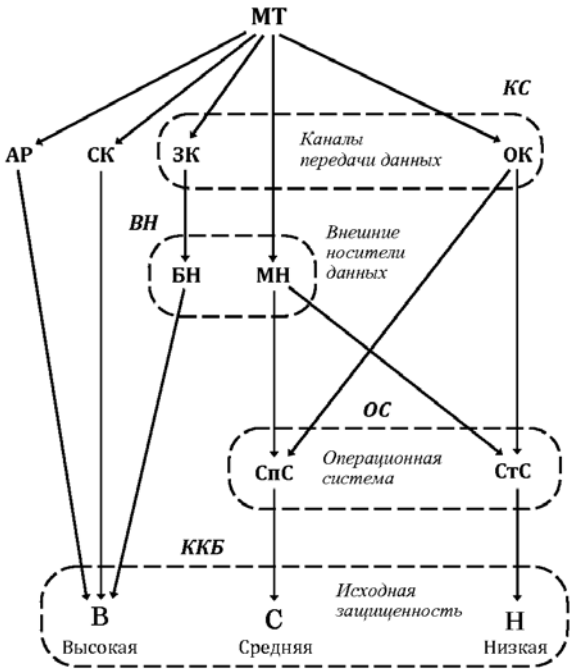

Рисунок – **Определение класса кибербезопасности изделия медицинской техники**

Проектирование и производство цифровой медицинской техники целесообразно осуществлять, в том числе с использованием подходов и методов создания защищенных информационных систем [15].

Для оценки уровня кибербезопасности изделия МТ при его работе в составе МИС конкретной медицинской организации необходимо построить модель угроз – определить перечень актуальных угроз (рисков) безопасности с оценкой возможных последствий в результате их реализации (каналы проникновения, утечки, нарушители, оценка рисков, ущерба, вреда и т.д.). Для этого можно использовать, например, методы моделирования угроз безопасности информации, изложенные в руководящих документах ФСТЭК и ФСБ России, а также положения и рекомендации, описанные в [14, 16–22]. При этом следует иметь в виду, что основой производственной инфраструктуры современного медицинского учреждения сегодня становятся интегрированные медицинские информационно-технологические комплексы, включающие медицинские аппараты, приборы и оборудование, медицинские территориально распределенные информационные системы, подключенные к внешним телекоммуникационным сетям и «облачным» информационным и вычислительным сервисам и хранилищам данных.

Разработку методики построения указанной модели, а также определения состава необходимых мер и средств защиты, нейтрализующих угрозы кибервоздействия на МТ и МИС в целом, с учетом классов исходной защищенности цифровой медицинской техники целесообразно осуществлять на основе документов ФСТЭК [23, 24] и положений, изложенных в ГОСТ Р 51583.

При определении требований к защите медицинской техники от НСВ необходимо учитывать, что, независимо от того, интегрирована или нет конкретная МТ в состав МИС, она является элементом сложной организационно-технической системы – медицинской организации, в которой реализуется определенная политика информационной безопасности, которая формируется исходя из анализа актуальных угроз кибербезопасности, идентификации и оценки рисков, связанных с использованием МИС и цифровой МТ, подключением к внешним телекоммуникационным сетям и т.д.

ВЫВОДЫ

1. Представляется целесообразным дополнительно к номенклатурной классификации медицинских изделий по видам и степени потенциального риска применения для цифровой медицинской техники предусмотреть еще один классификационный признак – класс кибербезопасности, определяемый на основе рассмотренных выше критериев.

2. Классификацию цифровой медицинской техники в зависимости от потенциального риска их применения необходимо осуществлять с учетом их класса кибербезопасности – уровня исходной защищенности от несанкционированного внешнего кибервоздействия.

3. Необходимо разработать отраслевую базовую модель угроз информационной безопасности для медицинских информационных систем, в состав которых интегрирована цифровая медицинская техника. Указанная модель должна включать типовой перечень организационно-технических мероприятий, мер и средств защиты от кибервоздействия, в том числе для обеспечения групповой, одиночной (индивидуальной) и смешанной системы защиты от НСВ цифровой медицинской техники.

В заключение хотелось бы заметить, что после многочисленных публикаций о «взломах» компьютерных систем, кражах и утечках персональных данных, вирусных атаках, нарушающих нормальную работу медицинской техники, информационных систем и баз данных медицинских учреждений, которые имели место в последнее время у определенной ча-

сти населения, и пациентов, и врачей, начала формироваться своего рода «киберфобия», чувство недоверия к современным ИТ и даже желание запретить обработку и обмен клиническими и персональными данными в электронном виде. Однако кибербезопасность во многом зависит от четкой организации работы администрации, пользователей и технического персонала информационных систем, знания, понимания и соблюдения ими основных принципов обеспечения информационной безопасности, их ответственности и самоконтроля.

ЛИТЕРАТУРА

1. Двусторонний проект Россия-США по выработке основ критически важной терминологии в области кибербезопасности. Выпуск 1. Апрель 2011 года; www.iisi.msu.ru/UserFiles/File/Terminology_IISI_EWI/Russia-USbilatera_on_terminology_RUS.pdf, доступ 20.07.2015.

2. *Столбов А.П.* О классах кибербезопасности медицинской техники // Математическая кардиология. Теория, клинические результаты, рекомендации, перспективы. Сб. научн. трудов под ред. В.А. Лищука и Д.Ш. Газизовой. – М.: ООО «ПРИНТ ПРО». – 2015. сс. 131–142.

3. Защита от несанкционированного доступа к информации. Термины и определения. Руководящий документ Гостехкомиссии от 30.03.1992 г.

4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии от 30.03.1992 г.

5. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии от 30.03.1992 г.

6. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии от 30.03.1992 г.

7. Номенклатурная классификация медицинских изделий. Приказ Минздрава России от 06.06.2012 г. № 4н (в ред. Приказа от 25.09.2014 г. № 557н).

8. Правила классификации медицинских изделий в зависимости от потенциального риска применения. Утверждены решением Коллегии Евразийской экономической комиссии от 22.12.2015 г. № 173.

9. ГОСТ 31508–2012 Изделия медицинские. Классификация в зависимости от потенциального риска применения. Общие требования.

10. ГОСТ ISO 14971–2011 Изделия медицинские. Применение менеджмента риска к медицинским изделиям.

11. ГОСТ Р 55544–2013 Программное обеспечение медицинских изделий. Часть 1. Руководство по применению ИСО 14971 к программному обеспечению изделий.

12. ГОСТ 30324.0.4–2002 Изделия медицинские электрические. Требования безопасности к программируемым медицинским электронным системам.

13. ГОСТ Р 51904–2002 Программное обеспечение встроенных систем. Общие требования к разработке и документированию.

14. ГОСТ Р МЭК 62304–2013 Изделия медицинские. Программное обеспечение. Процессы жизненного цикла.
15. ГОСТ Р 51583–2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
16. ГОСТ Р 56839–2015 Информатизация здоровья. Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 2–1. Пошаговый менеджмент рисков медицинских информационно-вычислительных сетей. Практическое применение и примеры.
17. ГОСТ Р 56841–2015 Информатизация здоровья. Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 2–4. Руководство по применению. Общее руководство для медицинских организаций.
18. ГОСТ Р 56837–2015 Информатизация здоровья. Менеджмент информационной безопасности удаленного технического обслуживания медицинских приборов и медицинских информационных систем. Часть 1. Требования и анализ рисков.
19. ГОСТ Р 56838–2015 Информатизация здоровья. Менеджмент информационной безопасности удаленного технического обслуживания медицинских приборов и медицинских информационных систем. Часть 2. Внедрение системы менеджмента информационной безопасности.
20. ГОСТ Р 56850–2015 Информатизация здоровья. Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 2–2. Руководство по выявлению и обмену информацией о защите медицинских приборов, рисках и управлении рисками.
21. ГОСТ Р 56840–2015 Информатизация здоровья. Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 2–3. Руководство по беспроводным сетям.
22. ГОСТ Р ИСО 27799–2015 Информатизация здоровья. Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002.
23. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11.02.2013 г. № 17.
24. Меры защиты информации в государственных информационных системах. Методический документ. Утвержден ФСТЭК России 11.02.2014 г.
25. Advanced Cyber-Physical Systems for National Priorities, 13.03.2014, www.nist.gov/public_affairs/factsheet/cyberphysicalsystems2015.cfm, доступ 20.07.2015 г.
26. The prognosis for healthcare payers and providers: Rising cybersecurity risks and costs, 17.12.2014, http://usblogs.pwc.com/cybersecurity/the-prognosis-for-healthcare-payers-and-providers-rising-cybersecurity-risks-and-costs, доступ 20.07.2015.
27. www.mcafee.com/us/resources/reports/rp-healthcare-iot-rewards-risks-summary, доступ 20.07.2015.
28. IMDRF/SaMD WG/N10:2013 Software as a Medical Device: Key Definitions, 9 December 2013; www.imdrf.org
29. IMDRF/SaMD WG/N12:2014 Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations, 18 September 2014; www.imdrf.org.