

"Методические рекомендации по порядку проведения экспертизы качества, эффективности и безопасности медицинских изделий (в части программного обеспечения) для Государственной регистрации в рамках национальной системы"
(утв. Росздравнадзором 24.08.2018)

Утверждаю
Генеральный директор
ФГБУ "ЦМИКЭЭ"
Росздравнадзора
И.В.ИВАНОВ

Генеральный директор
ФГБУ "ВНИИИМТ"
Росздравнадзора
Д.Т.ШАРИКАДЗЕ
24 августа 2018 года

Дата введения
24 августа 2018 года

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
ПО ПОРЯДКУ ПРОВЕДЕНИЯ ЭКСПЕРТИЗЫ КАЧЕСТВА, ЭФФЕКТИВНОСТИ
И БЕЗОПАСНОСТИ МЕДИЦИНСКИХ ИЗДЕЛИЙ (В ЧАСТИ ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ) ДЛЯ ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ
В РАМКАХ НАЦИОНАЛЬНОЙ СИСТЕМЫ**

Настоящие Методические рекомендации разработаны:

- специалистами ФГБУ "ВНИИИМТ" Росздравнадзора: заместителем генерального директора, д.м.н. Тарасенко О.А., начальником отдела экспертизы Никифоровой Л.Ю., руководителем испытательного центра Михеевым С.В.

Рецензенты: начальник управления организации государственного контроля и регистрации медицинских изделий Росздравнадзора, к.т.н. Астапенко Е.М., заместитель начальника управления организации государственного контроля и регистрации медицинских изделий Росздравнадзора Суханова М.М., генеральный директор ФГБУ "ЦМИКЭЭ" Росздравнадзора Иванов И.В.

Методические рекомендации предназначены для использования экспертными организациями Росздравнадзора, специалистами Росздравнадзора, для информирования субъектов обращения медицинских изделий.

Нет никаких ограничений на воспроизведение, распространение или использование этого документа, однако его включение, частично или полностью, в любой другой документ должно сопровождаться обязательной ссылкой на данный документ.

Экспертные организации:

- Федеральное государственное бюджетное учреждение "Всероссийский научно-исследовательский и испытательный институт медицинской техники" Федеральной службы по надзору в сфере здравоохранения (ФГБУ "ВНИИИМТ" Росздравнадзора);

- Федеральное государственное бюджетное учреждение "Центр мониторинга и клинико-экономической эффективности" Федеральной службы по надзору в сфере здравоохранения (ФГБУ "ЦМИКЭЭ" Росздравнадзора).

Настоящие Методические рекомендации разработаны в дополнение к действующим Методическим рекомендациям по экспертизе качества, эффективности и безопасности медицинских изделий для государственной регистрации, утвержденным ФГБУ "ВНИИИМТ" Росздравнадзора и ФГБУ "ЦМИКЭЭ" Росздравнадзора.

Введение

Методические рекомендации разработаны и утверждены для целей реализации следующих документов:

- Федеральный закон от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" Собрание законодательства Российской Федерации (с изменениями и дополнениями от 25 июня 2012 г., 2, 23 июля, 27 сентября, 25 ноября, 28 декабря 2013 г., 4 июня, 21 июля, 22 октября, 1, 31 декабря 2014 г., 8 марта, 6 апреля, 29 июня, 13 июля, 30 сентября, 14, 29 декабря 2015 г., 5, 26 апреля, 3 июля 2016 г., 3 апреля, 1 мая, 1, 29 июля, 5, 29 декабря 2017 г., 7 марта 2018 г.);

- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (в ред. Федеральных законов от 25.11.2009 N 266-ФЗ, от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ, от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ, от 29.11.2010 N 313-ФЗ, от 23.12.2010 N 359-ФЗ, от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ, от 05.04.2013 N 43-ФЗ, от 23.07.2013 N 205-ФЗ, от 21.12.2013 N 363-ФЗ, от 04.06.2014 N 142-ФЗ, от 21.07.2014 N 216-ФЗ, от 21.07.2014 N 242-ФЗ, от 03.07.2016 N 231-ФЗ, от 22.02.2017 N 16-ФЗ, от 01.07.2017 N 148-ФЗ, от 29.07.2017 N 223-ФЗ);

- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (с изменениями и дополнениями);

- Федеральный закон "О техническом регулировании" от 27 декабря 2002 года N 184-ФЗ (с изменениями и дополнениями);

- Постановление Правительства Российской Федерации от 27 декабря 2012 г. N 1416 "Об утверждении Правил государственной регистрации медицинских изделий" (в редакции постановления Правительства РФ от 17.10.2013 N 930, от 17.07.2014 N 670, от 10.02.2017 N 160, от 31 мая 2018 г. N 633);

- Постановление Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- Постановление Правительства Российской Федерации от 12.04.2018 N 447 "Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями";

- Постановление Правительства Российской Федерации от 6 июля 2015 года N 676 "О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации (с изменениями на 11 мая 2017 года)";

- Приказ Министерства здравоохранения Российской Федерации от 21 декабря 2012 г. N 1353н "Порядок экспертизы качества, эффективности и безопасности медицинских изделий" (в редакции Приказа Минздрава России от 03.06.2015 N 303н);

- Приказ Министерства здравоохранения Российской Федерации от 06.06.2012 N 4н "Об утверждении номенклатурной классификации медицинских изделий";

- Приказ Министерства здравоохранения Российской Федерации от 16.05.2013 N 300н "Об утверждении требований к медицинским организациям, проводящим

клинические испытания медицинских изделий, и порядка установления соответствия медицинских организаций этим требованиям";

- Приказ Министерства здравоохранения Российской Федерации от 19 января 2017 года N 11н "Об утверждении требований к содержанию технической и эксплуатационной документации производителя (изготовителя) медицинского изделия".

При подготовке настоящих Методических рекомендаций применялись в том числе положения нижеперечисленных документов:

Руководящий документ (РД) "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.";

Руководящий документ (РД) "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.";

Руководящий документ (РД) "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.";

Руководящий документ (РД) "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114";

Руководящий документ (РД) "Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003 г.";

ГОСТ 19.301-79 "Единая система программной документации (ЕСПД). Программа и методика испытаний. Требования к содержанию и оформлению";

ГОСТ Р ИСО/МЭК 9126-93 "Информационная технология (ИТ). Оценка программной продукции. Характеристики качества и руководства по их применению";

ГОСТ Р ИСО 9127-94 "Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов";

ГОСТ Р ИСО/МЭК 12119-2000 "Информационная технология (ИТ). Пакеты программ. Требования к качеству и тестирование";

ГОСТ Р ИСО 14155-2014 "Клинические исследования. Надлежащая клиническая практика";

ГОСТ ISO 14971-2011 "Изделия медицинские. Применение менеджмента риска к медицинским изделиям";

ГОСТ 28195-89 "Оценка качества программных средств. Общие положения";

ГОСТ Р 51188-98 "Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство";

ГОСТ Р 55544-2013/IEC/TR 80002-1:2009 "Программное обеспечение медицинских изделий. Часть 1. Руководство по применению ИСО 14971 к программному обеспечению изделий";

ГОСТ Р 56430-2015/GNTF/SG3/N18:2010 "Система менеджмента качества. Изделия медицинские. Руководство по корректирующим и предупреждающим действиям и связанным процессам системы менеджмента качества";

ГОСТ Р МЭК 62304-2013 "Изделия медицинские. Программное обеспечение. Процессы жизненного цикла";

IMDRF/SaMD WG/N41 (PF):2017 "Программное обеспечение как медицинское изделие (SaMD); Клиническая оценка (представлен с письмом Росздравнадзора от 27.11.2017 N 04-56500/17);

Информационное письмо Федеральной службы по надзору в сфере здравоохранения (Росздравнадзор) от 30.12.2015 N 01И-2358/15 "О регистрации программного обеспечения";

Действующие Методические рекомендации по экспертизе качества, эффективности и безопасности медицинских изделий для государственной регистрации, утвержденные ФГБУ "ВНИИИМТ" Росздравнадзора и ФГБУ "ЦМИКЭЭ" Росздравнадзора (далее - основные Методические рекомендации).

1. Общие положения

1.1. Настоящие Методические рекомендации, как и основные Методические рекомендации, предназначены для использования специалистами ФГБУ "ВНИИИМТ" Росздравнадзора и ФГБУ "ЦМИКЭЭ" Росздравнадзора, осуществляющими экспертизу качества, эффективности и безопасности программного обеспечения как самостоятельного медицинского изделия, проводимую для целей государственной регистрации в рамках национальной системы.

1.2. Методические рекомендации разработаны в целях:

- установления единообразных подходов при проведении экспертизы качества, эффективности и безопасности программного обеспечения как самостоятельного медицинского изделия;

- унификации оценки соответствия программного обеспечения как самостоятельного медицинского изделия требованиям нормативных документов в части состава и содержания документации, представляемой на экспертизу в рамках регистрационных процедур.

1.3. Экспертиза качества, эффективности и безопасности комплектов документов программного обеспечения, являющегося принадлежностью или составной частью другого медицинского изделия (аппарата, прибора, оборудования, системы, комплекса) и предназначенного для установки (инсталляции) на этом медицинском изделии, также рассматривается в настоящих рекомендациях.

1.4. Список сокращений, применяемых в методических рекомендациях:

КРД - комплект регистрационных документов (регистрационного досье);

МИ - медицинские изделия;

МР - методические рекомендации;

ПО - программное обеспечение.

2. Экспертиза для определения возможности (невозможности) проведения клинических испытаний (этап I) Программного обеспечения

2.1. Применяются все положения основных Методических рекомендаций с некоторыми дополнениями и уточнениями.

2.2. Отнесение заявленного к регистрации Программного обеспечения к медицинским изделиям.

При отнесении заявленного для государственной регистрации Программного обеспечения к медицинским изделиям применяется определение пункта 1 статьи 38 Федерального закона от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", а также разъяснения Росздравнадзора в Информационном письме от 30.12.2015 N 01И-2358/15 "О регистрации программного обеспечения" о том, что Программное обеспечение относится к медицинским изделиям в случае, если предназначено его производителем для:

- управления работой медицинского оборудования и мониторинга за его функционированием;

- получения от медицинского оборудования диагностических данных, их накопления и расчета в автоматическом режиме;

- мониторинга функций организма человека и передачи данных (в том числе посредством беспроводных технологий);

- расчета параметров подбора дозы (облучения, лекарственного средства, рентгеноконтрастного вещества и т.д.);

- для обработки данных, полученных с диагностического медицинского оборудования, передачи их на системы планирования и терапии;

- обработки медицинских изображений (включая изменение его качества, цветового разрешения и т.д.);

- для 3-D моделирования;

- связи диагностического и лечебного оборудования;

- для обработки цифровых изображений (в том числе с получением данных от медицинского диагностического оборудования в неизменном виде).

Дополнительно следует учитывать, что Программное обеспечение относится к медицинским изделиям в случае, если предназначено (некоторые примеры):

- для 3-D моделирования, например, в стоматологии и зуботехнике, протезировании и ортопедии, имплантологии, макетировании органов и костей и т.п.;

- для обработки, хранения и передачи медицинской документации;

- для оказания медицинской помощи с применением телемедицинских технологий;

- для установки в специальной информационной системе оказания медицинской помощи на дому;

- для обработки данных для электронной регистрации медицинского оборудования, что позволяет проводить учет применяемых в больнице медицинских изделий;

- для создания канала связи между пациентом и медицинским специалистом, чтобы пациент мог проводить самостоятельное лечение в соответствии с правилами, определенными в процессе использования приложения, и/или для обеспечения мониторинга населения;

- для установки в информационной системе банка крови, или существующих электронных вычислительных машинах, или децентрализованных компьютерах/сетях.

2.3. Назначение Программного обеспечения.

Проверяется назначение Программного обеспечения, указанное в Заявлении, а также его соответствие данным технической и эксплуатационной документации.

Критерии несоответствия определяются по основным Методическим рекомендациям с учетом следующего:

- не указаны конкретные медицинские цели Программного обеспечения и возможность влияния на различные медицинские процессы <1>;

<1> Примечание:

Например, указано "Программное обеспечение предназначено для сбора, хранения, архивирования и передачи данных", а должно быть указано "Программное обеспечение предназначено для сбора, хранения, архивации и передачи медицинских диагностических данных, в том числе рентгеновских и ультразвуковых изображений".

2.4. Вид (или виды) Программного обеспечения в соответствии с действующей Номенклатурной классификацией.

Проверяется вид Программного обеспечения, указанный в Заявлении о государственной регистрации, и в случае если выявляется несоответствие, эксперт устанавливает другой вид (или виды) медицинского изделия в соответствии с действующей номенклатурной классификацией (с обязательным обоснованием). Применяются критерии отнесения к видам в соответствии с основными Методическими рекомендациями.

2.5. Класс Программного обеспечения в соответствии с действующей Номенклатурной классификацией.

Проверяется указанный в Заявлении класс в зависимости потенциального риска применения медицинского изделия в соответствии с действующими правилами классификации.

В случае если выявляется несоответствие, эксперт устанавливает другой класс в зависимости потенциального риска применения Программного обеспечения в соответствии с действующей номенклатурной классификацией (с обязательным обоснованием). При этом обязательно учитывается следующее.

В соответствии с Номенклатурным классификатором медицинских изделий, утвержденным приказом Минздрава России от 06.06.2012 N 4н (Приложение 2, пункты 7 и 12), установлено для Программного обеспечения:

- для специального программного обеспечения, используемого совместно с

медицинским изделием, устанавливают тот же класс, что и для самого медицинского изделия;

- программное обеспечение, которое является самостоятельным медицинским изделием (самостоятельно распространяется), при определении класса риска медицинского применения должно рассматриваться как активное медицинское изделие;

- программное обеспечение, заявленное для широкого распространения и широкого спектра применения, должно классифицироваться по самому высокому классу.

Также при определении класса риска медицинского применения Программного обеспечения рекомендуется учитывать следующее:

- назначение и область применения Программного обеспечения должны быть точно определены и соответственно заявлены производителем (изготовителем);

- должна быть учтена степень функциональности Программного обеспечения и заложенная в нем возможность управления рисками со стороны производителя (изготовителя);

- классификация Программного обеспечения сохраняется в том случае, когда оно соединяется с другим Программным обеспечением, другими медицинскими изделиями или используется в качестве модуля в большей системе;

- программное обеспечение для экспертных систем и систем поддержки принятия решения должно рассматриваться на соответствие клиническим рекомендациям Минздрава России и иметь наивысший класс риска;

- программное обеспечение медицинских информационных систем, лабораторных информационных систем должны учитывать требования методических рекомендаций Минздрава России.

В соответствии с ГОСТ Р МЭК 62304-2013 Программное обеспечение должно классифицироваться следующим образом:

- а) каждой Программной системе изготовитель должен присвоить класс безопасности (А, В или С) согласно возможным воздействиям на пациента, пользователя или иных лиц, исходя из опасности, возникновению которой может способствовать система программного обеспечения.

Классы безопасности программного обеспечения должны быть разделены по степени тяжести следующим образом:

- класс А: невозможны никакие травмы или ущерб здоровью;

- класс В: возможны незначительные травмы;

- класс С: возможны серьезные травмы или смерть.

Если опасность может происходить из-за отказа в работе Программной системы, то вероятность такого отказа должна быть принята как стопроцентная.

3.30 СИСТЕМА (SYSTEM): совокупная композиция, состоящая из одного или более процессов, аппаратных средств, Программного обеспечения, людей и средств, которая обеспечивает способность удовлетворить заявленную потребность или цель.

2.6. Код ОКПД2 по Общероссийскому классификатору продукции по видам экономической деятельности ОК 034-2014 (КПЕС 2008) с изменением 25/2017 ОКПД2.

В случае если выявляется несоответствие, эксперт рекомендует другой код ОКПД2 Программного обеспечения в соответствии с действующим классификатором (с обязательным обоснованием).

2.7. Оценка сведений о нормативной документации.

При оценке документа "Сведения о нормативной документации" применяются все положения основных Методических рекомендаций с учетом перечня рекомендуемых стандартов для проведения технических испытаний. Перечень стандартов, рекомендуемых для подтверждения соответствия при проведении технических испытаний в аккредитованной испытательной организации, приведен в разделе Введение настоящих Методических рекомендаций.

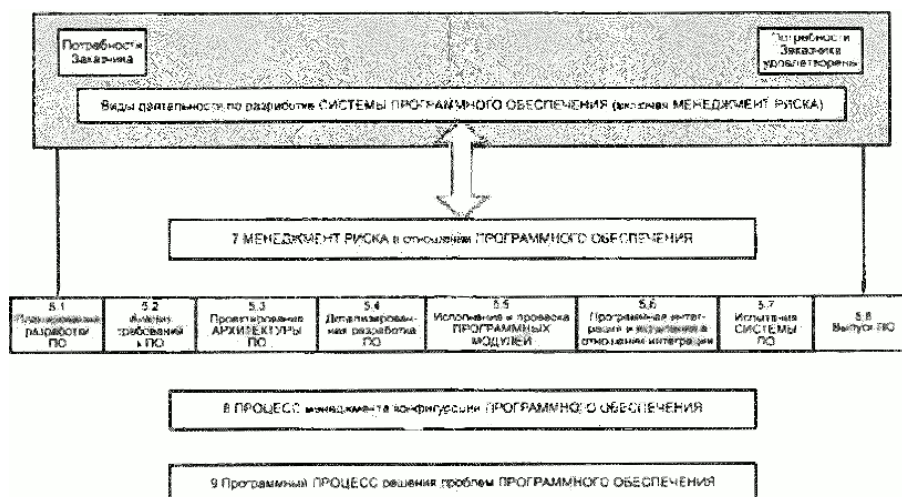
2.8. Оценка технической документации на Программное обеспечение.

Применяются положения основных Методических рекомендаций с учетом применения требований к Программному обеспечению, в том числе установленных приказом Минздрава России от 19 января 2017 года N 11н, а именно:

4. Техническая документация производителя (изготовителя) на медицинское изделие (далее - техническая документация), представляемая производителем (изготовителем) медицинского изделия или уполномоченным представителем производителя (изготовителя) медицинского изделия в составе регистрационного досье на медицинское изделие, должна содержать:

18) информацию о процессе проектирования, разработки и валидации программного обеспечения, используемого в готовом медицинском изделии (в случае наличия в медицинском изделии программного обеспечения, обеспечивающего его правильную эксплуатацию и (или) применение по назначению);

При проверке, представленной в рамках технической документации информации о процессах проектирования и разработки Программного обеспечения, следует учитывать рекомендации и требования ГОСТ Р МЭК 62304-2013:



Краткий обзор процессов разработки программного обеспечения и работ

Проверяется наличие и содержание файла менеджмента риска Программного обеспечения. В соответствии с ГОСТ Р МЭК 62304-2013:

3.14 процесс (process): совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующая входы в выходы.

3.20 файл менеджмента риска (risk management file): совокупность записей и других документов, создаваемых в процессе менеджмента риска.

Критерии несоответствия - по основным Методическим рекомендациям (все по применимости к конкретному Программному обеспечению), с учетом следующих особенностей:

а) отсутствуют сведения, регламентирующие конструкцию медицинского изделия - Программного обеспечения <1>;

<1> Примечания:

К сведениям, регламентирующим конструкцию Программного обеспечения, относятся:

- состав Программного обеспечения, взаимосвязь частей (модулей - при их наличии) и программных элементов конфигурации;

- описание конструктивных (архитектурных) особенностей, взаимосвязь с другими медицинскими и немедицинскими изделиями и другим Программным обеспечением;

особенности управления, имеющиеся потенциальные опасности (при необходимости);

- информация о Программном обеспечении (в том числе о его составных частях (модулях)) должна позволять осуществлять однозначную идентификацию;

- технические характеристики, требования и нормы, определяющие показатели качества, функциональные и эксплуатационные характеристики Программного обеспечения;

- перечень опасностей, связанных с применением Программного обеспечения, и описание мер/способов, принятых с целью обеспечения допустимости остаточных рисков (анализ рисков);

- основные принципы методов контроля и тестирования Программного обеспечения.

б) отсутствуют сведения, устанавливающие технические требования, данные для разработки и производства, надежность (безопасность) и данные для эксплуатации (применения) медицинского изделия - Программного обеспечения <2>;

<2> Примечание:

К таким сведениям относятся:

- требования к потенциальным возможностям и функциональности;

- функциональные характеристики Программного обеспечения должны содержать требования, влияющие на его способность действовать по назначению;

- физические характеристики (например, язык машинного кода, платформу, операционную систему);

- компьютерные характеристики (например, аппаратные средства, размер памяти, процессор, инфраструктуру сети);

- необходимость совместимости с модернизациями или другими версиями Программного обеспечения;

- входные и выходные данные Программного обеспечения (системы);

средства взаимодействия между модулями (элементами) Программного обеспечения и (или) другими изделиями;

- требования к защите информации, в том числе в отношении конфиденциальности (например, авторизация, идентификация пользователя, ведение журналов доступа и т.п.);

- определение данных (базы данных) и требование к ним (форма, размерность, функция и т.п.).

- описание условий и особенностей применения Программного обеспечения;

- порядок применения Программного обеспечения.

в) отсутствуют сведения о мерах, предпринимаемых производителем при разработке и производстве Программного обеспечения для обеспечения информационной безопасности <1>.

<1> Примечание:

К таким сведениям относятся:

- возможные риски при использовании Программного обеспечения по назначению в условиях, предусмотренных производителем;

- необходимые данные для применения, обосновывающие качество, безопасность и эффективность Программного обеспечения;

- не представлены формулировки надежности (защита против серьезных последствий ошибки пользователя, восстановление при ошибках, проверки достоверности исходных данных и т.п.);

- отсутствуют указания о порядке идентификации и проверки подлинности пользователей с санкционированным доступом при включении (начало/конец работы) Программного обеспечения по идентификатору (коду) и паролю условно-постоянного действия, определяемого производителем Программного обеспечения;

- отсутствуют указания о порядке регистрации входа (выхода) пользователей с санкционированным доступом при включении (начало/конец работы) Программного обеспечения либо регистрация загрузки и инициализации Программного обеспечения;

г) отсутствует информация о подтверждении качества достаточности средств защиты информации.

Производитель Программного обеспечения должен по возможности максимально обеспечить применение такой совокупности условий, возникающих в процессе разработки, производства, а в дальнейшем и эксплуатации в результате взаимодействия пользователей, интернет-сервисов, технологических устройств и сетевых связей, при которых все составляющие защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

Производитель Программного обеспечения при разработке изделия и технической

документации может руководствоваться действующими нормативными документами и действующими стандартами в части обеспечения информационной защиты, например, указанными во Введении к настоящим методическим рекомендациям.

Производитель должен самостоятельно определить распространение требований Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и постановления Правительства Российской Федерации от 01.11.2012 N 1119 в отношении Программного обеспечения как медицинского изделия, представленного для государственной регистрации. При определении распространения требований указанных федеральных законов следует учитывать следующие основные понятия статьи 3 N 152-ФЗ, в том числе:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

При определении распространения требований указанных Федеральных законов следует учитывать следующие основные положения и понятия статьи 1 и статьи 2 N 149-ФЗ, в том числе то, что Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

3) обеспечении защиты информации.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе:

информация - сведения (сообщения, данные) независимо от формы их представления;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Статья 14. Государственные информационные системы:

8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

В Федеральном законе от 27 декабря 2002 года N 184-ФЗ в статье 4 указано "федеральные органы исполнительной власти наделены правом издавать в сфере технического регулирования акты обязательного характера в случаях, установленных статьей 5".

Статья 5 Федерального закона от 27 декабря 2002 года N 184-ФЗ касается в том числе и продукции, используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного

доступа (в том числе "служебная информация госорганов").

Уполномоченным органом, наделенным правом устанавливать обязательные требования по защите информации, в соответствии со ст. 15 Федерального закона от 27.07.2006 N 149-ФЗ является Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

В случае, если производитель устанавливает возможность взаимодействия Программного обеспечения, являющегося медицинским изделием, с иными информационными системами (определение "иных информационных систем" приведено в постановлении Правительства Российской Федерации от 12.04.2018 N 447), он должен обеспечить защиту своего медицинского изделия от возможных угроз со стороны таких иных информационных систем. Защита должна обеспечиваться с учетом требований постановления Правительства Российской Федерации от 01.11.2012 N 1119.

Для подтверждения качества и достаточности средств защиты Программного обеспечения, являющегося медицинским изделием, необходимо предоставить сведения от уполномоченного Правительством Российской Федерации федерального органа власти.

В случае если выявляется несоответствие (в том числе опечатки и неточности), эксперт указывает об этом в том пункте заключения комиссии экспертов, который содержит анализ соответствия технической документации (Приложение А основных Методических рекомендаций).

2.9. Оценка эксплуатационной документации на Программное обеспечение.

Применяются положения основных Методических рекомендаций с учетом применения требований к Программному обеспечению, в том числе установленных приказом Минздрава России от 19 января 2017 года N 11н:

6. Эксплуатационная документация производителя (изготовителя) на медицинское изделие (далее - эксплуатационная документация), представляемая производителем (изготовителем) или уполномоченным представителем производителя (изготовителя), в составе регистрационного досье на медицинское изделие, должна содержать:

11) информацию для проверки правильности установки (монтажа) медицинского изделия и его готовности к безопасной работе эксплуатации, включая:

б) перечень предоставленных производителем (изготовителем) медицинского изделия сведений, ключей, паролей доступа, программ, необходимых для монтажа, наладки, эксплуатации и технического обслуживания медицинского изделия;

Критерии несоответствия - по основным Методическим рекомендациям (все по применимости к конкретному Программному обеспечению), с учетом следующих особенностей:

а) отсутствуют сведения, регламентирующие конструкцию, условия и правила эксплуатации Программного обеспечения <1>;

<1> Примечание:

- в соответствии с Примечанием <1> пункта 2.8 настоящих Методических рекомендаций:

- в описании Программного обеспечения не определены все целевые рабочие

задачи, которые могут быть выполнены данным Программным обеспечением;

- не определена система (технические и программные средства и их конфигурация), необходимая для ввода Программного обеспечения в эксплуатацию, включая наименования изготовителей и обозначения типов всех ее частей, например: процессоры, объем основной (оперативной) памяти, типы и объемы (памяти) периферийных запоминающих устройств, оборудование ввода и вывода, сетевое оборудование, системные и прочие программные средства;

- не указаны программные средства управления предупреждением и оповещением оператора;

- не определен каждый физический компонент Программного обеспечения, в частности, все печатные документы и все носители данных;

- не предусмотрено (или недостаточно предусмотрено) удобство и простота использования (эксплуатационная пригодность), которые чувствительны к человеческим ошибкам и обучению (поддержка операций, выполняемых вручную, взаимодействие между человеком и оборудованием, ограничения в отношении персонала, сведения о том, где требуется пристальное человеческое внимание);

- не установлен (не определен) план (или планы) технической поддержки Программного обеспечения для выполнения деятельности и задач процесса технической поддержки;

- не представлены сведения о порядке инсталляции Программного обеспечения;

- не приведен обзор функций Программного обеспечения, вызываемых пользователем, необходимых для них данных и предоставляемых средств;

- не установлены граничные значения Программного обеспечения (минимальные или максимальные значения, длины ключей, максимальное число записей в файле, максимальное число критериев поиска, минимальный объем выборки и т.п.);

- не определены конкретные знания, которые необходимо усвоить пользователю для применения соответствующего Программного обеспечения (знание соответствующей технической области, знание операционной системы, знания, получаемые в результате специального обучения, знание языков, отличных от языка, на котором написано описание продукта;

- не указаны инструментальные средства для проведения настройки Программного обеспечения (в случае, если возможна настройка пользователем) и условия их применения.

б) отсутствуют сведения о наличии, наименовании и местонахождении на территории Российской Федерации уполномоченного представителя производителя, в том числе авторизованного сервиса;

в) отсутствуют сведения о мерах, предпринимаемых пользователем Программного обеспечения для обеспечения информационной безопасности <1>.

<1> Примечание:

К таким сведениям относятся:

- не указан порядок применения имеющихся ключей доступа, а также порядок

определения пользователей с санкционированным доступом;

- отсутствуют сведения об уровне конфиденциальности информации, в том числе информации о пациенте, применяемой для осуществления функционирования Программного обеспечения;

- отсутствуют сведения о надлежащем кодировании (при необходимости) информации, предназначенной для передачи по интернет-сетям открытого доступа (например, в режиме телемедицинских консультаций);

- отсутствуют сведения о порядке обеспечения пользователем защиты информации, предназначенной для длительного хранения, от несанкционированного удаления;

- отсутствуют критерии оценки возможного повреждения и нарушения архитектуры Программного обеспечения для свидетельства попытки несанкционированного доступа.

В случае, если производитель устанавливает возможность взаимодействия Программного обеспечения, являющегося медицинским изделием, с иными информационными системами (определение "иных информационных систем" приведено в постановлении Правительства Российской Федерации от 12.04.2018 N 447), он должен информировать потребителя о возможных угрозах со стороны таких иных информационных систем. Информирование потребителя должно обеспечиваться с учетом требований постановления Правительства Российской Федерации от 01.11.2012 N 1119.

2.10. Оценка фотографических изображений медицинского изделия.

Проверяется наличие фотографий, предусмотренных подпунктом "д)" пункта 10 Правил государственной регистрации.

В качестве фотографий Программного обеспечения рассматриваются:

а) фотографическое изображение электронного носителя (при поставке Программного обеспечения на физическом носителе);

б) фотографическое изображение (скриншот) экрана в случае поставки Программного обеспечения без участия физического электронного носителя (по сети Интернет).

Фотография должна позволять четко и однозначно идентифицировать Программное обеспечение, включая его версию/дату выпуска.

2.11. Оценка объема и полноты проведенных технических испытаний Программного обеспечения.

Применяются положения основных Методических рекомендаций с учетом применения требований к Программному обеспечению. Перечень стандартов, рекомендуемых для подтверждения соответствия при проведении технических испытаний в аккредитованной испытательной организации, приведен в [разделе](#) Введение настоящих методических рекомендаций.

Для проведения испытаний системы Программного обеспечения должны быть определены и выполнены испытания, выраженные как входные данные, ожидаемые результаты, критерии приемки и процедуры, с целью учета всех требований Программного обеспечения.

Критерии несоответствия - по основным Методическим рекомендациям (все по применимости к конкретному Программному обеспечению), с учетом следующих

особенностей, в результирующих документах по техническим испытаниям:

- не определены тестируемые функции, тестовые данные, процедура тестирования, среда тестирования и другие условия (уточнение конфигурации средств испытаний и подготовительная работа);

- не представлены сведения о программных модулях, которые должны быть интегрированы в программные элементы и программные системы;

- не определены и не испытаны аппаратные элементы, программные элементы и поддержка ручного управления (например, интерфейс, приспособленный для человека, диалоговые меню подсказки, распознавание речи, речевое управление системой), интегрированные в систему;

- не приведены результаты тестирования комбинаций требований, для случаев если между требованиями существуют зависимости.

2.12. Оценка проведения тестирования информационной безопасности.

Под информационной безопасностью Программного обеспечения понимается состояние сохранности полноты, целостности, точности полученных данных и конфиденциальности при передаче, хранении и анализе данных пациентов. Неверный анализ или нарушенная передача информации о пациенте может привести к неправильной или несвоевременной диагностике и терапии.

При проведении оценки информационной безопасности рекомендуется опираться на положения ГОСТ Р 51188-98 "Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство". Испытательная организация может применять для тестирования защищенности Программного обеспечения и другие действующие нормативные документы и стандарты в соответствии со своей областью аккредитации.

Проверяются результаты технических испытаний Программного обеспечения на наличие оценки, представленной производителем (изготовителем) технической и эксплуатационной документации в части:

- соблюдения норм информационной безопасности при сохранении необходимого объема и своевременной доступности информации;

- наличия идентификации и внедрения безопасных и формализованных способов получения, хранения, преобразования и передачи данных;

- использования надлежащих мер контроля для обеспечения целостности данных в тех случаях, когда доступ к общей информации осуществляется несколькими видами Программного обеспечения;

- определения всех возможных опасностей при обновлении Программного обеспечения;

- обеспечения защиты конфиденциальной информации, в том числе в части достаточного контроля доступа и соответствующих ограничений системных настроек и процессов;

- обеспечения и учета возможных неблагоприятных взаимодействий Программного обеспечения с другими системами с включением соответствующих мер устойчивости и надежности.

2.13. Оценка документов, подтверждающих результаты испытаний медицинского

изделия в целях утверждения типа средств измерений (в отношении медицинских изделий, относящихся к средствам измерений в сфере государственного регулирования обеспечения единства измерений, перечень которых утверждается Министерством здравоохранения Российской Федерации).

Применяются положения основных Методических рекомендаций.

2.14. Оформление результатов экспертизы.

Результаты экспертизы оформляются в соответствии с основными Методическими рекомендациями.

3. Экспертиза полноты и результатов проведенных технических испытаний, клинических испытаний, а также испытаний в целях утверждения типа средств измерений Программного обеспечения (этап II)

3.1. Применяются все положения основных Методических рекомендаций с некоторыми дополнениями и уточнениями.

3.2. Оценка результатов технических испытаний и испытаний для целей утверждения типа средств измерений проводится в соответствии с [разделом 2](#) настоящих Методических рекомендаций.

3.3. Программное обеспечение - медицинское изделие должно проходить клинические исследования, целью которых должно служить подтверждение эффективности, безопасности использования, а также соответствие его характеристик использованию по назначению, указанному изготовителем.

3.4. В ходе клинических исследований должна быть дана клиническая оценка клинической связи (научной обоснованности), т.е. степени адекватности подбора данных и системы их анализа (концепция, измерения, заключение) целевому назначению. Оценка клинической значимости может подтвердить, что:

- Программное обеспечение имеет устойчивую клиническую связь, базирующуюся на документально подтвержденных результатах, как это определено в клинических рекомендациях, клинических исследованиях в рецензируемых журналах, согласии на использование Программного обеспечения, международных справочных материалах или других подобных хорошо зарекомендовавших себя данных;

- Программное обеспечение имеет новую клиническую значимость, базирующуюся на способности использовать новые входные данные, алгоритмы или результаты, новую целевую группу или новое предназначение.

3.5. Определение клинического значения является необходимым компонентом клинической оценки для любого Программного обеспечения, являющегося медицинским изделием и может быть продемонстрировано ссылками:

а) на существующие данные исследований, проведенных для того же предполагаемого использования;

б) на существующие данные исследований, проведенных для другого предполагаемого использования, где может быть оправдана экстраполяция таких данных;

в) генерацией и определением новых клинических данных для конкретного предполагаемого использования Программного обеспечения.

3.6. Необходимость проведения клинических испытаний Программного обеспечения

с участием человека в качестве субъекта устанавливается в соответствии с критериями пункта 37 Порядка, установленного приказом Минздрава России от 09.01.2014 N 2н.

БЛОК-СХЕМА ПРОВЕДЕНИЯ КЛИНИЧЕСКОЙ ОЦЕНКИ



3.7. Результаты клинических испытаний Программного обеспечения (как и любого другого медицинского изделия) должны быть оформлены в соответствии с Приложениями к приказу Минздрава России от 09.01.2014 N 2н.

3.8. Для проведения клинических испытаний необходимость инсталляции Программного обеспечения с применением технических средств клинической организации определяется испытательной клинической организацией и отражается в Программе проведения клинических испытаний.

В случае инсталляции (деинсталляции) программного обеспечения для проведения клинических испытаний медицинской организации следует руководствоваться положениями постановления Правительства Российской Федерации от 6 июля 2015 года N 676.

3.9. При оценке результатов клинических испытаний следует учитывать следующее:

- при проведении клинических испытаний Программного обеспечения как медицинского изделия для диагностики *in vitro* Программное обеспечение проверяется с применением биоматериалов и всего необходимого оборудования (в том числе медицинских изделий), предназначенного для обеспечения надлежащей работы Программного обеспечения;

- при проведении испытаний с участием человека в качестве субъекта Программное обеспечение проверяется с применением биоматериалов и всего необходимого оборудования (в том числе медицинских изделий), предназначенного для обеспечения надлежащей работы Программного обеспечения;

- в процессе проведения клинических испытаний Программного обеспечения как

медицинского изделия для диагностики *in vitro* или испытаний с участием человека в качестве субъекта должны быть задействованы все модули Программного обеспечения (при модульной архитектуре), опробованы все функции, указанные производителем в эксплуатационной документации (в случае невозможности такого опробования должны представляться подробные пояснения причин);

- в связи с тем, что Программное обеспечение для проведения клинических испытаний устанавливается (устанавливается) на соответствующем оборудовании до получения регистрационного удостоверения, в Протоколе клинических испытаний медицинских изделий для диагностики *in vitro* или испытаний с участием человека в качестве субъекта должны быть сведения о деинсталляции Программного обеспечения;

- при проведении клинических испытаний Программного обеспечения без участия человека в качестве субъекта должны быть оценены все позиции доказательных баз (клинические данные, анализ взаимозаменяемых медицинских изделий и т.п.), представленных производителем (изготовителем) в медицинскую организацию;

- при проведении клинических испытаний Программного обеспечения (любых) испытательная медицинская организация в обязательном порядке оценивает эксплуатационный документ (руководство пользователя) и делает вывод как о том, что содержание документа доступно и понятно специалистам соответствующего профиля, так и о том, что его содержание обеспечивает надлежащее эффективное и безопасное медицинское применение.

4. Экспертиза качества, эффективности и безопасности Программного обеспечения (медицинского изделия) 1 класса потенциального риска и медицинских изделий для диагностики *in vitro*

4.1. Применяются все положения основных Методических рекомендаций с некоторыми дополнениями и уточнениями.

4.2. Для изделий 1-го класса потенциального риска и медицинских изделий для диагностики *in vitro* осуществляется экспертиза заявления о регистрации и документов, указанных в пункте 10 Правил государственной регистрации, полноты и результатов проведенных технических испытаний, токсикологических исследований, клинических испытаний, а также испытаний в целях утверждения типа средств измерений <1>.

<1> Примечание: в случае, если программное обеспечение для диагностики *in vitro* (например, Лабораторная информационная система (ЛИС)) входит в состав (как модуль) другого программного обеспечения, имеющего в назначении, кроме диагностики *in vitro*, и другие функции (например Медицинская информационная система (МИС)), то к нему не применяются положения Правил регистрации, установленные для медицинских изделий для диагностики *in vitro* в части одноэтапности экспертизы, а экспертиза выполняется на общих основаниях, в два этапа.

4.3. Результаты экспертизы оформляются Заключением комиссии экспертов в соответствии с формой Приложения 3 Порядка проведения экспертизы, порядок заполнения формы Заключения приведен в Приложении А основных Методических рекомендаций.

4.4. Экспертиза документов, указанных в пункте 10 Правил государственной регистрации, полноты и результатов проведенных технических испытаний, токсикологических исследований, а также испытаний в целях утверждения типа средств измерений осуществляется в порядке, указанном в [разделе 2](#) настоящих Методических

рекомендаций.

4.5. Экспертиза полноты и результатов проведенных клинических испытаний осуществляется в порядке, указанном в [разделе 3](#) настоящих Методических рекомендаций.

5. Экспертиза для определения возможности (невозможности) внесения изменений в документы, входящие в регистрационное досье на Программное обеспечение (медицинские изделия)

5.1. Применяются все положения основных Методических рекомендаций.

5.2. В соответствии с пунктом 39 Правил государственной регистрации и Порядком проведения экспертизы экспертиза комплекта документов проводится в порядке, аналогичном порядку проведения экспертизы качества, эффективности и безопасности медицинского изделия для его государственной регистрации со следующими дополнениями:

5.2.1. Производитель (изготовитель) предоставляет сведения об изменении в документации регистрационного досье (прежде всего, в технической и эксплуатационной документации) в случае обновления программного обеспечения, если такое обновление затрагивает:

- порядок установки (инсталляции) программного обеспечения;
- функциональные технические характеристики (например, расширение и (или) уменьшение функций);
- внешний вид ярлыка (значка), обычно располагаемого на "рабочем столе" программного обеспечения;
- порядок работы с программным обеспечением (в этом случае необходимо предоставление новой версии руководства пользователя с идентификационным номером версии);
- любые другие изменения, которые необходимо принимать во внимание пользователю (в том числе медицинской организации) при применении программного обеспечения.

5.2.2. Производитель (изготовитель) предоставляет сведения в случае изменения электронного носителя программного обеспечения и предоставляет соответствующие фотографические изображения.

5.3. В соответствии с пунктом 39 Правил государственной регистрации регистрирующий орган оформляет и выдает задание на проведение экспертизы качества, эффективности и безопасности медицинского изделия экспертному учреждению.

5.4. Результаты экспертизы оформляются в соответствии с формой Приложения 4 Порядка проведения оценки. Детализированный пример и порядок заполнения формы Заключения приведен в Приложении А основных Методических рекомендаций.
