МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ КРЫМ

ПРИКАЗ

от «22» 04 2019 г. № 725

г. Симферополь

Об организации информационного взаимодействия медицинских организаций с государственной информационной системой «Единая медицинская информационная система здравоохранения Республики Крым» и внесении изменений в приказ Министерства здравоохранения Республики Крым от 19 февраля 2018 года № 267

В соответствии с Федеральным законом Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», статьей 79 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Приказами ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», Положением о Министерстве здравоохранения Республики Крым от 27 июня 2014 года № 149 (с изменениями), с целью обеспечения информационной безопасности при работе с Единой медицинской информационной системой здравоохранения Республики Крым,

ПРИКАЗЫВАЮ:

1. Внести изменения в приказ Министерства здравоохранения Республики Крым от 19 февраля 2018 года № 267 «Об утверждении

концепции информационной безопасности государственной информационной системы «ЕМИСЗ РК » изложив приложение 1 к нему в новой редакции.

2. Утвердить Единый регламент организации информационного взаимодействия медицинских организаций с государственной информационной системой «Единая медицинская информационная система здравоохранения Республики Крым» (приложение 1) к настоящему приказу.

3. Утвердить Типовое соглашение о защищенном информационном взаимодействии (приложение 2) к настоящему приказу.

4. Директору Государственного бюджетного учреждения Республики Крым «Крымский медицинский информационно-аналитический центр» Сагайдаку И.В.:

4.1. Разработать и довести в срок до 22 апреля 2019 года до руководителей медицинских организаций методические материалы (инструкции) о выполнении обязательных требований при подключении и работе с Единой медицинской информационной системой здравоохранения Республики Крым (далее – ЕМИСЗ РК).

4.2. В срок до 25 апреля 2019 года обеспечить техническую возможность подключения медицинских организаций к ЕМИСзРК исключительно с использованием персональной авторизации пользователей ЕМИСЗ РК на едином контролере безопасности Министерства здравоохранения Республики Крым – mzrk.local.

4.3. Обеспечить техническую и консультационную поддержку медицинских организаций, относящихся к ведению Министерства здравоохранения Республики Крым, при подключении автоматизированного рабочего места медицинских организаций к едином контролеру безопасности Министерства здравоохранения Республики Крым – mzrk.local собственными силами или с привлечением специализированных организаций.

5. Руководителям медицинских и фармацевтических организаций, относящихся к ведению Министерства здравоохранения Республики Крым, организовать работу по выполнению требований Концепции информационной безопасности и единого регламента информационного взаимодействия, а также в срок до 30 апреля 2019 года выполнение работ по подключению автоматизированных рабочих (используемых в работе ЕМИСЗ РК) к едином контролеру безопасности министерства здравоохранения – mzrk.local.

6. Контроль за исполнением настоящего приказа возложить на заместителя министра здравоохранения Республики Крым Деркача Н.Н.

Министр **А. Голенко**

Приложение 1
к приказу Министерства
здравоохранения Республики Крым
от 19 февраля 2018 года № 267
(в редакции приказа Министерства
здравоохранения Республики Крым
от «22» апреля 2019 г. №725)

КОНЦЕПЦИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ
«ЕДИНАЯ МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ КРЫМ»

г. Симферополь
2019 г.

Содержание

1. Перечень сокращений и определений

Единая государственная информационная система в сфере здравоохранения (далее - ЕГИСЗ) – совокупность информационно-технологических и технических средств, обеспечивающих информационную поддержку методического и организационного обеспечения деятельности участников системы здравоохранения.

Единая медицинская информационная система здравоохранения Республики Крым (далее - ЕМИСЗ РК) – государственная информационная система Республики Крым, состоящая из комплекса программных и технических средств, баз данных, обеспечивающих информационно-технологическую поддержку функционирования системы здравоохранения Республики Крым, и предназначенную для выполнения функций регионального фрагмента ЕГИСЗ.

Министерство здравоохранения Республики Крым (далее-МЗ РК) – исполнительный орган государственной власти Республики Крым, проводящий государственную политику и осуществляющий функции по нормативно-правовому регулированию в сфере охраны здоровья граждан на территории Республики Крым, контроль в сфере охраны здоровья, отраслевое или межотраслевое управление в наиболее важных отраслях и установленных сферах деятельности, оказание государственных услуг в сфере охраны здоровья и управление государственным имуществом, а также координирующий в установленных случаях деятельность в этой сфере иных исполнительных органов государственной власти Республики Крым.

Медицинская организация (далее-МО) – организация, осуществляющая деятельность в области здравоохранения или оказания медицинских услуг, поддерживающая развитие медицины как науки, занимающаяся мероприятиями по поддержанию здоровья и оказания медицинской помощи людям посредством изучения, диагностики, лечения и возможной профилактики болезней и травм.

Оператор информационной системы (далее-оператор) – физическое или юридическое лицо, осуществляющее деятельность по эксплуатации информационной систем, в том числе по обработке информации, содержащейся в ее базе данных.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная безопасность – непрерывный во времени процесс обеспечения конфиденциальности (кроме общедоступной информации), целостности и доступности защищаемой информации.

Средства обеспечения информационной безопасности ЕМИСЗ РК – технические и организационные меры, используемые для обеспечения информационной безопасности ЕМИСЗ РК.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Государственные информационные системы (далее-ГИС) – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

Персональные данные (далее-ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователи ЕМИСЗ РК – сотрудники МО, сотрудники органа управления здравоохранением, пациенты МО, иные участники информационного взаимодействия в сфере здравоохранения (на основании заключенных договоров), участвующие в функционировании ЕМИСЗ РК или использующие результаты ее функционирования.

Средства криптографической защиты информации (СКЗИ) – Реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

Защищенная локально-вычислительная сеть (далее-ЗЛВС) – закрытая сеть для обеспечения защиты информации.

Несанкционированный доступ (далее-НСД) – доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Средство защиты информации от несанкционированного доступа (далее-СЗИ от НСД) – набор программных или программно-аппаратных средств защиты информации, реализующих функции защиты от НСД путем разграничения доступа.

Антивирусное программное обеспечение (далее-АвПО) – программное обеспечение для обнаружения компьютерных вирусов и нежелательных программ, а также для предотвращения заражения файлов или операционной системы вредоносным кодом.

Основные руководящие документы (далее-ОРД) – это документы, в которых четко описана техническая сторона производственной деятельности.

АРМ в защищенном исполнении – АРМ, с установленным СЗИ от НСД, АВПО и лицензионное ПО.

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации.

2. Общие положения

В соответствии с постановлением Совета министров Республики Крым от 20 декабря 2016 года №612 «О единой медицинской информационной системе здравоохранения Республики Крым» для ПДн, содержащихся в ЕМИСЗ РК выполняются мероприятия по исключению неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

Защита ПДн, обрабатываемых в ЕМИСЗ РК, осуществляется в соответствии с требованиями ст. 19 Федерального закона (далее-ФЗ РФ) от 27.07.2006 г. №152 «О персональных данных», нормативными актами Правительства РФ, принятым во исполнение указанного закона, нормативными актами и руководящими документами федеральных органов исполнительной власти, уполномоченных в области безопасности, а также в области противодействия иностранным техническим разведкам и технической защиты информации.

Защита ПДн, обрабатываемых в ЕМИСЗ РК, достигается также за счет выполнения комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, СЗИ от НСД, АвПО и защищенного канала передачи данных.

В соответствии со ст. 79 Федерального закона от 21 ноября 2011 года N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», соблюдение врачебной тайны, в том числе персональных данных, используемых в медицинских информационных системах, является обязанностью любой медицинской организации.

Концепция безопасности информации государственной информационной системы «Единая медицинская информационная система здравоохранения Республики Крым» является официальным документом и представляет собой систему взглядов на организацию и функционирование процессов обеспечения безопасности информации, в том числе персональных данных, обрабатываемых в системе.

Настоящая концепция определяет основные цели и задачи, а также стратегию построения системы защиты информации Единой медицинской информационной системы здравоохранения Республики Крым. Концепция определяет основные требования и подходы к их реализации, необходимые для достижения необходимого уровня безопасности информации.

Концепция разработана в соответствии с постановлением Совета Министров Республики Крым от 20 декабря 2016 года № 612 «О единой медицинской информационной системе здравоохранения Республики Крым», «Техническим проектом на создание информационно-технологической инфраструктуры лечебно-профилактических учреждений Министерства здравоохранения Республики Крым».

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности медицинских организаций, осуществляющих эксплуатацию Единой медицинской информационной системы здравоохранения Республики Крым.

Концепция является методологической основой для:

– формирования и проведения единой политики в области обеспечения защиты информации в Единой медицинской информационной системе здравоохранения Республики Крым;

– формирования единых требований к автоматизированным рабочим местам пользователей Единой медицинской информационной системе здравоохранения Республики Крым;

– координации деятельности медицинских организаций при разработке организационно-распорядительной документации по защите информации, содержащейся в Единой медицинской информационной системе здравоохранения Республики Крым.

Область применения Концепции распространяется на медицинские организации и другие Учреждения, эксплуатирующие Единую медицинскую информационную систему здравоохранения Республики Крым, а также на подразделения или организации, осуществляющие сопровождение, обслуживание и обеспечение функционирования Единой медицинской информационной системы здравоохранения Республики Крым.

Данная Концепция не распространяется на другие информационные системы, используемые в медицинских организациях.

Правовой основой для разработки настоящей Концепции служат требования действующих в Российской Федерации законодательных и нормативных документов по обеспечению безопасности информации и персональных данных.

2.1. Объекты защиты

В соответствии с п.8 Приказа ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», объектами защиты в ЕМИСЗ РК являются:

– обрабатываемая информация;

– программные, технические и программно-технические средства обработки информации;

– средства защиты информации;

– средства и системы связи и передачи данных;

– общесистемное, прикладное, специальное программное обеспечение.

ЕМИСЗ РК имеет клиент-серверную архитектуру, включает серверную часть, состоящую из сервера баз данных, сервера приложений, веб-сервера, и клиентскую часть – «тонкого клиента» (веб-браузера) и реализуется для работы по модели «облачных вычислений». В состав объектов защиты ЕМИСЗ РК входят автоматизированные рабочие места, серверы, структурированная кабельная система, средства защиты информации.

3. Основные цели и задачи обеспечения информационной безопасности

3.1. Цели обеспечения информационной безопасности

Основными целями обеспечения информационной безопасности являются:

– предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию;

– повышение качества оказания населению государственных и муниципальных услуг в электронном виде в сфере здравоохранения;

– повышение эффективности использования современных информационных технологий;

– соответствие применяемых мер защиты информации действующему законодательству Российской Федерации, нормативным и методическим документам уполномоченных органов.

3.2. Задачи обеспечения информационной безопасности

Задачами деятельности по обеспечению информационной безопасности являются:

– формирование и проведение единой политики в области обеспечения защиты информации в ЕМИСЗ РК;

– формирование единых требований к АРМ пользователей ЕМИСЗ РК;

– координация деятельности МО при разработке организационно-распорядительной документации по защите информации, содержащейся в ЕМИСЗ РК.

– поддержание системы информационной безопасности в состоянии, устойчивом к существующим и вновь выявляемым угрозам в информационной сфере;

– разработка и внедрение в информационную инфраструктуру МО современных методов и средств обеспечения информационной безопасности;

– организация контроля состояния и оценки эффективности системы информационной безопасности и реализация мер по её совершенствованию.

4. Правовые основы деятельности по обеспечению безопасности персональных данных

Деятельность по обеспечению информационной безопасности, должна осуществляться в рамках действующего законодательства, руководящих документов уполномоченных государственных органов исполнительной власти, рекомендаций Министерства здравоохранения РФ, ведомственных документов МЗ РК и настоящей Концепции.

В части организации обработки и защиты персональных данных следует руководствоваться следующими документами:

– Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

– Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Федеральный закон от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

– Постановление Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

– Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление Правительства РФ №1119).

– Постановление Правительства РФ от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

– Постановление Правительства РФ от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

– Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15.02.2008, утвержденная ФСТЭК РФ

– План мероприятий ("Дорожной карты") по развитию Единой государственной информационной системы в сфере здравоохранения (далее - ЕГИСЗ) в 2015 - 2018 гг., в соответствии с Соглашением между Министерством здравоохранения Российской Федерации и Советом Министров Республики Крым о взаимодействии в сфере развития Единой

государственной информационной системы в сфере здравоохранения в 2015 – 2018 гг. от 30 июня 2015г..

В части осуществления деятельности по обеспечению безопасности ЕМИСЗ РК следует руководствоваться следующими документами:

– Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России №17 от 11.02.2013 (далее – Приказ ФСТЭК №17);

– Меры защиты информации в ГИС, утвержденный ФСТЭК России 11 февраля 2014 года.

В части осуществления деятельности по обеспечению безопасности ПДн с помощью СКЗИ следует руководствоваться следующими документами:

– «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ №152 от 13 июня 2001 г.

– приказ ФСБ России от 10.07.2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

– «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России 31 марта 2015 года №149/7/2/6-432.

5. Организационная структура информатизации и информационной безопасности ЕМИСЗ РК

Для организации информатизации здравоохранения в Республике Крым и обеспечения информационной безопасности ЕМИСЗ РК приказом МЗ РК создается Рабочая группа.

Рабочая группа создается для решения следующих задач:

– компьютеризация и информатизация медицинской сферы;

– формирование и совершенствование элементов системы информационной безопасности ЕМИСЗ РК;

– обеспечение соответствия подсистем защиты информации ЕМИСЗ РК требованиям нормативно-правовых актов РФ, приведенным в разделе 4;

– реализация единой технической политики в части информационной безопасности при организации работ;

– мониторинг внутренних и внешних условий функционирования объектов защиты, анализ эффективности управления защитой информации и подготовка решений по корректировке состава и содержания структурных элементов системы обеспечения информационной безопасности.

Состав Рабочей группы, его организационная структура утверждается отдельным приказом МЗ РК.

В рамках обеспечения информационной безопасности ЕМИСЗ РК технический оператор обеспечивает:

– организацию процесса разработки методических документов в сфере информационной безопасности МО;

– информирование МО РК о необходимых мероприятиях по обеспечению информационной безопасности;

– контроль выполнения мероприятий по обеспечению информационной безопасности в МО.

Руководители МО:

– организуют работу по обеспечению информационной безопасности в учреждениях здравоохранения Республики Крым;

– создают подразделение (назначают сотрудника), отвечающее за обеспечение информационной безопасности;

– назначают лицо, ответственное за организацию обработки ПДн (им может быть в том числе руководитель МО);

– согласуют изменения в программном и аппаратном обеспечении АРМ ЕМИСЗ РК с Рабочей группой.

Работники МО, ответственные за организацию обработки персональных данных:

– организуют взаимодействие с субъектами персональных данных в соответствии с требованиями законодательства РФ;

– доводят до сведения работников МО положения законодательства Российской Федерации, локальных актов МЗ РК по вопросам обработки персональных данных, требований к защите персональных данных;

– осуществляют внутренний контроль соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных и доводят результаты контроля до МЗ РК.

6. Средства обеспечения информационной безопасности ЕМИСЗ РК

6.1. Общие положения.

Средства обеспечения информационной безопасности ЕМИСЗ РК – технические и организационные меры, используемые для обеспечения информационной безопасности ЕМИСЗ РК.

Защита информации, содержащейся в информационных системах, является составной частью работ по созданию и эксплуатации

информационной системы и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы защиты информации информационной системы (далее – подсистема защиты информации).

6.2. Порядок создания системы защиты информации в информационных системах.

В общем случае порядок создания систем защиты информации приведён в ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Создание системы защиты информации должно выполняться в следующем порядке:

– формирование требований к защите информации, содержащейся в информационной системе;

– разработка подсистемы защиты информации;

– внедрение подсистемы защиты информации;

– аттестация информационной системы по требованиям защиты информации (далее – аттестация информационной системы) и ввод ее в эксплуатацию.

Формирование требований к защите информации, содержащейся в информационной системе, включает:

– принятие решения о необходимости защиты информации, содержащейся в информационной системе;

– классификацию информационной системы в соответствии с Постановлением Правительства РФ №1119 и Приказом ФСТЭК России №17 (далее – классификация информационной системы);

– определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

– определение требований к подсистеме защиты информации информационной системы.

Разработка подсистемы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание подсистемы защиты информации информационной системы и включает:

– проектирование подсистемы защиты информации информационной системы;

– разработку эксплуатационной документации на подсистему защиты информации информационной системы;

– макетирование и тестирование подсистемы защиты информации информационной системы (при необходимости).

В типовых случаях разработка подсистемы защиты информации заменяется планированием внедрения подсистемы защиты информации.

Внедрение подсистемы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на подсистему защиты информации информационной системы и в том числе включает:

– установку и настройку технических и программных средств защиты информации в информационной системе;

– разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее – организационно-распорядительные документы по защите информации);

– внедрение организационных мер защиты информации;

– предварительные испытания подсистемы защиты информации информационной системы;

– опытную эксплуатацию подсистемы защиты информации информационной системы;

– анализ уязвимостей информационной системы и принятие мер по их устранению;

– приемочные испытания подсистемы защиты информации информационной системы.

Аттестация информационной системы организуется обладателем информации (заказчиком) или оператором и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие системы защиты информации информационной системы требованиям безопасности информации.

Повторная аттестация информационной системы осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

6.3. Мероприятия по обеспечению информационной безопасности

Мероприятия по обеспечению информационной безопасности ЕМИСЗ РК должны носить упреждающий характер и быть направлены на предотвращение инцидентов, реализующих угрозы безопасности информации.

При выборе мер защиты информации, обрабатываемой с применением средств автоматизации необходимо определить актуальные угрозы для данной ИС, тип обрабатываемых данных, тип самой ИС, её класс защищённости и иные параметры, определяемые действующим

законодательством в качестве основополагающих при выборе правил и мер защиты информации.

В целях нейтрализации угроз безопасности информации применяются организационные и технические меры защиты информации.

Организационные меры обеспечения информационной безопасности предусматривают:

– назначение ответственных за организацию обработки ПДн, за обеспечение безопасности информационной системы, за техническое обслуживание информационной системы, за проведение мероприятий по обезличиванию обрабатываемых ПДн, за хранение материальных носителей информации;

– ознакомление сотрудников с законодательством и внутренними документами МЗ РК в области информационной безопасности;

– обучение сотрудников, непосредственно осуществляющих обработку ПДн, правилам безопасной работы с персональными данными;

– повышение квалификации специалистов по защите информации и лиц, ответственных за организацию защиты информации;

– назначение ответственности сотрудников и руководителей всех уровней за выполнение установленных требований по защите информации;

– проведение контроля соблюдения сотрудниками требований по обеспечению информационной безопасности;

– обезличивание ПДн в случаях, когда не требуется определение субъекта персональных данных;

– прием и обработку обращений и запросов субъектов ПДн или их представителей;

– установление уровней защищенности ПДн в ИСПДн;

– установление класса защищенности ГИС;

– оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей по защите ПДн;

– уведомление уполномоченного органа по защите прав субъектов ПДн (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) о начале обработки ПДн в соответствии со ст.22 Федерального закона № 152-ФЗ;

– выявление угроз безопасности и разработку моделей угроз и нарушителя;

– управление доступом сотрудников к информационной системе;

– назначение минимально необходимых прав и привилегий пользователям;

– регистрацию всех действий пользователей;

– обучение пользователей и персонала, обслуживающего системы защиты информации, правилам и способам работы с подсистемой информационной безопасности;

– учет машинных носителей информации;

– применение средств защиты информации, прошедших обязательный контроль соответствия требованиям нормативных документов по защите информации;

– мероприятия по обеспечению физической безопасности средств вычислительной техники и материальных носителей информации;

– оценку эффективности реализованных мер по обеспечению безопасности ПДн (аттестация ЕМИСЗ РК и ее сегментов по требованиям безопасности информации);

– унификацию и стандартизацию средств защиты информации;

– проведение анализа эффективности и достаточности принятых мер по защите информации;

– разработку и реализацию предложений по совершенствованию систем защиты информации;

– выявление незарегистрированных технических устройств и программного обеспечения, в том числе имеющего признаки контрафактности;

– противодействие перехвату информации в каналах связи;

– организацию безопасного доступа к ресурсам сети Интернет;

– резервирование информации и ее восстановление в случае возникновения инцидентов безопасности информации;

– обеспечение гарантированной доступности информационных ресурсов информационных систем с помощью:

– резервирования оборудования и каналов связи;

– балансировки нагрузки на сервера и каналы связи;

– обеспечения гарантированного электропитания;

– контроль, в том числе с использованием программных и технических средств, за действиями пользователей и реакцию на нарушение установленных мер защиты.

Технические меры обеспечения безопасности ПДн включают использование средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации и шифровальных (криптографических) средств защиты информации.

7. Механизмы реализации концепции

7.1. Общие положения.

В общем случае, реализация требований настоящей Концепции состоит из следующих шагов:

– реализация организационной структуры системы информационной безопасности МЗ РК и МО РК;

– разработка внутренних организационно-распорядительных документов;

– реализация технических мер защиты информации с последующей процедурой оценки эффективности.

В целях рационального расходования денежных средств и обеспечения непрерывности процесса оказания государственных и муниципальных услуг допускается разбиение работ по построению и модернизации подсистем информационной безопасности на отдельные этапы. При этом необходимо понимать, что в любом случае, процесс построения и модернизации систем информационной безопасности должен вестись непрерывно до достижения своих целей. Разбиение таких работ на этапы не подразумевает возможность приостановки работ, а только лишь позволяет расставить приоритеты в реализации определённых законодателем мер по защите информации.

7.2. Организационные и технические меры.

7.2.1. Разработка внутренних организационно-распорядительных документов.

В качестве первоочередного мероприятия должна выполняться разработка комплекта организационно-распорядительной документации (далее-ОРД) по защите персональных данных, обрабатываемых в ЕМИСЗ РК.

Документы, обеспечивающие деятельность по защите ПДн, обрабатываемых в ЕМИСЗ РК, разрабатываются самостоятельно (силами МО РК) с помощью специализированного Регионального ПО, доступ к которому будет предоставлен всем МО РК, эксплуатирующим ЕМИСЗ РК.

Региональное ПО должно удовлетворять следующим критериям:

– предоставляться организацией, специализирующейся в области защиты информации, имеющей лицензии ФСТЭК и ФСБ России.

– отвечать требованиям круглосуточной доступности и высокому уровню технической поддержки.

– обеспечивать возможность разработки документов в объеме необходимом и достаточном для реализации требований законодательства РФ в области безопасности ПДн.

– должно быть зарегистрировано в реестре Отечественного ПО.

Технический оператор должен иметь возможность осуществить контроль процесса выполнения разработки ОРД по защите ПДн, обрабатываемых в ЕМИСЗ РК. Для координации деятельности МО РК по разработке ОРД, МЗ РК совместно с техническим оператором организует единое мероприятие по обучению сотрудников МО РК по работе с Региональным ПО.

7.2.2. Реализация технических мер защиты информации.

Перечень технических мер защиты информационных систем формируется в соответствие с требованиями приказов ФСТЭК России № 17 и № 21.

Перечень технических мер защиты информационных систем включает в себя следующие группы:

– Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ).

– Управление доступом субъектов доступа к объектам доступа (УПД).

– Ограничение программной среды (ОПС).

– Защита машинных носителей информации (ЗНИ).

– Регистрация событий безопасности (РСБ).

– Антивирусная защита (АВЗ).

– Обнаружение вторжений (СОВ).

– Контроль (анализ) защищенности информации (АНЗ).

– Обеспечение целостности информационной системы и информации (ОЦЛ).

– Обеспечение доступности информации (ОДТ).

– Защита среды виртуализации (ЗСВ).

– Защита технических средств (ЗТС).

– Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС).

Перечень защитных мер должен быть адаптирован применительно к структурно-функциональным характеристикам выбранной информационной системы и особенностям её функционирования. Допускается исключение из перечня мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе.

При невозможности реализации в информационной системе, в рамках ее системы защиты информации, отдельных выбранных мер защиты информации, могут разрабатываться компенсирующие меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации. Достаточность и адекватность компенсирующих мер подтверждается в ходе аттестационных испытаний информационной системы.

7.3. Средства защиты информации.

В составе подсистемы информационной безопасности информационных систем допускается использовать только средства защиты информации, сертифицированные на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также требуемого класса защищенности. В случае, если с помощью сертифицированных средств защиты невозможно реализовать отдельные защитные меры, должны разрабатываться компенсирующие меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

7.4. Использование существующих средств защиты информации.

Для защиты информации, обрабатываемой в ЕМИСЗ РК, МЗ РК совместно с организацией-лицензиатом ФСТЭК и ФБС России, был выполнен комплекс технических мер, направленных на реализацию требований законодательства в области защиты информации.

Для обеспечения защиты канала связи между операторами ЕМИСЗ РК развернута и функционирует защищенная сеть передачи данных, построенная с использованием технологии ViPNet (сеть ViPNet № 4960).

В каждую МО, для работы в ЕМИСЗ РК была осуществлена поставка АРМ в защищенном исполнении. Поставляемые АРМ оснащены сертифицированным средством защиты информации от несанкционированного доступа, а также сертифицированным антивирусным программным средством.

7.5. Требования к АРМ ЕМИСЗ РК.

Для обеспечения необходимого уровня безопасности ЕМИСЗ РК на АРМ, непосредственно участвующих в эксплуатации данной системы, должно находится только программное обеспечение (далее-ПО), необходимое для работы в ЕМИСЗ РК. Категорически запрещается устанавливать на АРМ ПО, использующее технологию «толстого клиента» с выходом в сеть Интернет к различным источникам БД, отличных от ЕМИСЗ РК, за исключением федеральных и иных ресурсов, необходимых для оказания медицинской помощи населению.

На АРМ может находится другое ПО, необходимое для выполнения производственных задач ЕМИСЗ РК, при этом данное ПО должно быть официально приобретенно МЗ РК или МО самостоятельно, или быть условно-бесплатным. К такому ПО могут быть отнесены: офисные пакеты, архиваторы, файловые менеджеры, ПО для обработки изображений и другое локальное ПО. Для установки вышеописанного ПО на АРМ, МО направляет официальное письмо в адрес «Технического оператора» ЕМИСЗ РК с описанием, версией, количеством и обоснованием производственной необходимости планируемого к установке ПО на АРМ. После рассмотрения заявки, Рабочая группа принимает решение о возможности установки данного ПО и направляет в адрес МО положительное или отрицательное заключение.

Категорически запрещается удалять средства защиты информации, функционирующие на данных АРМ.

Категорически запрещается без согласования с техническим оператором устанавливать средства защиты информации, отличные от средств защиты информации, поставляемые совместно с АРМ для работы с ЕМИСЗ РК (Приложение 1).

В целях обеспечения подтверждения источника/получателя информации, а также исключения возможности отрицания факта получения/отправки конфиденциальной информации, авторизация, подпись

медицинских документов и производственная переписка в ЕМИСЗ РК осуществляется только с применением электронной подписи.

7.6. Подключение к ЕМИСЗ РК.

Для организации подключения организации-претендента (далее-претендент) к ЕМИСЗ РК, МЗ РК утверждены Регламент подключения (далее-Регламент) и типовое Техническое задание, в которых отражены основные требования к составу технических и программных средств, средствам защиты информации, а также к мерам защиты информации. Для осуществления подключения к защищенному сегменту ЕМИСЗ РК, претендент должен выполнить все требования вышеуказанных документов. Выполнение требований проводится претендентом самостоятельно или централизовано силами МЗ РК.

В связи с научно-техническим прогрессом, а также с изменениями законодательства РФ в области защиты информации Регламент и Техническое задание подлежат актуализации сроком раз в год. Актуализация Регламента и Технического задания происходит силами технического оператора. Итоговые актуализированные документы подлежат согласованию с Рабочей группой.

7.7. Обслуживание ЕМИСЗ РК.

Обслуживание ЕМИСЗ РК осуществляется техническим оператором самостоятельно или с привлечением на договорной основе сторонних организаций, имеющих соответствующие компетенции и лицензии. В целях обеспечения штатного и бесперебойного функционирования ЕМИСЗ РК, устранения технических и иных проблем на базе технического оператора организован Единый контакт центр по приему обращений от пользователей ЕМИСЗ РК.

Порядок и сроки решения обращений от пользователей ЕМИСЗ РК отражены в «Регламенте приема обращений Единого контакт центра».

7.8. Аттестация ЕМИСЗ РК по требованиям защиты информации

Аттестация ЕМИСЗ РК по требованиям защиты информации организуется МЗ РК и включает проведение комплекса организационных и технических мероприятий, в результате которых устанавливается степень соответствия ЕМИСЗ РК безопасности информации.

Аттестация ЕМИСЗ РК должна проводиться МЗ РК с привлечением организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

По результатам аттестационных мероприятий оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям защиты информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

При выполнении МО РК требований настоящей Концепции, регламента подключения и технического задания допускается аттестация рабочих мест МО ЕМИСЗ РК, реализующих полную технологию обработки информации на основе результатов аттестационных испытаний типового рабочего места ЕМИСЗ РК.

В качестве исходных данных, необходимых для оценки эффективности реализованных мер по обеспечению информационной безопасности, должны использоваться:

– модель угроз информационной безопасности;

– акт установления уровня защищённости или акт классификации ИС;

– техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание подсистемы информационной безопасности;

– проектная и эксплуатационная документация на подсистему информационной безопасности ЕМИСЗ РК;

– организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационных систем, материалы предварительных и приёмочных испытаний системы информационной безопасности информационной системы, а также иные документы, разрабатываемые в соответствии с требованиями уполномоченных органов.

Повторная аттестация информационной системы осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищённости информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

При необходимости привлечения сторонних организаций к проведению работ по проектированию системы информационной безопасности, внедрению средств защиты информации и аттестации информационных систем, должны привлекаться организации имеющие лицензии ФСТЭК России и ФСБ России на оказание услуг в области защиты конфиденциальной информации.

Приложение

к Концепции информационной безопасности
государственной информационной системы
«Единая медицинская информационная
система здравоохранения Республики Крым»
от 19 февраля 2018 года № 267(в редакции
приказа Министерства здравоохранения
Республики Крым
от «___»_____2019г. №_____

Описание технических и программных средств обеспечения информационной безопасности ЕМИСЗ РК

1. Общая структура ЕМИСЗ РК

Общая структура ЕМИСЗ РК представлена:

- уровень ядра ЕМИСЗ РК;
- уровень МО РК.

1.1. Уровень ядра ЕМИСЗ РК

Уровень ядра ЕМИСЗ РК располагается у технического оператора и представлен центром обработки данных (далее - ЦОД), в котором располагаются сервера ЕМИСЗ РК, а также необходимое сетевое телекоммуникационное оборудование и каналы связи с МО РК и федеральным сегментом единой государственной информационной системы в сфере здравоохранения. Меры по защите ЦОД и рекомендованный состав средств защиты информации для обеспечения информационной безопасности представлен в разделе 3 настоящего Приложения.

1.2. Уровень МО РК

Уровень МО РК представляет из себя защищенный сегмент локально-вычислительной сети (далее-ЛВС) МО РК, предназначенный для работы с ЕМИСЗ РК, и АРМ в защищенном исполнении.

Защищенный сегмент ЛВС МО РК, предназначенный для работы с ЕМИСЗ, функционирует на основе персональных компьютеров, располагающихся в выделенном сегменте ЛВС МО РК и подключающихся к ЦОД технического оператора посредством организации защищенного взаимодействия по каналам связи. Меры по защите сегмента ЛВС МО РК, предназначенного для работы с ЕМИСЗ РК, и состав средств защиты информации для обеспечения информационной безопасности представлен в разделе 3 настоящего Приложения.

2. Организация защищенного межсетевого взаимодействия

Для организации защищенного межсетевого взаимодействия по каналам связи общего доступа между всеми участниками ЕМИСЗ РК должна применяться защищенная частная виртуальная сеть ViPNet № 4960.

На уровне технического оператора располагается ядро защищенной сети – ПО ViPNet Administrator, которое обеспечивает централизованное управление элементами сети ViPNet и централизованную рассылку ключей шифрования.

ПАК ViPNet Coordinator HW 2000, установленный у технического оператора в режиме горячего резервирования, обеспечивает безотказное защищенное взаимодействие с учреждениями здравоохранения, а также используется для защиты и разграничения доступа к серверам ЦОД.

На уровне МО РК должна производится установка ПАК ViPNet Coordinator HW1000, обеспечивающих защиту ЛВС МО РК от различных видов сетевых атак, а также реализующих защищенное взаимодействие с другими МО РК и ЦОД технического оператора. При территориальной удаленности зданий МО РК (т.е. в случае, если каждое здание имеет собственную локальную сеть и точку выхода в сети международного обмена), для организации безопасного межсетевого взаимодействия должна быть произведена установка ПАК в каждом территориально удаленном здании. Для отдельных, локально удаленных АРМ производится установка ViPNet Клиент для защищенного взаимодействия с сетью 4960.

Для организации работы персонала с ЕМИСЗ РК в ЛВС МО РК организуется выделенный сегмент. Межсетевое экранирование и защита каналов связи данного сегмента осуществляется ПАК ViPNet Coordinator. В случае необходимости использования дополнительных АРМ (персональных компьютеров) в качестве тонких клиентов, необходимо подключить данные АРМ к выделенному сегменту ЛВС и выполнить мероприятия по их защите. Меры по защите АРМ, используемых в качестве тонких клиентов для работы с ЕМИСЗ РК, и состав средств защиты информации для обеспечения информационной безопасности представлен в разделах 3.3-3.7.

В случае наличия в МО РК распределенных иных ИСПДн (ввиду территориальной удаленности зданий Учреждения здравоохранения) передача персональных данных должна осуществляться только посредством защищенной частной виртуальной сети ViPNet № 4960.

3. Система защиты информации

3.1. Состав системы защиты ЦОД

Для реализации мер защиты ЦОД используются следующие средства защиты информации:

- средства межсетевого экранирования;

– средства криптографической защиты информации;
– средства защиты от несанкционированного доступа (далее - НСД);
– средства антивирусной защиты;
– средства анализа защищенности;
– средства обнаружения вторжений.

3.2. Состав системы защиты сегмента МО РК, предназначенного для работы с ЕМИСЗ РК

Для реализации мер защиты защищенного сегмента МО РК, предназначенного для работы с ЕМИСЗ РК, должны использоваться следующие средства защиты информации:

– средства межсетевого экранирования;
– средства криптографической защиты информации;
– средства защиты от НСД;
– средства антивирусной защиты;
– средства анализа защищенности.

3.3. Средства межсетевого экранирования и криптографической защиты информации

В соответствии с приказом ФСТЭК России № 17 должны быть реализованы меры по разбиению информационной системы на сегменты и защита периметров сегментов (ЗИС.17), управлению информационными потоками между сегментами информационной системы и между информационными системами (УПД.3), защищенному удаленному доступу через информационно-телекоммуникационные сети (УПД.13).

Данные требования реализуются продуктовой линейкой ViPNet производства компании ИнфоТеКС, реализующей в себе функции межсетевого экранирования и криптографической защиты информации. В состав линейки, в том числе, входят следующие продукты:

– ViPNet Administrator;
– ViPNet Coordinator;
– ViPNet Client.

ПО ViPNet Administrator установлено в ГБУ РК «КМ ИАЦ». На границах подключения сегментов ГИС к сетям связи общего пользования в МО РК, ГБУ РК «КМ ИАЦ» используются криптошлюзы ViPNet Coordinator HW 1000 и HW 2000.

Данные продукты обладают сертификатами ФСТЭК И ФСБ России и позволяют использовать данные продукты для защиты ГИС до первого класса включительно.

3.4. Средства защиты от НСД.

В соответствии с приказом ФСТЭК России № 17, должны быть реализованы меры по идентификации и аутентификации пользователей (ИАФ), управлению доступом (УПД), защиты машинных носителей (ЗНИ), регистрации событий безопасности на серверах и АРМ пользователей ЕМИСЗ РК (РСБ), обеспечение целостности компонентов информационной системы (ОЦЛ).

Необходимо подобрать оптимальное решение, реализующее данные требования на серверах и АРМ пользователей ГИС. Оптимальным решением должно выступать средство защиты информации от несанкционированного доступа, обладающее сертификатом ФСТЭК России на соответствие 4-му уровню контроля отсутствия НДВ, 5-му классу защищенности от НСД. В качестве такого средства, сервера ЕМИСЗ РК, а также АРМ пользователей оснащены СЗИ от НСД Dallas Lock 8.0-K.

3.5. Средства антивирусной защиты

В соответствии с приказом ФСТЭК России № 17, должны быть реализованы меры по антивирусной защите (АВЗ).

Антивирусное программное обеспечение должно иметь сертификат ФСТЭК России на соответствие требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ» (ФСТЭК России, 2012) и «Профиль защиты средств антивирусной защиты типа В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Г четвертого класса защиты. ИТ.САВЗ.Г4.ПЗ».

Для антивирусной защиты серверов и АРМ пользователей ЕМИСЗ РК используется ссертифицированное ФСТЭК России АВПО Kaspersky Anti-Virus.

3.6. Средства анализа защищенности.

В соответствии с приказом ФСТЭК России № 17, для установленного класса ЕМИСЗ РК должны быть реализованы меры по выявлению и анализу уязвимостей информационной системы, контроль правильности настройки программного обеспечения и средств защиты информации (АНЗ).

Требования по анализу защищенности должны реализовываться сертифицированным ФСТЭК России средством защиты информации с функциями по сканированию защищенности компонентов ГИС и обнаружению уязвимостей, содержащихся в компонентах информационной системы.

Средство защиты информации с функциями сканирования защищенности компонентов ГИС и обнаружения уязвимостей должно иметь сертификат ФСТЭК России на соответствие 4-му уровню контроля отсутствия НДВ.

3.7. Средства обнаружения вторжений.

В соответствии с приказом ФСТЭК России № 17, для установленного класса ЕМИСЗ РК должны быть реализованы меры по обнаружению вторжений в сетевом трафике (СОВ.1), автоматическое обновление базы сигнатур атак (СОВ.2).

Требования по обнаружению вторжений должны быть реализованы с использованием сертифицированного ФСТЭК и ФСБ России средства

защиты информации с функцией обнаружения вторжений. Средство обнаружения вторжений устанавливается на границе подключения ЕМИСЗ РК к сети связи общего пользования.

Средство защиты информации с функцией обнаружения вторжений должно иметь сертификат ФСТЭК России на соответствие 4 классу защиты для СОВ и сертификат ФСБ России на соответствие классу В для систем обнаружения компьютерных атак.

В качестве средства обнаружения вторжений в ЦОД ЕМИСЗ РК установлен ПАК ViPNet IDS 2(версия 2.4), который полностью выполняет требования приказа ФСТЭК России № 17 и обладает необходимыми сертификатами ФСТЭК России и ФСБ России.

4. Изменение состава средств защиты информации ЕМИСЗ РК

Состав средств защиты информации, используемых в целях защиты информации, подлежит изменению только при:

– изменении законодательства Российской Федерации в области обработки и защиты персональных данных;

– изменении актуальных угроз безопасности персональных данных;

– значительных изменений технологического процесса обработки персональных данных;

– изменении технологии построения защищенной сети;

– окончании срока действия сертификатов соответствия ФСТЭК России и ФСБ России на используемые средства защиты информации.

Приложение 1
к приказу Министерства
здравоохранения Республики Крым
от «22»апреля 2019 г. №725

ЕДИНЫЙ РЕГЛАМЕНТ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МЕДИЦИНСКИХ ОРГАНИЗАЦИЙ С ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ «ЕДИНАЯ МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ КРЫМ»

Симферополь, 2019 г.

Содержание

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ГИС - государственная информационная система.

ЕГИСЗ - Единая государственная информационная система в сфере здравоохранения.

ЕМИСЗ РК – единая медицинская информационная система здравоохранения Республики Крым, состоящая из комплекса программных и технических средств, баз данных, обеспечивающих информационно-технологическую поддержку функционирования системы здравоохранения республики Крым, и предназначенную для выполнения функций регионального фрагмента ЕГИСЗ.

МО - медицинская организация, осуществляющая деятельность в области здравоохранения или оказания медицинских услуг, поддерживающая развитие медицины как науки, занимающаяся мероприятиями по поддержанию здоровья и оказания медицинской помощи людям посредством изучения, диагностики, лечения и возможной профилактики болезней и травм.

СЗИ-средства защиты информации.

КМИАЦ - Крымский медицинский информационно-аналитический центр осуществляющий организацию и управление системой медицинского статистического учета и отчетности в МО Республики Крым. Является техническим оператором ЕМИСЗ РК.

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

МЗРК-Министерство здравоохранения Республики Крым.

Информационная безопасность – непрерывный во времени процесс обеспечения конфиденциальности (кроме общедоступной информации), целостности и доступности защищаемой информации.

Информационная система персональных данных (далее-ИСПДн)-информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без

использования таких средств.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Персональные данные (далее-ПДн)- любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователи ЕМИСЗ РК – работники МО, сотрудники органа управления здравоохранением, пациенты МО, участвующие в функционировании ЕМИСЗ РК или использующие результаты ее функционирования.

Средства криптографической защиты информации (СКЗИ) – Реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

Защищенная локально-вычислительная сеть (далее-ЗЛВС) - закрытая сеть для обеспечения защиты информации.

Несанкционированный доступ (далее-НСД) - доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Средство защиты информации от несанкционированного доступа (далее-СЗИ от НСД)-набор программных или программно-аппаратных средств защиты информации, реализующих функции защиты от НСД путем разграничения доступа.

Антивирусное программное обеспечение (далее-АВПО)-программное обеспечение для обнаружения компьютерных вирусов и нежелательных программ, а также для предотвращения заражения файлов или операционной системы вредоносным кодом.

Претендент- МО, желающая осуществлять работу в ГИС ЕМИСЗ РК.

Участник – МО, осуществляющее работу в ГИС ЕМИСЗ РК.

АРМ – автоматизированное рабочее место.

ФСБ России – федеральная служба безопасности Российской Федерации.

ФСТЭК России – федеральная служба по техническому и экспортному контролю Российской Федерации.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий регламент организации информационного взаимодействия (далее - Регламент) с ГИС ЕМИСЗ РК разработан в соответствии с:

– Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее- ФЗ № 149);

– Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее- ФЗ № 152);

– Постановлением правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее- ПП РФ № 1119);

– Постановлением Правительства Российской Федерации № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (далее-ПП РФ № 211);

– Приказом ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее- Приказ ФСТЭК России № 21);

– Приказом ФСБ России № 378 от 10 июля 2014 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (далее -Приказ ФСБ России № 378).

– Приказом ФСТЭК России № 17 от 11 февраля 2013 года «Об утверждении требований о защите информации, не составляющей

государственную тайну, содержащейся в государственных информационных системах» (далее - Приказ ФСТЭК России № 17).

– Концепцией информационной безопасности государственной информационной системы «Единая медицинская информационная система здравоохранения Республики Крым» утвержденной Приказом Министерства Здравоохранения №267 от 19 февраля 2018 года.

2.2.Настоящий Регламент определяет и устанавливает порядок организации подключения медицинских организаций и учреждений здравоохранения к ГИС ЕМИСЗ РК МЗ РК.

3. ОПИСАНИЕ ГИС ЕМИСЗ РК

3.1. ЕМИСЗ РК имеет клиент-серверную архитектуру, включает серверную часть (сегмент ЦОД), состоящую из сервера баз данных, сервера приложений, веб-сервера, и клиентскую часть (пользовательский сегмент)-«тонкого клиента» (веб-браузера) и реализуется для работы по модели «облачных вычислений».

3.2. ГИС ЕМИСЗ РК создана для обработки ПДн граждан, обратившихся в МО МЗРК за получением медицинских услуг.

3.3. Цели и содержание обрабатываемых ПДн в ГИС ЕМИСЗ РК определены Техническим оператором ГИС ЕМИСЗ РК.

3.4. В соответствии с Приказом ФСТЭК России № 17 и ПП РФ № 1119 для ГИС ЕМИСЗ РК установлен второй класс защищенности с обеспечением второго уровня защищенности обрабатываемых ПДн.

3.5. При проектировании ГИС ЕМИСЗ РК были учтены требования законодательства Российской Федерации в области защиты информации (в том числе персональных данных). На момент написания настоящего регламента ГИС ЕМИСЗ РК находится в тестовой эксплуатации. По завершении процедуры аттестации ГИС ЕМИСЗ РК по требованиям безопасности информации, данная система будет введена в промышленную эксплуатацию.

3.6. Для организации защищенного канала связи между сегментом ЦОД и пользовательскими сегментами ГИС ЕМИСЗ РК, а также в целях информационного взаимодействия ГИС ЕМИСЗ РК с внешними информационными системами применяются средства криптографической

защиты информации (далее-СКЗИ) на базе продуктовой линейки «ViPNet» компании ОАО «ИнфоТеКС».

3.7. При подключении к ГИС ЕМИСЗ РК все Претенденты обязаны выполнить требования по защите информации и ПДн, установленные настоящим регламентом и действующим законодательством Российской Федерации. Выполнение требований проводится Претендентом самостоятельно или централизовано силами МЗ РК.

4. ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

4.1. Организация подключения Претендента к ГИС ЕМИСЗ РК должна осуществляться в соответствии с:

– требованиями законодательства Российской Федерации в области защиты информации и ПДн.

– требованиями настоящего Регламента.

4.2. Подключение сегмента ЗЛВС Претендента к ГИС ЕМИСЗ РК осуществляется посредством использования информационных сетей общего пользования (Интернет).

4.3. При организации подключения к ГИС ЕМИСЗ РК, Претендентом должны быть учтены все АРМ Претендента, задействованные в обработке ПДн, передаваемых в рамках информационного взаимодействия с ГИС ЕМИСЗ РК. Подключение\расширение дополнительных АРМ должно осуществляться в соответствии со специальными требованиями к организации информационного взаимодействия, указанными в разделе 6 настоящего Регламента.

4.4. Подключение Претендента к ГИС ЕМИСЗ РК осуществляется после выполнения им организационных и технических мероприятий информационной безопасности, а также проведения процедуры аттестации, подтверждающей соответствие системы защиты информации Претендента требованиям безопасности информации.

4.5. В целях реализации технических мер защиты информации на стороне Претендента должны применяться СЗИ, прошедшие процедуру оценки соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

4.6. Для организации подключения к ГИС ЕМИСЗ РК, на стороне Претендента должны применяться СКЗИ продуктовой линейки «ViPNet» компании ОАО «ИнфоТеКС».

4.7. Информационное взаимодействие Претендента и ГИС ЕМИСЗ РК осуществляется посредством защищенной частной виртуальной сети ViPNet № 4960.

5. ОРГАНИЗАЦИОНЫЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

5.1. Для организации информационного взаимодействия Претендента и ГИС ЕМИСЗ РК Претендент должен направить в адрес технического оператора ГИС ЕМИСЗ РК заявление о намерении стать участником информационного взаимодействия (далее – Заявление). Форма заявления отражена в Приложении № 1 настоящего Регламента.

5.2. В заявлении Претендент должен указать следующую информацию:

- полное и краткое наименование Учреждения;
- ИНН;
- фамилию, имя, отчество и контактные сведения лица, ответственного за организацию информационного взаимодействия;
- цель подключения к ГИС ЕМИСЗ РК;
- количество АРМ, подключаемых к ГИС ЕМИСЗ РК;
- количество и перечень СЗИ, используемых с целью защиты информации;
- сведения о конфигурации АРМ Претендента, с указанием технических характеристик и обязательным указанием чипсета материнской платы АРМ;
- сертификаты ФСТЭК РФ на используемых на АРМ СЗИ;
- сертификаты ФСБ РФ на используемые в МО средства криптографической защиты;
- NetBIOS идентификатор контролера домена безопасности Претендента, к которому подключены АРМ.
- прочие сведения.

Данная информация вносится в региональный сервис учета подсистемы информационной безопасности ЕМИСЗ РК – DocShell 4.0, под соответствующей

учетной записью МО ответственным за информационную безопасность в данном МО.

Претендент в обязательном порядке должен приложить заверенную руководителем Претендента скан.копию заявления на подключение, образец которого приведен в данном техническом Регламенте.

5.3. Технический оператор ГИС ЕМИСЗ РК в течение трёх рабочих дней со дня поступления заявления от Претендента осуществляет:

– оценку оснований для информационного взаимодействия Претендента с ГИС ЕМИСЗ РК;

– оценку технической возможности организации информационного взаимодействия с ГИС ЕМИСЗ РК;

– оценку достаточности выполнения мероприятий по защите информации на стороне Претендента.

5.4. Технический оператор ГИС ЕМИСЗ РК уведомляет ответственное за организацию информационного взаимодействия лицо Претендента о принятии решения о таком взаимодействии (отказе от взаимодействия), посредством электронного сообщения, отправленного на указанный в заявлении адрес электронной почты. Рассмотрение заявки Претедента, обсуждение, согласование или отклонение выполняется средствами онлайн сервиса DocShell 4.0.

5.5. Работы по организации информационного взаимодействия Претендента и ГИС ЕМИСЗ РК осуществляются после уведомления техническим оператором ГИС ЕМИСЗ РК ответственного лица Претендента о возможности такого взаимодействия.

5.6. По окончании работ по организации информационного взаимодействия Претендент переходит в статус Участника, а подключенные к ГИС ЕМИСЗ РК АРМ Участника образуют пользовательский сегмент ГИС ЕМИСЗ РК.

6. СПЕЦИАЛЬНЫЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

6.1. Передача информации от Претендента в сегмент ЦОД ГИС ЕМИСЗ РК должна выполняться по защищенным с использованием СКЗИ каналам связи. В качестве СКЗИ должны выступать продукты компании ОАО «ИнфоТеКС» из продуктовой линейки «ViPNet». СКЗИ могут иметь программное или

программно-аппаратное исполнение. Исполнение СКЗИ определяется исходя из количества АРМ Претендента, подключаемых к ГИС ЕМИСЗ РК.

6.2. АРМ Претендента, подключаемые к ГИС ЕМИСЗ РК должны быть оснащены сертифицированным ФСТЭК России или ФСБ России антивирусным программным обеспечением.

6.3. АРМ Претендента, подключаемые к ГИС ЕМИСЗ РК должны быть оснащены сертифицированным ФСТЭК России СЗИ от НСД полностью совместимым с продуктом «Dallas Lock 8.0-К» компании ООО «Конфидент» и входить в единый домен безопасности mzrk.local (сервер безопасности «Dallas Lock 8.0-К»), развернутый в КМИАЦ РК.

6.4. АРМ Претендента, подключаемые к ГИС ЕМИСЗ РК должны быть зарегистрированы на контроллере домена безопасности своей МО, синхронизированного с корневым контролером домена безопасности ЕМИСЗ РК.

6.5. Авторизация пользователей в учетной записи домена МО, а также СЗИ от НСД, должна выполняться с помощью носителя ключа усиленной квалифицированной электронной подписи (далее-КВЭП). Также должен быть активен аварийный режим входа под учетной записью пользователя на основе пары логин/пароль, на случай выхода из строя носителя ключа КВЭП или на момент оформления/переоформления КВЭП. Требования и единые стандарты, предъявляемые к функционалу КВЭП изложены в техническом регламенте использования усиленной квалифицированной электронной подписи при работе с ГИС ЕМИСЗ РК.

7. ПРОЧИЕ ТРЕБОВАНИЯ

7.1. Помещения, в которых размещены технические средства Участника должны удовлетворять требованиям эксплуатационной документации и требованиями уполномоченных федеральных органов в области эксплуатации таких технических средств.

7.2. Работы по первоначальной настройке и последующей эксплуатации СЗИ, в том числе СКЗИ, осуществляются в соответствии с требованиями уполномоченных федеральных органов в области обеспечения безопасности информации и ПДн, требованиями эксплуатационной документации на такие средства и требованиям настоящего Регламента.

7.3. Оптимальные технико-параметрические требования, предъявляемые эксплуатационными характеристиками ЕМИСЗ РК к АРМ и серверному оборудованию изложены в Приложении №3 данного Регламента.

8. ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ТРЕБОВАНИЙ РЕГЛАМЕНТА

8.1. Ответственность за соблюдение требований настоящего Регламента, обеспечение защиты информации, в ходе эксплуатации баз данных ГИС ЕМИСЗ РК на стороне Участника, а также ответственность за соблюдение требований к эксплуатации СЗИ и СКЗИ в составе системы защиты Участника лежит исключительно на Участнике.

Приложение №1
к Единому регламенту организации
информационного взаимодействия
с государственной информационной
системой «Единая медицинская
информационная система здравоохранения
Республики Крым», утвержденному
приказом Министерства здравоохранения
Республики Крым
от «__» _____ 2019 г. № _____

Директору ГБУЗ РК «КМИАЦ»
_____ (ФИО)

_____
(должностное лицо учреждения здравоохранения)

ЗАЯВЛЕНИЕ
на организацию информационного взаимодействия
с государственной информационной системой ЕМИСЗ РК

Прошу рассмотреть возможность организации информационного взаимодействия

_____
(наименование учреждения здравоохранения)

с государственной информационной системой ЕМИСЗ РК.

Работы по защите информации, согласно регламенту организации информационного взаимодействия, с государственной информационной системой ЕМИСЗ РК МЗРК проведены.

АРМ готовы к работе в защищенной корпоративной сети передачи данных министерства здравоохранения Республики Крым (сеть ViPNet №4960).

Сведения, необходимые в соответствии с регламентом организации информационного взаимодействия с государственной информационной системой ЕМИСЗ РК, приведены в таблице 1.

Таблица 1 – Предварительные сведения

№ п/п	Описание параметра	Значение
1	Полное наименование МО	
2	Цель подключения	
3	Краткое наименование МО	
4	ИНН	
5	Количество подключаемых АРМ	

6	Наименование абонентских пунктов в сети ViPNet №4960 / IP-адреса АРМ	
7	Количество и наименование АВПО, установленных на АРМ в подключаемом сегменте ЗЛВС	
8	Количество и наименование средств от НСД, установленных на АРМ в подключаемом сегменте ЗЛВС	
9	Конфигурация АРМ, абонентских пунктов сегмента ЗЛВС Претендента, с указанием технических характеристик и обязательным указанием чипсета материнской платы АРМ	
10	NetBIOS идентификатор контролера домена безопасности Претендента.	

Контактное лицо, ответственное за организацию информационного взаимодействия:

Должность:

_____

Ф.И.О.:

_____

Контактные данные: телефон _____, e-mail: _____.

_____
(должность руководителя)

_____/_____
(подпись) М.П. (расшифровка)

Дата составления заявления: _____

Приложение 2
к приказу Министерства
здравоохранения Республики Крым
от «22» апреля 2019 г. №725

ШАБЛОН ТИПОВОГО СОГЛАШЕНИЯ
О ЗАЩИЩЕННОМ ИНФОРМАЦИОННОМ ВЗАИМОДЕЙСТВИИ
№ _____

г. Симферополь «___» _____ 201__г.

Министерство здравоохранения Республики Крым, именуемое в дальнейшем – «Сторона 1»**,** в лице Министра здравоохранения Республики Крым Голенко Александра Ивановича, действующего на основании Положения о Министерстве здравоохранения Республики Крым, утвержденного постановлением Совета министров Республики Крым 27.06.2014 № 149, и _____, именуемый в дальнейшем – «Сторона 2», в лице директора _____, действующего на основании Устава, утвержденного приказом Министерства здравоохранения Республики Крым от _____ № _____, вместе именуемые Стороны, в целях организации использования средств защиты информации при осуществлении электронного документооборота между Сторонами, заключили настоящее Соглашение о нижеследующем.

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. Предметом настоящего Соглашения являются порядок и условия информационного взаимодействия между Сторонами в целях формирования, функционирования и координации защищенного документооборота.

1.2. Стороны осуществляют обмен документами в электронном виде.

1.3. Стороны признают, что в соответствии с Федеральным законом от 06.04.2012
№ 63-ФЗ «Об электронной подписи», полученный ими электронный документ, подписанный усиленной квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

1.4. Стороны организуют взаимодействие и координируют свою деятельность в следующих основных направлениях по защите информации:

− обмен информацией, представляющей интерес для обеих Сторон;

− организация технической эксплуатации и использование аппаратно-программных средств защиты информации, в виде консультаций и информирования пользователей об обнаруженных ошибках и методах их исправления;

− организация мероприятий по восстановлению взаимного электронного документооборота в случае компрометации криптографических ключей и электронной подписи (ЭП).

1.5. Стороны признают, что используемые ими при электронном обмене средства защиты, обеспечивающие защиту от несанкционированного доступа через каналы связи, шифрование и электронная подпись, достаточны для обеспечения конфиденциальности информационного взаимодействия сторон, а также для подтверждения того, что:

− электронный документ исходит от стороны, его передавшей (подтверждение авторства документа);

− электронный документ не претерпел изменений при информационном взаимодействии сторон (подтверждение целостности и подлинности документа);

− электронный документ доставлен получателю в срок, указанный в формируемом и подписанным получателем извещении о доставке документа,

− электронный документ юридически эквивалентен документу на бумажном носителе.

1.6. Стороны при организации взаимодействия и координации деятельности руководствуются следующими принципами:

− строгого соблюдения Сторонами законодательства Российской Федерации, нормативных актов в области защиты информации с ограниченным доступом, не содержащей сведения, составляющие государственную тайну;

− своевременности представления информации о нарушениях в работе защищенной сети электронного документооборота;

− обязательности и безупречности исполнения достигнутых Сторонами договоренностей.

2. ТЕХНИЧЕСКИЕ УСЛОВИЯ

2.1. Стороны обеспечивают работоспособность средств защиты информации и ЭП, аналогичных средствам защиты, используемым Сторонами.

2.2. Стороны могут приобретать за свой счет средства защиты информации и ЭП, аналогичные средствам защиты, используемым Сторонами, При этом Стороны проводят организацию межсетевого взаимодействия между сетями с установленными средствами защиты информации ViPNet.

2.3. Стороны самостоятельно оплачивают средства связи и каналы связи, необходимые для работы в системе межсетевого взаимодействия.

2.4. Получение сертификатов ключей подписи для Участников электронного документооборота Сторон осуществляется самостоятельно в одном из аккредитованных удостоверяющих центров за свой счет.

3. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

3.1. Обмен информацией при защищенном электронном документообороте между Сторонами осуществляется по открытым каналам связи с использованием средств криптографической защиты информации и

ЭП, в соответствии с документацией разработчика средств защиты информациипо организации защищенного информационного взаимодействия с использованием процедур межсетевого обмена ViPNet.

3.2. Обмен электронными документами, их подпись и подтверждение целостности и подлинности документа осуществляется в соответствии с руководствами пользователей на технические средства и средства защиты, обеспечивающие такой обмен.

3.3. Отправленные и полученные электронные документы сохраняются и могут быть перенесены на любые носители.

3.4. Стороны должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных журналах регистрации электронных документов.

3.5. Хранение подписанных электронных документов.

Все подписанные электронные документы должны храниться в подписанном виде в течение сроков, предусмотренных законодательством Российской Федерации, нормативными документами сторон, а в случае возникновения споров - до их разрешения.

3.6. Обязанности по организации архивов электронных документов возлагаются на каждую из Сторон, в части их касающейся.

3.7. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1. Стороны принимают на себя следующие права и обязанности:

– осуществлять обмен информацией, представляющей интерес для обеих Сторон;

− обеспечивать организацию технической эксплуатации и использования аппаратно-программных средств защиты информации, в виде консультаций и информирования пользователей об обнаруженных ошибках и методах их исправления;

− обеспечивать организацию мероприятий по восстановлению взаимного электронного документооборота в случае компрометации криптографических ключей и ЭП;

− обеспечить функционирование всего необходимого оборудования со своих сторон, необходимого для обмена электронными документами с электронной подписью;

− немедленно информировать другую сторону и Администратора безопасности о компрометации ключей шифрования и электронной подписи;

− немедленно приостанавливать обмен электронными документами при получении от другой стороны или Администратора безопасности сообщения о компрометации ключей шифрования и электронной подписи;

− соблюдать правила работы и требования эксплуатационной документации на средства защиты информации;

− содержать в исправном состоянии рабочие станции, участвующие в электронном взаимодействии, принимать организационные меры для предотвращения несанкционированного доступа к данным рабочим

станциям, установленному на них программному обеспечению и средствам защиты информации, а также в помещения, в которых они установлены;

− не допускать появления на взаимодействующих рабочих станциях компьютерных вирусов;

− не уничтожать и (или) не модифицировать архивы открытых ключей электронной подписи, электронных документов (в том числе электронные квитанции и журналы регистрации); стороны несут ответственность за целостность и достоверность своих электронных архивов;

− допускать к работе со средствами защиты информации и электронной подписи только обученных специалистов;

− обеспечить правильность функционирования средств защиты информации электронного документооборота и электронной подписи.

4.2. Стороны обязуются при обмене электронными документами руководствоваться правилами и техническими требованиями, установленными действующим законодательством Российской Федерации и другими нормативными актами.

4.3. Сторона, для которой создалась невозможность исполнения обязательств по настоящему Соглашению, должна немедленно извещать другую сторону о наступлении и прекращении обстоятельств, препятствующих исполнению обязательств, обмен электронными документами на время действия этих обстоятельств приостанавливается.

4.4. При возникновении споров, связанных с принятием или непринятием и (или) с исполнением или неисполнением электронного документа, стороны обязаны соблюдать порядок согласования разногласий, предусмотренный настоящим Соглашением.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. Стороны несут ответственность за использование информации в соответствии с законодательством Российской Федерации.

5.2. Стороны несут ответственность за обеспечение конфиденциальности информации в соответствии с законодательством Российской Федерации.

5.3. Стороны не несут ответственности за ущерб, возникший в результате:

− неправильного заполнения пользователем системы другой Стороны электронных документов;

− разглашения пользователем другой Стороны паролей или доступности третьим лицам ключей шифрования и электронной подписи в случае получения информации об этом после принятия электронного документа к исполнению.

5.4. Стороны несут ответственность за сохранность программного обеспечения системы, архивов открытых ключей электронной подписи и электронных документов, размещенных на своих рабочих станциях.

5.5. Если одна из сторон предъявляет другой стороне претензии по электронному документу при наличии подписанного ЭП другой стороны извещения о получении такого документа, а другая сторона не может представить архивную копию спорного электронного документа вследствие нарушения требований к хранению архива, последняя сторона не вправе

ссылаться на такую архивную копию спорного документа как на основания своей позиции.

5.6. Стороны:

− обеспечивают своевременный обмен информацией;

− организуют проведение совместных мероприятий по координации работы в целях обеспечения информационной безопасности систем электронного документооборота организаций.

6. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

6.1. Настоящее Соглашение вступает в силу с момента его подписания и действует до 31 декабря 201__ года.

6.2. В случае если ни одна из сторон не известила другую о прекращении действия Соглашения за один месяц до истечения срока его действия, Соглашение считается пролонгированным на один год.

6.3. Изменения и дополнения к настоящему Соглашению оформляются в письменной форме и действительны с момента подписания Сторонами.

6.4. Настоящее Соглашение может быть расторгнуто по инициативе любой из Сторон, о чем необходимо письменно уведомить другую Сторону не позднее, чем за один месяц до дня его расторжения.

6.5. Настоящее Соглашение составлено в двух экземплярах, имеющих равную юридическую силу по одному экземпляру для каждой из сторон.

Сторона 1	**Сторона 2**
Министерство здравоохранения Республики Крым Юридический адрес: 295005, Республика Крым, г. Симферополь, проспект Кирова, д.13 ИНН 9102012869 КПП 910201001 ОКПО 00182225 ОГРН 1149102018504 Банковские реквизиты: УФК по Республике Крым (Минздрав РК л/с03752202870) БИК: 043510001 Банк: ОТДЕЛЕНИЕ РЕСПУБЛИКА КРЫМ р/сч: 40201810635100000006 л/сч.: 03752202870	
Министр здравоохранения Республики Крым	
_____/А.И.Голенко/	_____/ /
м.п.	м.п.

ПРОТОКОЛ
установления межсетевого взаимодействия

г.Симферополь	"__" _____ 201__ г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организации
N 4960	Министерство здравоохранения Республики Крым
N _____	

2. Целью установления межсетевого взаимодействия является защищенное информационное взаимодействие пользователей ViPNet-сетей указанных организаций.

3. При установлении межсетевого взаимодействия в части ЭП были произведены импорты справочников ЭП Следующих абонентов сетей

Номер сети	Должность	ФИО
N 4960	Администратор безопасности	
N _____	Администратор безопасности	

4. Смена межсетевых ключей, изменение состава АП, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствамивзаимногоэкспорта/импорта,очемадминистраторызащищенныхсетейуведомляютдругдругаспомощьюПОViPNet [Клиент][Деловая почта] с указанием производимых изменений.

5. Стороны обязуются без предварительного согласования не производить изменений в настройках и структуре защищенных сетей, могущих привести к нарушению межсетевого взаимодействия.

Работы по установлению межсетевого взаимодействия выполнили:

Орган криптографической защиты информации № 4960 ООО «Информационные системы и Аутсорсинг/_____/

Администратор безопасности сети №_____ _____/_____/

Сторона 1 **Сторона 2:**

Министр здравоохранения Республики Крым — Выберите элемент.

_____/А.И.Голенко/ _____/_____/