



**РЕСПУБЛИКА КРЫМ
МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ**

**ДЕРЖАВНИЙ БЮДЖЕТНИЙ
ЗАКЛАД ОХОРОНИ
ЗДОРОВ'Я РЕСПУБЛІКИ
КРИМ «СУДАЦЬКА МІСЬКА
ЛІКАРНЯ»**

**ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ КРЫМ
«СУДАКСКАЯ ГОРОДСКАЯ
БОЛЬНИЦА»**

**КЪЫРЫМ
ДЖУМХУРИЕТИНИНЪ
САГЪЛЫКЪ САКЪЛАВ ДЕВЛЕТ
БЮЖЕТ МУЭССИСЕСИ
«СУДАКЪ ШЕЭР
ХАСТАХАНЕСИ»**

298000, г. Судак, ул. Гвардейская, д. 1
телефон/факс : 3-48-04, e-mail: gbuzrksqb@yandex.ru
ОКПО 00805560 ОГРН 1149102174528 , ИНН/КПП 9108116840/910801001

П Р И К А З

г.Судак

« 04 _ » _____ июня __ 2020г

№249

**«Об ответственности за
персональные данные
служебной и врачебной тайны»**

На основании Приказа Министерства здравоохранения Республики Крым №1308 от 01.06.2020г.

ПРИКАЗЫВАЮ:

1. Заместителям главного врача Форащук М.А., Овсиенко О.В., Овсиенко И.В., Аблямитовой Ф.У., Климову Е.А., заведующему поликлиникой, врачу-методисту Репиной М.А., главной медицинской сестре Гнутовой Н.В., старшей медицинской сестре Лакеенко Т.В. ознакомить до 15.06.2020г. сотрудников ГБУЗ РК «Судакская городская больница» под подпись со следующими документами:
 - статья 81 Трудового кодекса Российской Федерации и пунктом 43 Постановления Пленума ВС РФ от 17.03.2004 №2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации»- в части расторжения трудового договора по инициативе работодателя по подпункту в) пункта 6 части первой статьи 81 ТК РФ (разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника).
 - положениями Федерального закона от 21. Ноября 2011 года №323 –ФЗ «Об основах охраны здоровья граждан в Российской Федерации» относительно соблюдения врачебной тайны.
 - Положением о государственной информационной системе «Единая медицинская информационная система здравоохранения Республики Крым», утвержденным постановлением Совета министров Республики Крым от 20 декабря 2016 года №612 «О Единой медицинской информационной системе здравоохранения Республики Крым»;

-Концепцией информационной безопасности государственной информационной системы «Единая медицинская информационная система здравоохранения Республики Крым», утвержденной приказом Министерства здравоохранения Республики Крым от 19 февраля 2018 года №267 (в редакции приказа Министерства здравоохранения Республики Крым от 22 апреля 2019 года №725);

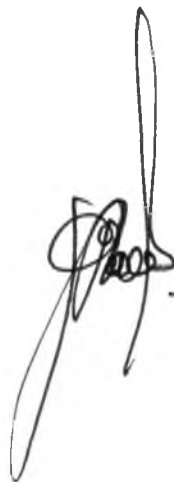
-Единым регламентом организации информационного взаимодействия медицинских организаций с государственной информационной системой «Единая медицинская информационная система здравоохранения Республики Крым», утвержденным приказом Министерства здравоохранения Республики Крым от 22 апреля 2019 года №725;

-письмом Министерства здравоохранения Республики Крым от 05 февраля 2020 года №01419-01- А1 «О работе в Единой медицинской информационной системе здравоохранения Республики Крым.

2. Начальнику отдела кадров Тихановец М.Е. внести соответствующие изменения в трудовые договора с работниками.
3. Контроль за исполнением данного приказа оставляю за собой.

Приложение: нормативные докумкеты указанные в данном приказе

Главный врач



К.В. Скорупский

ТК РФ Статья 81. Расторжение трудового договора по инициативе работодателя

Трудовой договор может быть расторгнут работодателем в случаях:

1) ликвидации организации либо прекращения деятельности индивидуальным предпринимателем;

(в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

2) сокращения численности или штата работников организации, индивидуального предпринимателя;

(в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

3) несоответствия работника занимаемой должности или выполняемой работе вследствие недостаточной квалификации, подтвержденной результатами аттестации;

(п. 3 в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

4) смены собственника имущества организации (в отношении руководителя организации, его заместителей и главного бухгалтера);

5) неоднократного неисполнения работником без уважительных причин трудовых обязанностей, если он имеет дисциплинарное взыскание;

б) однократного грубого нарушения работником трудовых обязанностей:

а) прогула, то есть отсутствия на рабочем месте без уважительных причин в течение всего рабочего дня (смены), независимо от его (ее) продолжительности, а также в случае отсутствия на рабочем месте без уважительных причин более четырех часов подряд в течение рабочего дня (смены);

(в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

б) появления работника на работе (на своем рабочем месте либо на территории организации - работодателя или объекта, где по поручению работодателя работник должен выполнять трудовую функцию) в состоянии алкогольного, наркотического или иного токсического опьянения;

(пп. "б" в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника;

(в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

г) совершения по месту работы хищения (в том числе мелкого) чужого имущества, растраты, умышленного его уничтожения или повреждения, установленных вступившим в законную силу приговором суда или постановлением судьи, органа, должностного лица, уполномоченных рассматривать дела об административных правонарушениях;

(в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

д) установленного комиссией по охране труда или уполномоченным по охране труда нарушения работником требований охраны труда, если это нарушение повлекло за собой тяжкие последствия (несчастный случай на производстве, авария, катастрофа) либо заведомо создавало реальную угрозу наступления таких последствий;

(в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

7) совершения виновных действий работником, непосредственно обслуживающим денежные или товарные ценности, если эти действия дают основание для утраты доверия к нему со стороны работодателя;

7.1) неприятия работником мер по предотвращению или урегулированию конфликта интересов, стороной которого он является, непредставления или представления неполных или недостоверных сведений о своих доходах, расходах, об имуществе и обязательствах имущественного характера либо непредставления или представления

заведомо неполных или недостоверных сведений о доходах, расходах, об имуществе и обязательствах имущественного характера своих супруга (супруги) и несовершеннолетних детей, открытия (наличия) счетов (вкладов), хранения наличных денежных средств и ценностей в иностранных банках, расположенных за пределами территории Российской Федерации, владения и (или) пользования иностранными финансовыми инструментами работником, его супругом (супругой) и несовершеннолетними детьми в случаях, предусмотренных настоящим Кодексом, другими федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации, если указанные действия дают основание для утраты доверия к работнику со стороны работодателя. Понятие "иностраные финансовые инструменты" используется в настоящем Кодексе в значении, определенном Федеральным законом от 7 мая 2013 года N 79-ФЗ "О запрете отдельным категориям лиц открывать и иметь счета (вклады), хранить наличные денежные средства и ценности в иностранных банках, расположенных за пределами территории Российской Федерации, владеть и (или) пользоваться иностранными финансовыми инструментами"; (п. 7.1 введен Федеральным законом от 03.12.2012 N 231-ФЗ, в ред. Федеральных законов от 29.12.2012 N 280-ФЗ, от 07.05.2013 N 102-ФЗ, от 28.12.2016 N 505-ФЗ)

8) совершения работником, выполняющим воспитательные функции, аморального проступка, несовместимого с продолжением данной работы;

9) принятия необоснованного решения руководителем организации (филиала, представительства), его заместителями и главным бухгалтером, повлекшего за собой нарушение сохранности имущества, неправомерное его использование или иной ущерб имуществу организации;

10) однократного грубого нарушения руководителем организации (филиала, представительства), его заместителями своих трудовых обязанностей;

11) представления работником работодателю подложных документов при заключении трудового договора;

(в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

12) утратил силу. - Федеральный закон от 30.06.2006 N 90-ФЗ;

13) предусмотренных трудовым договором с руководителем организации, членами коллегиального исполнительного органа организации;

14) в других случаях, установленных настоящим Кодексом и иными федеральными законами.

Порядок проведения аттестации (пункт 3 части первой настоящей статьи) устанавливается трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права, локальными нормативными актами, принимаемыми с учетом мнения представительного органа работников.

(часть вторая в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

Увольнение по основанию, предусмотренному пунктом 2 или 3 части первой настоящей статьи, допускается, если невозможно перевести работника с его письменного согласия на другую имеющуюся у работодателя работу (как вакантную должность или работу, соответствующую квалификации работника, так и вакантную нижестоящую должность или нижеоплачиваемую работу), которую работник может выполнять с учетом его состояния здоровья. При этом работодатель обязан предлагать работнику все отвечающие указанным требованиям вакансии, имеющиеся у него в данной местности. Предлагать вакансии в других местностях работодатель обязан, если это предусмотрено коллективным договором, соглашениями, трудовым договором.

(часть третья в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

В случае прекращения деятельности филиала, представительства или иного обособленного структурного подразделения организации, расположенного в другой местности, расторжение трудовых договоров с работниками этого подразделения производится по правилам, предусмотренным для случаев ликвидации организации.

(часть четвертая в ред. Федерального закона от 30.06.2006 N 90-ФЗ)

Увольнение работника по основанию, предусмотренному пунктом 7 или 8 части первой настоящей статьи, в случаях, когда виновные действия, дающие основания для утраты доверия, либо соответственно аморальный проступок совершены работником вне места работы или по месту работы, но не в связи с исполнением им трудовых обязанностей, не допускается позднее одного года со дня обнаружения проступка работодателем.

(часть пятая введена Федеральным законом от 30.06.2006 N 90-ФЗ)

Не допускается увольнение работника по инициативе работодателя (за исключением случая ликвидации организации либо прекращения деятельности индивидуальным предпринимателем) в период его временной нетрудоспособности и в период пребывания в отпуске.

(часть шестая введена Федеральным законом от 30.06.2006 N 90-ФЗ)

Сведения о применении к работнику дисциплинарного взыскания в виде увольнения в связи с утратой доверия на основании пункта 7.1 части первой настоящей статьи включаются работодателем в реестр лиц, уволенных в связи с утратой доверия, предусмотренный статьей 15 Федерального закона от 25 декабря 2008 года N 273-ФЗ "О противодействии коррупции".

(часть седьмая введена Федеральным законом от 01.07.2017 N 132-ФЗ)

П. 43. Постановления

Пленума Верховного Суда РФ от 17.03.2004 N 2 (ред. от 24.11.2015) "О применении судами Российской Федерации Трудового кодекса Российской Федерации"

43. В случае оспаривания работником увольнения по подпункту "в" пункта 6 части первой статьи 81 Кодекса работодатель обязан представить доказательства, свидетельствующие о том, что сведения, которые работник разгласил, в соответствии с действующим законодательством относятся к государственной, служебной, коммерческой или иной охраняемой законом тайне, либо к персональным данным другого работника, эти сведения стали известны работнику в связи с исполнением им трудовых обязанностей и он обязывался не разглашать такие сведения.

**Федеральный закон от 21.11.2011 N 323-ФЗ (ред. от 08.06.2020) "Об основах
охраны здоровья граждан в Российской Федерации"**

Статья 13. Соблюдение врачебной тайны

1. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну.

2. Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных частями 3 и 4 настоящей статьи.

3. С письменного согласия гражданина или его законного представителя допускается разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

4. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учетом положений пункта 1 части 9 статьи 20 настоящего Федерального закона;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно, а также в связи с исполнением осужденным обязанности пройти лечение от наркомании и медицинскую и (или) социальную реабилитацию;

(в ред. Федеральных законов от 23.07.2013 N 205-ФЗ, от 01.04.2020 N 93-ФЗ)

(см. текст в предыдущей редакции)

3.1) в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией либо потребляющими наркотические средства или психотропные вещества без назначения врача либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;

(п. 3.1 введен Федеральным законом от 13.07.2015 N 230-ФЗ)

4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 настоящего Федерального закона, а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 настоящего Федерального закона, для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти и федеральных государственных органов, в которых федеральным законом предусмотрена военная и приравненная к ней служба; (в ред. Федерального закона от 04.06.2014 N 145-ФЗ)

(см. текст в предыдущей редакции)

7) в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность, и в соответствии с частью 6 статьи 34.1 Федерального закона от 4 декабря 2007 года N 329-ФЗ "О физической культуре и спорте в Российской Федерации" несчастного случая с лицом, проходящим спортивную подготовку и не состоящим в трудовых отношениях с физкультурно-спортивной организацией, не осуществляющей спортивной подготовки и являющейся заказчиком услуг по спортивной подготовке, во время прохождения таким лицом спортивной подготовки в организации, осуществляющей спортивную подготовку, в том числе во время его участия в спортивных соревнованиях, предусмотренных реализуемыми программами спортивной подготовки;

(в ред. Федеральных законов от 25.11.2013 N 317-ФЗ, от 06.04.2015 N 78-ФЗ)

(см. текст в предыдущей редакции)

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с настоящим Федеральным законом;

11) утратил силу. - Федеральный закон от 25.11.2013 N 317-ФЗ.

(см. текст в предыдущей редакции)

Положение о государственной информационной системе "Единая медицинская информационная система здравоохранения Республики Крым"

Приложение
к постановлению
Совета министров
Республики Крым
от 20.12.2016 N 612

1. Общие положения

1.1. Настоящее Положение определяет цели и принципы создания, назначение, структуру, функции, порядок эксплуатации государственной информационной системы "Единая медицинская информационная система здравоохранения Республики Крым" (далее - ЕМИСЗ РК) и порядок доступа к ней.

1.2. ЕМИСЗ РК представляет собой государственную информационную систему Республики Крым, состоящую из комплекса программных и технических средств, баз данных, обеспечивающих информационно-технологическую поддержку функционирования системы здравоохранения Республики Крым, и предназначенную для выполнения в Республике Крым функций регионального фрагмента Единой государственной информационной системы в сфере здравоохранения (далее - ЕГИСЗ), установленных в Концепции создания ЕГИСЗ, утвержденной приказом Министерства здравоохранения и социального развития Российской Федерации от 28 апреля 2011 года N 364.

1.3. Для целей настоящего Положения используются следующие основные понятия:
администраторы ЕМИСЗ РК - сотрудники оператора ЕМИСЗ РК, обеспечивающие ее функционирование;
авторизованный пациент - физическое лицо, обращающееся за медицинской помощью в медицинскую организацию Республики Крым (далее - МО), прошедшее установленную процедуру идентификации и авторизации в ЕМИСЗ РК в целях подтверждения своих прав на доступ к просмотру и изменению информации в ЕМИСЗ РК в соответствии с ее регламентом; оператор ЕМИСЗ РК - организация, определенная Министерством здравоохранения Республики Крым;
(в ред. Постановления Совета министров Республики Крым от 08.05.2020 N 260)
орган управления здравоохранением - Министерство здравоохранения Республики Крым;
пользователи ЕМИСЗ РК - работники медицинской организации (далее - МО), сотрудники органа управления здравоохранением, пациенты МО, участвующие в функционировании ЕМИСЗ РК или использующие результаты ее функционирования;

электронный сервис - элемент ЕМИСЗ РК, поставляемый используемыми при создании ЕМИСЗ РК функциональными компонентами для выполнения отдельной функции или группы взаимосвязанных функций ЕМИСЗ РК;

предоставление электронного сервиса - действия ЕМИСЗ РК, обеспечивающие возможность взаимодействия с ЕМИСЗ РК посредством использования электронного сервиса способами, указанными в описании электронного сервиса;

подключение электронного сервиса - действия ЕМИСЗ РК, обеспечивающие возможность использования функциональных компонентов для обеспечения требуемого функционального поведения ЕМИСЗ РК;

функциональные компоненты, модули - взаимосвязанный набор прикладных программных операций, обеспечивающих выполнение заданных прикладных функций ЕМИСЗ РК и рассчитанных на непосредственное взаимодействие с пользователями;

регламент ЕМИСЗ РК - элемент организационного обеспечения ЕМИСЗ РК, представляющий совокупность документов, устанавливающих права и обязанности пользователей и эксплуатационного персонала ЕМИСЗ РК в условиях функционирования, проверки и обеспечения работоспособности ЕМИСЗ РК;

иные понятия и термины используются в значениях, установленных федеральным законодательством.

1.4. 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", обеспечивающей повсеместный и удобный сетевой доступ к единому централизованному пулу вычислительных ресурсов: единой защищенной телекоммуникационной среде системы здравоохранения Республики Крым, единому центру обработки данных (единой серверной платформе), единому хранилищу данных, единой точке доступа к функциям ЕМИСЗ РК, единой системе аутентификации.

1.5. В ЕМИСЗ РК реализована централизованная модель развертывания, обеспечивающая централизованное администрирование ЕМИСЗ РК и предоставление доступа к ЕМИСЗ РК пользователей по технологии "тонкого клиента" посредством веб-интерфейса без необходимости в установке в МО прикладного программного обеспечения и локального экземпляра базы данных. Подключение к работе в ЕМИСЗ РК пользователей обеспечивается их регистрацией в ЕМИСЗ РК с заданием логина, пароля, роли и прав доступа к функциональным компонентам.

1.6. ЕМИСЗ РК осуществляет информационное и процессное взаимодействие со следующими внешними системами:

федеральным фрагментом (уровнем) ЕГИСЗ;

автоматизированной информационной системой Территориального фонда обязательного медицинского страхования Республики Крым (далее - ТФОМС Республики Крым);

медицинскими информационными системами учреждений здравоохранения Республики Крым.

2. Назначение ЕМИСЗ РК

2.1. Назначениями ЕМИСЗ РК являются:

1) централизованное предоставление населению и организациям государственных услуг в сфере здравоохранения через единый портал государственных услуг;

- 2) автоматизация процесса сбора, хранения и анализа данных о случаях оказания медицинской помощи гражданам;
- 3) формирование и поддержка актуальности единого банка данных случаев оказания медицинской помощи и паспортов МО;
- 4) ведение единой электронной медицинской карты гражданина;
- 5) ведение специализированных регистров по заболеваниям и карт диспансерного наблюдения;
- 6) автоматизация учетной и отчетной медицинской деятельности МО, органа управления здравоохранением региона;
- 7) информационно-техническое сопровождение при формировании счетов за фактически оказанную медицинскую помощь, в рамках системы обязательного медицинского страхования (далее - ОМС), на основании персонифицированных реестров пациентов в медицинских организациях, находящихся в ведении Министерства здравоохранения Республики Крым;
- 8) поддержка информационного обмена в системе обеспечения лекарственными препаратами, изделиями медицинского назначения и специализированными продуктами лечебного питания при амбулаторном лечении за счет средств федерального бюджета и бюджета Республики Крым;
- 9) ведение реестра льготных категорий граждан, имеющих право на меры социальной поддержки в лекарственном обеспечении за счет средств бюджета Республики Крым;
- 10) учет движения лекарственных препаратов, изделий медицинского назначения и специализированных продуктов лечебного питания по программам обеспечения необходимыми лекарственными средствами (далее - ОНЛС), регионального лекарственного обеспечения (далее - РЛО) и семи высокостратных нозологий;
- 11) организация, мониторинг и управление потоками пациентов при оказании плановой и экстренной медицинской помощи населению;
- 12) мониторинг деятельности системы здравоохранения Республики Крым и состояния здоровья граждан Республики Крым;
- 13) автоматизированный контроль качества и доступности оказания медицинской помощи;
- 14) централизованное предоставление населению и организациям государственных услуг в сфере здравоохранения по принципу "единого окна";
- 15) обмен информацией с другими информационными системами;
- 16) мониторинг диспансеризации определенной категории граждан взрослого населения и медицинских осмотров несовершеннолетних.

3. Функции ЕМИСЗ РК

3.1. ЕМИСЗ РК обеспечивает выполнение следующих функций:

- 1) персонифицированный учет оказанной медицинской помощи;
- 2) взаимодействие при расчетах за оказанную медицинскую помощь;
- 3) управление потоками пациентов;
- 4) управление ресурсами в сфере здравоохранения;
- 5) ведение лекарственным обеспечением;
- 6) удаленный мониторинг состояния здоровья отдельных категорий пациентов;
- 7) архивное хранение медицинских изображений и предоставление доступа к ним;

- 8) электронный документооборот в сфере здравоохранения;
- 9) предоставление государственных услуг в электронной форме в сфере здравоохранения;
- 10) формирование, ведение и распространение нормативно-справочной информации в сфере здравоохранения;
- 11) анализ функционирования сферы здравоохранения;
- 12) информирование граждан, медицинских специалистов, организаторов здравоохранения и иных заинтересованных лиц по вопросам здравоохранения.

4. Состав ЕМИСЗ РК

4.1. В состав ЕМИСЗ РК входят следующие функциональные компоненты (далее - ФК):

- "Центр обработки данных";
- "Территориальный орган управления здравоохранением";
- "Электронная медицинская карта пациента";
- "Амбулаторно-поликлинические отделения МО";
- "Стационарные отделения МО";
- "Параклинические отделения МО";
- "Лабораторная информационная система";
- "Функциональная диагностика";
- "Патолого-анатомические бюро";
- "Аптечные учреждения региона";
- "Электронная регистратура";
- "Запись на прием";
- "Станция скорой медицинской помощи".

4.2. В состав ЕМИСЗ РК входят следующие модули:

- "Регистр медицинских работников";
- "Отчетность";

"Мониторинг и анализ показателей на основе OLAP-подхода"; "Регистр лекарственных средств Российской Федерации";

"Обмен сообщениями";

"Финансово-экономический модуль".

5. Основные функции ФК

5.1. ФК "Медицинский информационно-аналитический центр (Центр обработки данных)" обеспечивает выполнение следующих функций:

- 1) авторизация и аутентификация пользователя в системе;
- 2) полный доступ ко всем функциональным компонентам и модулям ЕМИСЗ РК;
- 3) ведение справочника ролей пользователей;
- 4) управление правами доступа к ресурсам ЕМИСЗ РК;
- 5) изменение настроек функциональных подсистем;
- 6) ведение картотеки пользователей ЕМИСЗ РК;
- 7) контроль за выполняемыми операциями в базе данных;
- 8) работа с журналом операций в базе данных;

- 9) настройка правил контроля корректности данных;
- 10) настройка структуры файлов информационного обмена;
- 11) централизованное ведение нормативно-справочной информации;
- 12) создание страховой копии базы данных;
- 13) идентификация страховой принадлежности пролеченных пациентов посредством взаимодействия с информационной системой ТФОМС Республики Крым;
- 14) корректировка персональных данных гражданина, работа с двойниками (поиск, объединение);
- 15) ведение регистра МО;
- 16) работа со сведениями о сертификатах ключей электронной подписи;
- 17) поддержка справочника "Регистр лекарственных средств и изделий медицинского назначения Российской Федерации";
- 18) автоматическое обновление регистра федеральных льготников по данным регионального отделения Пенсионного фонда Российской Федерации;
- 19) экспорт данных в Федеральный информационный ресурс (регистр медицинских работников, паспорт МО, паспорт субъекта Российской Федерации, мониторинг программы модернизации и т.д.) по требованию Министерства здравоохранения Российской Федерации;
- 20) настройка рабочего места пользователя.

5.2. ФК "Территориальный орган управления здравоохранением" обеспечивает выполнение следующих функций:

- 1) авторизация и аутентификация пользователя в системе;
- 2) доступ в режиме просмотра к ФК "Амбулаторно-поликлинические отделения МО", "Стационарные отделения МО", "Параклинические отделения МО", "Станция скорой медицинской помощи", "Патолого-анатомические бюро", "Аптечные учреждения региона", "Региональный аптечный склад", "Электронная регистратура";
- 3) автоматическое формирование региональной потребности в лекарственных препаратах, изделиях медицинского назначения и специализированных продуктах лечебного питания по программам ОНЛС, РЛО и семи высокзатратных нозологий;
- 4) доступ к функциям модуля "Отчетность";
- 5) доступ к функциям модуля "Мониторинг и анализ показателей на основе OLAP-подхода";
- 6) настройка рабочего места пользователя.

5.3. ФК "Электронная медицинская карта пациента" обеспечивает доступ к следующим функциям электронной медицинской карты (далее - ЭМК) пациента в режиме онлайн:

- 1) поиск электронной медицинской карты по всем ее основным реквизитам, пациенту, исследованию, медицинскому специалисту и пр.;
- 2) учет сведений о пациенте;
- 3) просмотр сигнальной информации о пациенте;
- 4) просмотр случаев лечения пациента и других событий ЭМК:
стационарное лечение;
амбулаторное лечение;
осмотры врачей;
сведения о диспансеризации и профосмотрах;

данные лабораторно-диагностических исследований - доступ к ФК "Функциональная диагностика";

5) данные временной нетрудоспособности, сведения о смерти пациента;

6) автоматическое получение данных результата параклинического исследования из ФК "Параклинические отделения МО";

7) формирование протоколов осмотров, услуг в автоматизированном режиме на основе ранее составленных протоколов;

8) просмотр списка записанных пациентов на прием на дату, на диапазон дат;

9) прием пациента без записи (поиск и выбор пациента, открытие ЭМК пациента);

10) запись пациента (на выбранные дату и время);

11) возможность резервирования времени в расписании для приема повторных и экстренных пациентов;

12) освобождение времени приема в случае отказа пациента от записи;

13) перенос времени приема до наступления даты приема;

14) возможность поиска пациентов, записанных на прием;

15) печать списка записанных по выбранному периоду;

16) автоматизация расчета финансового результата по участку, по МО;

17) телемедицинские функции:

хранение и просмотр снимков в рамках ЭМК (результатов параклинических исследований);

доступ к ФК "Функциональная диагностика"; доступ к функциям модуля "Обмен сообщениями"; доступ к функциям модуля "Отчетность";

18) автоматизация рабочего места врача стационара: автоматизированное рабочее место (далее - АРМ) врача:

приемного отделения - содержит сгруппированный по статусам список направлений в МО на плановую и экстренную госпитализации и список пациентов, обратившихся самостоятельно;

редактирование данных о поступлении пациента; ввод данных осмотра пациента в приемном отделении; назначение диагностических исследований; просмотр результатов исследований;

направление пациента в стационарное отделение для госпитализации;

отмена госпитализации;

19) АРМ врача профильного отделения включает:

список пациентов, сгруппированный по статусам ("Не поступал", "Вновь поступивший", "В отделении", "К выписке", "Выписан");

список пациентов, находящихся в отделении, сгруппированный по палатам;

возможность назначения врачом профильного отделения палаты выбранному пациенту, перевода в другую палату, смены лечащего врача, перевода в другое отделение,

оформления осмотра, лечебных и диагностических назначений, выписки пациента;

просмотр ЭИБ (электронная история болезни); возможность резервирования коек в расписании для экстренных пациентов;

планирование операций;

телемедицинские функции (хранение и просмотр снимков в рамках ЭМК (результатов параклинических исследований), доступ к ФК "Функциональная диагностика", доступ к функциям модуля "Обмен сообщениями", ведение электронной истории болезни);

обеспечение доступа к актуальным данным системы в режиме реального времени;

20) автоматизация рабочего места врача параклиники:

автоматическое получение данных о назначенном параклиническом исследовании из ФК "Амбулаторно-поликлинические отделения МО" и "Стационарные отделения МО";

автоматическое получение данных результата исследования с анализатора в ФК "Параклинические отделения МО", доступ к ФК "Лабораторная информационная система";

автоматическая передача данных результата исследования в ФК "Амбулаторно-поликлинические отделения МО" и "Стационарные отделения МО";

телемедицинские функции (хранение и просмотр снимков в рамках ЭМК (результатов параклинических исследований), доступ к ФК "Функциональная диагностика", функциям модуля "Обмен сообщениями");

все функции АРМ врача должны обеспечивать доступ к актуальным данным системы в режиме реального времени.

5.4. ФК "Амбулаторно-поликлинические отделения МО" обеспечивает выполнение следующих функций:

- 1) авторизация и аутентификация пользователя в системе;
- 2) поиск в регистре пролеченных по данным ЭМК пациента;
- 3) корректировка персональных данных гражданина по допустимым для редактирования атрибутам;
- 4) ведение регистра прикрепленного населения;
- 5) прикрепление человека с указанием МО, участка, периода прикрепления, а также в разрезе терапевтического, педиатрического, гинекологического и стоматологического типов прикрепления;
- 6) печать заявления о прикреплении;
- 7) поиск в регистре прикрепленного населения;
- 8) ведение учета случаев амбулаторно-поликлинического лечения пациента в МО:
ввод данных случая амбулаторно-поликлинического лечения;
поиск случая амбулаторно-поликлинического лечения по всем атрибутам случая;
учет посещений пациентами МО;
учет медицинских услуг, оказанных пациенту;
учет данных о диагнозах, поставленных пациенту;
выписка листов и справок о временной нетрудоспособности;
учет данных о результатах лечения;
печать талона амбулаторного пациента;
ведение диспансерного учета;
- 9) ведение учета данных о диспансеризации определенной категории граждан взрослого населения и профилактических осмотрах несовершеннолетних;
- 10) ведение учета данных о медицинских осмотрах несовершеннолетних;
- 11) ведение учета данных об углубленном диспансерном обследовании участников Великой Отечественной войны;
- 12) планирование вакцинации пациентов на основе календарей вакцинации, контроль ее проведения, учет результатов;

- 13) получение списков граждан для углубленного медицинского обследования и передача данных о результатах обследования;
- 14) организация, мониторинг и управление потоками пациентов при оказании плановой медицинской помощи населению (доступ к модулю "Электронная регистратура");
- 15) доступ к функциям модуля "Регистр лекарственных средств РФ";
- 16) автоматизация учета льготного лекарственного обеспечения:
 - поиск в регистре федеральных льготополучателей по категории льготы, по периоду ее действия;
 - ведение регистра региональных льготополучателей с указанием категории льготы, периода ее действия;
 - автоматическое получение данных об остатках медикаментов из ФК "Аптечные учреждения региона" и "Региональный аптечный склад";
 - выписка рецептов на льготное лекарственное обеспечение;
 - формирование данных рецепта на основании сведений ЭМК, печать рецепта на бланке;
 - поиск выписанных рецептов по всем реквизитам рецепта и сведениям о пациенте;
 - поиск отоваренных рецептов и рецептов, находящихся на отсроченном обслуживании;
 - ведение регистра социально значимых заболеваний;
 - доступ к функциям модуля "Мониторинг и анализ показателей на основе OLAP-подхода";
- 17) ведение журнала учета клинико-экспертной работы МО, ввод данных протокола учета клинико-экспертной работы;
- 18) доступ к функциям модуля "Паспорт и структура МО";
- 19) доступ к функциям модуля "Регистр медицинских работников";
- 20) доступ к модулю "Финансово-экономический модуль".

5.5. ФК "Стационарные отделения МО" обеспечивает выполнение следующих функций:

- 1) авторизация и аутентификация пользователя в системе;
- 2) поиск в регистре пролеченных по данным ЭМК пациента;
- 3) ведение учета случаев стационарного лечения пациента в МО:
 - ввод, редактирование и поиск случаев лечения пациента в МО;
 - учет данных из приемного отделения; учет данных о диагнозах, поставленных пациенту;
 - учет медицинских услуг, оказанных пациенту;
 - учет данных о направлении на стационарное лечение;
 - ведение учета выписанных листов и справок о временной нетрудоспособности;
 - учет данных об исходе госпитализации и выписке;
 - автоматическая передача информации о факте госпитализации пациента в амбулаторно-поликлиническую сеть участковому врачу средствами ФК "Амбулаторно-поликлинические отделения МО";
 - учет загруженности стационарных отделений; печать карты выбывшего из стационара;
- 4) ведение учета выданных медицинских свидетельств о перинатальной смерти;
- 5) ведение учета извещений о дорожно-транспортном происшествии (о раненых, о скончавшихся);
- 6) персонифицированный учет движения медикаментов в аптеке МО;
- 7) доступ к функциям модуля "Регистр лекарственных средств РФ";
- 8) доступ к функциям модуля "Отчетность";

- 9) доступ к функциям модуля "Мониторинг и анализ показателей на основе OLAP-подхода";
- 10) ведение журнала учета клинико-экспертной работы МО, ввод данных протокола учета клинико-экспертной работы;
- 11) доступ к функциям модуля "Паспорт и структура МО";
- 12) доступ к функциям модуля "Регистр медицинских работников";
- 13) доступ к модулю "Финансово-экономический модуль";
- 14) настройка рабочего места пользователя.

5.6. ФК "Параклинические отделения МО" обеспечивает выполнение следующих функций:

- 1) авторизация и аутентификация пользователя в системе;
- 2) поиск в регистре пролеченных по данным ЭМК пациента;
- 3) корректировка персональных данных гражданина по допустимым для редактирования атрибутам;
- 4) ведение персонифицированного учета параклинических услуг: ввод (поточный ввод), редактирование и поиск выполненных параклинических услуг;
- 5) ввод данных об оказанной параклинической услуге: направление, место выполнения, наименование услуги, медицинский персонал, вид оплаты, количество;
- 6) доступ к модулям "Паспорт и структура МО", "Финансово-экономический модуль";
- 7) доступ к функциям модулей "Регистр медицинских работников", "Отчетность", "Мониторинг и анализ показателей на основе OLAP-подхода", "Регистр лекарственных средств РФ";
- 8) настройка рабочего места пользователя.

5.7. ФК "Лабораторная информационная система" обеспечивает информационную поддержку проведения исследований, исключение дублирующих исследований, автоматический учет оказанных услуг, оперативное предоставление результатов исследований.

Драйверы для работы с лабораторными приборами представляют из себя системные сервисы операционной системы и устанавливаются на конечные рабочие места, к которым осуществлено подключение лабораторных приборов. Сервер ЛИС должен самостоятельно взаимодействовать с драйверами лабораторных приборов посредством обмена запросами и ответами в формате XML через протокол http.

ФК "Лабораторная информационная система" обеспечивает выполнение следующих функций:

- 1) учет лабораторных нарядов:

формирование и учет лабораторных нарядов на основании сведений о назначениях, направлениях;

поиск нарядов по заданным критериям;

распределение лабораторных нарядов между лабораторными подразделениями, врачами, лаборантами, включая внешние лаборатории и лабораторные системы;

контроль корректности данных;
ведение журнала браков;
формирование и учет бланков для заполнения результатов лабораторных исследований на основании лабораторных нарядов;
учет исполнения лабораторных нарядов (выполнение исследований, ввод результатов, обеспечение возможности удостоверения результатов электронной подписью врача лаборатории);
направление сведений лабораторного наряда и результатов исследований в учреждение здравоохранения (филиал), выдавшее назначение, направление на исследование;

2) учет результатов исследований:

ввод или автоматическое получение от лабораторного анализатора результатов исследований в соответствии с лабораторными нарядами, обеспечение возможности удостоверения результатов электронной подписью врача лаборатории; доступ к ФК "Функциональная диагностика";
настройка контрольных значений (норм) результатов клинико-диагностических исследований;
настройка логики определения результатов исследований; хранение истории результатов исследований; автоматизированный контроль соответствия фактических значений результатов клинико-диагностических исследований контрольным;
автоматизированная оценка динамики результатов при повторном выполнении исследования;

3) отчеты ФК "Лабораторная информационная система": журнал регистрации анализов и их результатов;

журнал взятия проб;

журнал учета услуг, выполненных по системе ОМС; листок ежедневного учета работы врача-лаборанта; журнал хранения и утилизации биоматериала; журнал регистрации микробиологических и паразитологических исследований;
рабочий журнал;

4) доступ к функциям модуля "Обмен сообщениями".

5.8. ФК "Функциональная диагностика" реализует функции автоматизации процессов проведения диагностических исследований с использованием диагностического оборудования и сохранения полученных результатов в специальных удаленных архивах на DICOM-серверах с возможностью быстрого поиска и просмотра интересующей информации (DICOM - отраслевой стандарт создания, хранения, передачи и визуализации медицинских изображений и документов обследованных пациентов).

5.8.1. Диагностическое оборудование может быть подключено к сервису следующими способами:

- 1) средствами виртуальной печати для программного обеспечения под управлением Windows-совместимых операционных систем;
- 2) с применением активной опции DICOM медицинского аппарата;
- 3) через программный конвертер для передачи информации в цифровом виде;
- 4) через модуль видеозахвата.

5.8.2. Возможности программного обеспечения DICOM-Архив:

- 1) получение цифровых медицинских изображений по сетевому интерфейсу в стандарте DICOM;
- 2) полная совместимость с любой диагностической аппаратурой, поддерживающей стандарт DICOM 3.0;
- 3) полная поддержка DICOM-сервисов: DICOM Store (SCP), DICOM Query/Retrieve (SCP, SCU), DICOM Storage Commitment (SCU), WorkList;
- 4) полная поддержка основных DICOM-команд: Echo, Find, Get, Set, Store, Move;
- 5) поддержка изображений следующих модальностей: US, CT, MR, CR, MG, XA, DX, DR, OT;
- 6) поддержка следующих типов медицинских изображений: холтеровское мониторирование (инкапсулированный PDF), рентген, сцинтиграфия (в том числе вторичный захват), электрокардиография, функциональная диагностика (инкапсулированный PDF);
- 7) многопоточный прием данных;
- 8) одновременная передача и прием данных;
- 9) поддержка работы с изображениями в формате JPEG 2000;
- 10) архивирование в виде одно- и многотомных архивов на локальных, сетевых или съемных дисках;
- 11) создание резервных копий базы данных DICOM-Архива;
- 12) тома оперативного хранения;
- 13) тома долговременного хранения;
- 14) автоматическое перемещение исследований из оперативных в долговременные тома по настраиваемому временному критерию;
- 15) отслеживание основных событий и ведение журнала событий;
- 16) оповещение системного администратора о событиях в работе DICOM-Архива;
- 17) возможность добавления DICOM-файлов в DICOM-Архив из локальной или сетевой папок;
- 18) возможность запроса исследований из удаленного DICOM-устройства;
- 19) возможность добавления исследований из структурированной папки (DICOM DIR);
- 20) возможность добавления исследований с компакт-диска, записанного в формате DICOM;
- 21) возможность передачи исследований на удаленное устройство;
- 22) возможность сохранения одного или нескольких исследований на диске;
- 23) серверный интерфейс для передачи данных в стандарте HL7;
- 24) возможность передачи в сообщении HL7 любых данных об исследовании, хранящихся в DICOM-файлах;
- 25) поиск исследований в архиве через веб-интерфейс в локальной и удаленной базах;
- 26) возможность управления DICOM-пересылкой изображений и исследований через веб-интерфейс;
- 27) возможность подключения к DICOM-Архиву неограниченного количества облегченных просмотрных рабочих станций;
- 28) непрерывная работа диагностических аппаратов в МО при отсутствии связи (при наличии в МО локального PACS-сервера).

5.8.3. Возможности внешней просмотровой мультимодальной рабочей станции:

- 1) передача подтверждений об успешной архивации исследования (Storage commitment);
- 2) просмотр списка запланированных исследований;
- 3) возможность сохранения одного или нескольких исследований на любые электронные носители;
- 4) возможность просмотра полученных результатов (изображений);
- 5) предоставление доступа к результатам исследований в соответствии с назначенными пользователю правами;
- 6) передача данных о запланированных исследованиях непосредственно на консоли диагностических аппаратов;
- 7) поиск и просмотр данных пациентов и их исследований;
- 8) получение цифровых медицинских изображений по сетевому интерфейсу;
- 9) поддержка изображений следующих модальностей: US, CT, MR, CR, MG, XA, DX, DR, OT;
- 10) работа с электронными архивами (удаленная база, Storage (архив));
- 11) изменение параметра "окно/уровень" ("яркость/контрастность"); установка "предопределенных значений" уровней контрастности и яркости, наиболее подходящих для текущего изображения; установка стандартных для КТ "оптических окон";
- 12) воспроизведение кинопетли в замкнутом цикле;
- 13) просмотр DICOM-файлов, содержащих кинопетли, с различной скоростью;
- 14) просмотр DICOM-файлов, содержащих видео в формате MPEG-2;
- 15) просмотр DICOM-файлов, содержащих инкапсулированный PDF-объект;
- 16) отражение по горизонтали;
- 17) отражение по вертикали;
- 18) поворот на 90 градусов по часовой стрелке;
- 19) поворот на 90 градусов против часовой стрелки;
- 20) инструмент "отрезок", измеряющий расстояние между двумя точками на изображении в абсолютных единицах (см, мм);
- 21) инструмент "угол", позволяющий измерять угол между двумя отрезками на изображении;
- 22) инверсия изображения, изменение/применение палитры;
- 23) измерение площади и плотности по шкале Хаунсфилда (HU);
- 24) доступ к функциям модуля "Обмен сообщениями".

5.9. ФК "Патолого-анатомические бюро" обеспечивает выполнение следующих функций:

- 1) авторизация и аутентификация пользователя в системе;
- 2) доступ к функциям модуля "Паспорт и структура МО";
- 3) доступ к функциям модуля "Регистр медицинских работников";
- 4) автоматическое получение данных о направлениях на патоморфогистологические и патологогистологические исследования из ФК "Амбулаторно-поликлинические отделения МО" и "Стационарные отделения МО";

- 5) ввод данных в протокол патоморфогистологического и патологистологического исследований с последующей автоматической передачей протокола в ФК "Амбулаторно-поликлинические отделения МО" и "Стационарные отделения МО";
- 6) ввод параметров патологистологического исследования: связь с направлением на исследование, серия и номер исследования, дата поступления материала, биопсия диагностическая, операционный материал, патологистологическое заключение, диагноз, дата исследования, патологоанатом, лаборант, количество кусочков, количество блоков, макроскопическое описание;
- 7) ввод параметров патоморфогистологического исследования: связь с направлением на исследование, серия и номер исследования, дата исследования, связь со стационарным случаем лечения, дата и время смерти, дата вскрытия, врач, диагноз направившего учреждения, диагноз при поступлении, дата установления клинических диагнозов, клинический диагноз, результаты клинико-лабораторных исследований, патолого-анатомический диагноз, расхождения диагнозов по основному заболеванию (тип ошибки клинической диагностики, причина расхождения диагноза), коды диагнозов, клинико-патолого-анатомический эпикриз, патологоанатом, заведующий отделением, вес органов тела (мозг, сердце, легкие, печень, селезенка, почка левая, почка правая), взято кусочков, изготовлено блоков, материал для других методов исследования, текст протокола;
- 8) доступ к функциям модуля "Обмен сообщениями";
- 9) доступ к функциям модуля "Отчетность";
- 10) доступ к функциям модуля "Мониторинг и анализ показателей на основе OLAP-подхода";
- 11) настройка рабочего места пользователя.

5.10. ФК "Аптечные учреждения региона" обеспечивает выполнение следующих функций:

- 1) авторизация и аутентификация пользователя в системе;
- 2) ведение справочников: "Медикаменты", "Контрагенты", "Материально ответственные лица";
- 3) ведение документов учета движения медикаментов: ввод остатков медикаментов, актов списания медикаментов, прихода/расхода, инвентаризационных ведомостей;
- 4) ведение учета отоваренных медикаментов в аптечном учреждении (поиск рецепта, отоваривание рецепта);
- 5) формирование дефектуры на основании журнала отсроченного обслуживания рецептов и данных контроля по нормам неснижаемых остатков;
- 6) формирование заявок на поставку медикаментов в ручном и автоматическом режимах на основании дефектуры;
- 7) формирование заявок на поставку медикаментов в разрезе источников финансирования и программ лекарственного обеспечения;
- 8) бронирование заявленного количества медикаментов в момент передачи заявки;
- 9) "посерийный" учет медикаментов;
- 10) автоматическое получение данных о выписанных рецептах из ФК "Амбулаторно-поликлинические отделения МО";
- 11) автоматическое резервирование количества выписанного медикамента за пациентом;
- 12) отпуск по одному рецепту остатков препаратов из разных поступлений (серий);

- 13) поиск рецепта по серии и номеру при отпуске медикамента; возможность выбора серии медикаментов, по которой следует формировать строку документа учета;
- 14) автоматическая передача данных об отоваренных медикаментах и рецептах, находящихся на отсроченном обеспечении в ФК "Амбулаторно-поликлинические отделения МО" и "Стационарные отделения МО";
- 15) автоматическая передача данных о текущих остатках медикаментов в ФК "Амбулаторно-поликлинические отделения МО" и "Стационарные отделения МО";
- 16) доступ к функциям модулей "Обмен сообщениями", "Отчетность", "Мониторинг и анализ показателей на основе OLAP-подхода";
- 17) настройка рабочего места пользователя.

5.11. ФК "Электронная регистратура" обеспечивает осуществление записи на прием через центр записи путем непосредственного обслуживания входящих вызовов, поступивших посредством телефонных сетей общего пользования, и включает следующие функции:

- 1) запись на прием пациентов в соответствии с картотекой прикрепленного населения;
- 2) ведение расписания работы специалистов, записи на прием, формирование списков записанного на прием населения, получение отчетности;
-) обеспечение функциональных возможностей ЕМИСЗ РК для записи на прием пациентов через собственную(-ые) регистратуру(-ы) МО:
 - формирование расписания работы врачей на 2 недели;
 - автоматическое формирование расписания согласно нормам приема на одного пациента;
 - возможность резервирования времени в расписании для приема повторных и экстренных пациентов;
 - резервирование времени приема для определенных категорий пациентов;
 - автоматизированная отмена резервирования времени приема в день приема;
 - освобождение времени приема в случае отказа пациента от записи;
 - перенос времени приема до наступления даты приема;
 - отображение расписания на экраны для информирования пациентов;
 - возможность поиска пациентов, записанных на прием;
 - возможность ввода дополнительных бирок в расписание работы;
 - формирование отчетов по количеству записанных пациентов в разрезе профилей МО;
 - ведение информации в части записи на прием;
- 4) формирование направления для пациента;
- 5) обеспечение обработки медико-статистических данных;
- 6) автоматическая передача данных о записи на прием, направлении, очереди в МО (куда записан), расписании в ФК "Амбулаторно-поликлинические отделения МО", "Стационарные отделения МО", "Параклинические отделения МО";
- 7) СМС-информирование, информирование по электронной почте пациента о дате и времени записи на прием;
- 8) доступ к функциям модуля "Обмен сообщениями".

5.12. ФК "Запись на прием" обеспечивает функциональные возможности для пациентов по записи на прием в МО через портал регионального здравоохранения в сети Интернет, позволяющий пользователям выполнять следующие действия:

- 1) регистрация учетной записи пользователя портала;
- 2) обеспечение защиты от автоматической регистрации;
- 3) обеспечение активации учетной записи через электронную почту;
- 4) восстановление пароля через электронную почту;
- 5) вход в систему путем ввода логина и пароля;
- 6) просмотр и редактирование параметров пользователя веб-портала (смена пароля, фамилии, имени, отчества, даты рождения);
- 7) ведение пользователем собственной картотеки пациентов;
- 8) редактирование данных ранее добавленного пациента (смена адреса, телефона);
- 9) удаление данных ранее добавленного пациента;
- 10) определение места прикрепления пациента для медицинского обслуживания;
- 11) определение профиля врачебной помощи;
- 12) осуществление записи на прием к врачу;
- 13) отмена записей на прием;
- 14) формирование отчетных форм по записанным на прием через Интернет и по выписанным направлениям в различных разрезах;
- 15) автоматическая передача данных о записи на прием, направлении, очереди в МО (куда записан), расписании в ФК "Амбулаторно-поликлинические отделения МО", "Стационарные отделения МО", "Параклинические отделения МО";
- 16) размещение на веб-портале информации о МО региона;
- 17) возможность регистрации на веб-портале жалоб и обращений пациентов, поддержка форума.

5.13. ФК "Станция скорой медицинской помощи" обеспечивает выполнение следующих функций:

- 1) авторизация и аутентификация пользователя в системе;
- 2) доступ к функциям модуля "Паспорт и структура МО";
- 3) доступ к функциям модуля "Регистр медицинских работников";
- 4) поиск в регистре пролеченных по данным ЭМК пациента;
- 5) корректировка персональных данных гражданина по допустимым для редактирования атрибутам;
- 6) прием и регистрация вызова скорой и неотложной помощи, плановой и экстренной перевозки по нештатной ситуации с контролем на дубль и повторность вызова, на часто вызывающих больных и вызовы на особо опасные объекты;
- 7) формирование карты вызова: данные о приеме вызова, время, место, тип, повод, данные о пациенте;
- 8) распределение вызовов по бригадам станции скорой медицинской помощи (далее - ССМП) (данные об управлении вызовом, о контроле вызова, о бригаде);
- 9) автоматическая расстановка принятых вызовов в порядке приоритетности их обслуживания;
- 10) оперативная обработка всех принятых вызовов в режиме реального времени;
- 11) слежение за местоположением и состоянием подвижного состава, контроль времени;
- 12) заполнение карт вызова с возможностью формирования статистической отчетности в соответствии с законодательством;

- 13) заполнение талона к сопроводительному листу для дальнейшего формирования раздела статистической отчетности по сличительной диагностике;
- 14) автоматизированное закрытие смены с возможностью получения статистической сводки за прошедшие сутки - суточного рапорта;
- 15) формирование графика нарядов;
- 16) отметка выхода на работу подвижного состава и невыездного персонала ССМП;
- 17) учет поступления и расхода медикаментов;
- 18) ведение путевых листов водителей медицинского автотранспорта и учет прихода и расхода горюче-смазочных материалов;
- 19) ведение табеля работников станции с дальнейшим формированием печатного документа для бухгалтерии;
- 20) формирование базы хронических больных, часто вызывающих скорую медицинскую помощь (далее - СМП);
- 21) возможность передачи врачам бригады медицинских данных о пациенте;
- 22) закрытие карты вызова (диагноз, результат вызова);
- 23) автоматическое получение из ФК "Стационарные отделения МО" сведений о результатах лечения пациентов, доставленных СМП;
- 24) автоматическая передача в амбулаторно-поликлиническую сеть информации о факте вызова СМП и/или о необходимости активного вызова врача на дом;
- 25) ведение журнала учета клинико-экспертной работы МО, ввод данных протокола учета клинико-экспертной работы;
- 26) доступ к функциям модулей "Отчетность", "Мониторинг и анализ показателей на основе OLAP-подхода", "Регистр лекарственных средств Российской Федерации", "Обмен сообщениями", "Финансово-экономический модуль";
- 27) настройка рабочего места пользователя.

5.14. ФК "Пищеблок" обеспечивает выполнение следующих функций:

- 1) ведение списка рецептуры (блюд) и технологий: хранение произвольного списка блюд; учет технологий приготовления блюд согласно сборникам рецептов (приготовление, разделка, разукomплектация); хранение произвольного количества составов блюд или технико-технологических карт с учетом нормативов расхода продуктов и их аналогов, химического состава (количество жиров, белков и углеводов), калорийности, минерального состава; хранение описаний блюд и способа их приготовления с учетом сезонности; возможность автоматического создания новых блюд путем пересчета ингредиентного состава относительно выходного веса; автоматический расчет энергетической ценности, а также белкового, углеводного и жирового состава блюда; подбор индивидуального состава блюд; формирование и печать технологических карт;
- 2) учет продуктов и калькуляция: отражение всех необходимых операций по движению сырья (продуктов); калькуляция; производство готовой продукции и реализация; отчетность;
- 3) диетпитание.

5.15. Модуль "Регистр медицинских работников" обеспечивает ведение регистра медицинских работников и сотрудников МО немедицинских специальностей и включает следующие функции:

- 1) ведение персональных данных сотрудника (основные сведения, документы, адрес, награды, дополнительные сведения, код врача в системе лекарственного обеспечения);
- 2) автоматическая генерация кода врача в системе лекарственного обеспечения и контроль уникальности кода в случае ручного редактирования;
- 3) ведение данных об образовании (специальность по диплому, послевузовское образование, квалификационная категория, переподготовка, повышение квалификации, специальность по сертификату специалиста);
- 4) ведение личного дела сотрудника (срока штатного расписания, табельный номер, ставка, тип занятия должности, режим работы, квалификационный уровень, непрерывный медицинский стаж на момент начала работы, специальный медицинский стаж на момент начала работы, отношение к военной службе, тип подразделения, признак работы в системе ОМС, данные о приеме на работу с указанием даты приема и номера приказа, о дополнительном соглашении с указанием даты заключения и номера, об увольнении с указанием номера приказа и даты, о переводах на другие ставки, о невыплатах с указанием причины и периода, о периоде работы в системе лекарственного обеспечения);
- 5) контроль уникальности основного места работы;
- 6) контроль неперевышения фактического количества ставок над плановым в строке штатного расписания;
- 7) поиск медработника по персональным данным (фамилия, имя, отчество, идентификационный номер налогоплательщика (ИНН), страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования (СНИЛС)), а также по следующим признакам: фактически работающий, работающий в системе лекарственного обеспечения, первичное звено, первичное звено на одну ставку и более;
- 8) просмотр списка мест работы выбранного сотрудника;
- 9) выбор врача из регистра медицинских работников при заполнении медицинских учетных документов;
- 10) выгрузка данных в федеральный портал регистра медицинских работников, выгрузка справочника врачей в информационную систему ТФОМС Республики Крым;
- 11) ведение тарификационных списков (данные об окладах, категории персонала, дополнительном и накопленном непрерывном стаже, выплатах, профессиональных группах, источниках финансирования, видах работ, коэффициентах за руководство, почетных званиях);
- 12) автоматизация расчета основной заработной платы;
- 13) доступ к функциям модуля "Отчетность".

5.16. Модуль "Отчетность" формирует финансовые, отчетные и аналитические данные о медико-статистической и медико-экономической учетной деятельности МО, территории, региона и включает следующие функции:

- 1) формирование государственных и статистических отчетов: информация о здоровье населения, объеме и качестве получаемой медицинской помощи, ресурсах МО и эффективности их использования;

- 2) конструктор отчетов: создание произвольных отчетов фиксированной формы для различных периодов, территорий, МО;
- 3) возможность ручного и автоматического заполнения ячеек отчетов с использованием источников данных: прямого доступа к базе данных либо на основе веб-сервиса; использование ранее созданных в модуле отчетности документов;
- 4) возможность установки контроля типов данных в ячейках отчетов;
- 5) возможность настройки внутри- и межтабличных контролей;
- 6) возможность передачи сформированного отчета на контроль или пересформирование путем смены статуса отчета;
- 7) возможность печати отчета;
- 8) возможность выгрузки отчета в форматах xls, html, pdf;
- 9) автоматическое сохранение данных отчета в случае потери связи с сервером и с последующим восстановлением данных;
- 10) настройка прав доступа к отчетам, видимости данных и статусов пользователей (принимающий отчет, сдающий отчет);
- 11) просмотр справочной информации по территориям/МО с использованием картографического, табличного и шаблонного подхода;
- 12) поддержка функций поиска, фильтрации, ввода и редактирование справочной информации;
- 13) редактирование записей внутренних справочников отчетной формы;
- 14) редактирование нескольких отчетных форм одновременно;
- 15) ввод показателей в формах как вручную с клавиатуры, так и выбором из специализированных справочников.

5.17. Модуль "Мониторинг и анализ показателей на основе OLAP-подхода"

обеспечивает получение произвольных аналитических отчетов и включает следующие функции:

- 1) процедура импорта первичных учетных данных в систему мониторинга и анализа показателей;
- 2) произвольные запросы к базе данных, позволяющие извлечь информацию по любым критериям (анализ результатов деятельности территорий/МО на основе данных, содержащихся в ЕМИСЗ РК);
- 3) возможность визуального конструирования отчетных форм и их сохранения;
- 4) создание динамических аналитических отчетов с использованием OLAP-технологии;
- 5) построение отчетов на произвольных наборах параметров в разрезе территорий/МО, времени и направлений деятельности;
- 6) возможность наложения фильтров на измерения и показатели анализируемых данных;
- 7) минимальный перечень показателей для анализа должен содержать все показатели государственных отчетных форм, перечисленных в требованиях к модулю "Отчетность".

5.18. Модуль "Регистр лекарственных средств Российской Федерации" обеспечивает быстрый доступ к полной информации о лекарственных средствах и включает следующие функции:

- 1) поиск медикамента по заданным параметрам;
- 2) просмотр списка найденных медикаментов по заданным параметрам;
- 3) просмотр данных по выбранному медикаменту;

- 4) возможность быстрого перехода из режима просмотра данных по выбранному медикаменту в режим просмотра данных торгового наименования выбранного медикамента;
- 5) возможность добавления медикаментов в справочник, а также изделий медицинского назначения;
- 6) поиск в справочнике торговых наименований, просмотр списка найденных торговых наименований;
- 7) просмотр данных по выбранному торговому наименованию;
- 8) поиск в справочнике действующих веществ;
- 9) просмотр списка найденных действующих веществ;
- 10) поиск в справочнике производителя;
- 11) просмотр списка найденных производителей;
- 12) просмотр по выбранному производителю перечня выпускаемых им торговых наименований;
- 13) выбор значения в классификаторе фармакологических групп и просмотр по выбранной группе перечня торговых наименований и их действующих веществ;
- 14) выбор значения в классификаторе нозологий МКБ-10 и просмотр по выбранной нозологии перечня соответствующих торговых наименований, сгруппированных по фармакологическим группам и действующим веществам;
- 15) выбор значения в классификаторе АТХ и просмотр по выбранному значению перечня соответствующих торговых наименований, сгруппированных по действующим веществам;
- 16) наличие доступа к модулю "Регистр лекарственных средств Российской Федерации" из всех функциональных компонентов, в которых осуществляется выбор медикамента по действующему веществу, по торговому наименованию.

5.19. Модуль "Обмен сообщениями" обеспечивает обмен сообщениями между пользователями ЕМИСЗ РК, автоматическое уведомление пользователей о различных событиях в ЕМИСЗ РК и включает следующие функции:

- 1) возможность отправки экспресс-сообщений пользователям ЕМИСЗ РК;
- 2) просмотр списка входящих/отправленных сообщений/уведомлений со следующими данными: прочитано, заголовок, дата, время, автор;
- 3) возможность множественного выбора сообщений/уведомлений;
- 4) удаление сообщений/уведомлений;
- 5) работа с адресной книгой (добавление/удаление групп пользователей; добавление/удаление пользователя в группу);
- 6) просмотр в адресной книге информации о пользователе: логин, фамилия, имя, отчество, e-mail, о себе, МО, место работы;
- 7) автоматическая система уведомлений (информация о пациентах: госпитализация, вызов скорой медицинской помощи, передача пациента в актив, новые результаты исследований, поступление пациента в приемное отделение и др.).

5.20. Модуль "Финансово-экономический модуль" выполняет следующие функции:

- 1) ведение реестра страховых медицинских организаций и иных контрагентов;
- 2) ведение реестра договоров с контрагентами;
- 3) информационный обмен с контрагентами;
- 4) учет взаиморасчетов с контрагентами, включая:
учет счетов, выставленных контрагенту;
учет наличных и безналичных поступлений;

возможность квотирования с поступлениями по расчетному счету(-ам) и в кассу;
формирование актов сверки;
формирование и выставление счетов по заданным параметрам;
формирование реестров счетов;
формирование акта проведенной экспертизы с указанием конкретных услуг из счета, по которым был составлен акт экспертизы, обнаруженных в ходе экспертизы несоответствий (возможной причины отказа в оплате счета), должностного лица, допустившего обнаруженные несоответствия (должность, Ф.И.О.);
формирование выходных документов, сопутствующих выставлению счета на бумажном носителе и в электронном виде;
автоматизированный контроль кредиторской или дебиторской задолженности по взаиморасчетам с контрагентами, корректировка задолженности в соответствии с актами экспертизы;
автоматический контроль корректности формируемого счета, в том числе исключение возможности повторного внесения услуги в счет, повторного назначения первичных консультаций в рамках одного случая, предоставления услуг, несовместимых между собой, услуг, не допустимых для данного пациента (например, по признаку пола);
автоматизированный учет отказов в оплате счетов;

- 5) реестр страховых медицинских организаций и иных контрагентов;
- 6) учет начислений и поступлений, включая автоматизированный расчет стоимости услуг: в рамках ОМС согласно тарифному соглашению и добровольного медицинского страхования;
- 7) учет гарантийных писем, включая ведение реестра гарантийных писем;
- 8) реестр договоров с контрагентами;
- 9) формирование реестров и счетов на оплату за оказанные услуги в МО пациентам, застрахованным по программе ОМС.

5.21. Модуль "Льготное лекарственное обеспечение" обеспечивает следующее:

- 1) учет пациентов, имеющих право на льготное лекарственное обеспечение, включая ДЛО и льготы по 7 высокочувствительным нозологиям;
- 2) учет выписанных льготных рецептов и передача соответствующих сведений;
- 3) печать льготных рецептов установленного образца;
- 4) проверку наличия пациента в региональном реестре лиц, имеющих право на дополнительное лекарственное обеспечение, на основании данных централизованной системы выдачи и обслуживания рецептов;
- 5) получение сведений об отпущенных лекарственных средствах из аптечных учреждений на основании выписанных льготных рецептов, а также получение информации об остатках лекарственных средств в аптечных учреждениях;
- 6) автоматическую выгрузку информации о выписанных льготных рецептах в региональную информационную систему учета и обеспечения дополнительного лекарственного обеспечения.

6. Доступ к электронным сервисам системы

6.1. Права доступа к электронному сервису определяет оператор ЕМИСЗ РК в соответствии с ее регламентом.

6.2. Информация о правах доступа к электронному сервису заносится в подсистему управления доступом к электронным сервисам администраторами ЕМИСЗ РК.

- 6.3. Для авторизации пользователя ЕМИСЗ РК используются логин и пароль.
- 6.4. Для получения логина и пароля пользователи ЕМИСЗ РК отправляют заявку оператору ЕМИСЗ РК. В заявке указываются пользователи ЕМИСЗ РК, которым будут выданы логин и пароль. Логин и пароль передаются оператором ЕМИСЗ РК лицу, указанному в заявке, в письменном виде в срок до 5 дней с момента подачи заявки.
- 6.5. Пользователи ЕМИСЗ РК - работники медицинской организации и сотрудники Министерства здравоохранения Республики Крым обладают правами доступа к функциональным компонентам ЕМИСЗ РК.
- 6.6. Пользователи ЕМИСЗ РК - пациенты МО обладают правами доступа к следующим электронным сервисам:
запись на прием к врачу;
контроль готовности результатов исследований;
просмотр расписаний;
регистрация жалоб и заявлений.
- 6.7. Предоставление информации с использованием электронных сервисов, подключенных к ЕМИСЗ РК, осуществляется с применением средств криптографической защиты информации.

7. Защита персональных данных в ЕМИСЗ РК

- 7.1. Мероприятия по защите персональных данных, обрабатываемых в ЕМИСЗ РК, выполняются в целях исключения неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
- 7.2. Защита персональных данных, обрабатываемых в ЕМИСЗ РК, осуществляется в соответствии с требованиями статьи 19 Федерального закона Российской Федерации "О персональных данных", нормативными актами Правительства Российской Федерации, принятыми во исполнение указанного Федерального 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.
- 7.3. Защита персональных данных, обрабатываемых в ЕМИСЗ РК, достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности персональных данных в процессе их обработки, хранения и передачи по каналам связи, а также работоспособности технических средств, входящих в состав ЕМИСЗ РК.

Заместитель Председателя Совета министров
Республики Крым -
руководитель Аппарата Совета министров
Республики Крым
Л.ОПАНАСЮК

**Концепция информационной безопасности государственной информационной
системы "Единая медицинская информационная система здравоохранения
Республики Крым"**

Приложение 1
к приказу
Министерства здравоохранения
Республики Крым
от 19.02.2018 N 267
(в ред. Приказа Министерства здравоохранения Республики Крым от 22.04.2019 N 725)

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 предназначенная 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 оказанию 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 системы, 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 N 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 N 152 "О персональных данных", нормативными актами Правительства РФ, принятыми 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 применения 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 N 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 системы 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. N 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 - "тонкий клиент" (веб-браузер) - 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 ее 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 N 152-ФЗ "О персональных данных";
- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";
- Постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (далее - Постановление Правительства РФ N 1119);
- Постановление Правительства РФ от 06.07.2008 N 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 N 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 N 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 ("Дорожная карта") 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 2015 г.

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 N 17 от 11.02.2013 (далее - Приказ ФСТЭК N 17);

- Меры защиты информации в ГИС, утвержденные 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 N 152 от 13 июня 2001 г.:

- приказ ФСБ России от 10.07.2014 N 378 "Об утверждении Состав 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 N 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 утверждаются 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 приведен 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 N 1119 и Приказом ФСТЭК России N 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, ее класс защищенности 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;
- оценку вреда, который может быть причинен субъектам ПДн в случае нарушения требований Федерального закона N 152-ФЗ, соотношения 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 N 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 серверы и каналы связи;
 - обеспечения гарантированного электропитания;
 - контроль, в том числе с использованием программных и технических средств, за действиями пользователей и реакцией 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 определенных 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 осуществлять 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 соответствии с требованиями приказов ФСТЭК России N 17 и N 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 ее 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 подтверждаются 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 ФСБ 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 N 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 находиться 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 находиться другое ПО, необходимое для выполнения производственных задач ЕМИСЗ РК, при этом данное ПО должно быть официально приобретено 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 централизованно 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 защищенности 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 приемочных 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 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.

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.

Описание технических и программных средств обеспечения информационной безопасности ЕМИСЗ РК

Приложение
к Концепции
информационной безопасности
государственной информационной системы
"Единая медицинская информационная система
здравоохранения Республики Крым"
от 19.02.2018 N 267

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 серверы 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 представлены 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 представлены 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 N 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 производиться установка ПАК ViPNet Coordinator HW 1000, 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 осуществляются 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 представлены 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 N 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 N 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 N 17 должны быть реализованы меры по идентификации и аутентификации пользователей (ИАФ), управлению доступом (УПД), защите 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 серверы ЕМИСЗ РК, а также АРМ пользователей оснащены СЗИ от НСД Dallas Lock 8.0-К.

3.5. Средства антивирусной защиты.

В соответствии с приказом ФСТЭК России N 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 сертифицированное ФСТЭК России АвПО Kaspersky Anti-Virus.

3.6. Средства анализа защищенности.

В соответствии с приказом ФСТЭК России N 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 N 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 N 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 изменениях 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.

Единый регламент организации информационного взаимодействия медицинских организаций с государственной информационной системой "Единая медицинская информационная система здравоохранения Республики Крым"

Приложение 1
к приказу
Министерства здравоохранения
Республики Крым
от 22.04.2019 N 725
(в ред. Приказа Министерства здравоохранения Республики Крым от 26.11.2019 N 2190)

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 предназначенная 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 оказанию 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.

МЗ РК - 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, осуществляющая 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 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (далее - ФЗ N 149);
- Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных" (далее - ФЗ N 152);

- Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (далее - ПП РФ N 1119);
- Постановлением Правительства Российской Федерации N 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 N 211);
- Приказом ФСТЭК России N 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 N 21);
- Приказом ФСБ России N 378 от 10 июля 2014 года "Об утверждении Состав 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 N 378);
- Приказом ФСТЭК России N 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 N 17);
- Концепцией информационной безопасности государственной информационной системы "Единая медицинская информационная система здравоохранения Республики Крым", утвержденной Приказом Министерства Здравоохранения N 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) - "тонкий клиент" (веб-браузер) - и реализуется для работы по модели "облачных вычислений".

3.2. ГИС ЕМИСЗ РК создана для обработки ПДн граждан, обратившихся в МО МЗ РК 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 N 17 и ПП РФ N 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 опытной эксплуатации. По завершении процедуры аттестации ГИС ЕМИСЗ РК по

требованиям безопасности информации данная система будет введена в промышленную эксплуатацию.

(п. 3.5 в ред. Приказа Министерства здравоохранения Республики Крым от 26.11.2019 N 2190)

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 централизованно 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 N 4960.

5. Организационные 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 N 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 контроллера 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 данной 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 трех 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 Претендента, 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 mrgk.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 контроллером 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 требованиям 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 требованиями настоящего Регламента.

7.3. Оптимальные технико-параметрические требования, предъявляемые эксплуатационными характеристиками ЕМИСЗ РК к АРМ и серверному оборудованию, изложены в Приложении N 3* данного Регламента.

* Приложение N 3 не приводится. - Примечание изготовителя базы данных.

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 N 1. Заявление на организацию информационного взаимодействия с
государственной информационной системой ЕМИСЗ РК

Приложение N 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 22.04.2019 N 725

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 МЗ РК проведены.

АРМ готовы к работе в защищенной корпоративной сети передачи данных
Министерства здравоохранения Республики Крым (сеть ViPNet N 4960).

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

Таблица 1. Предварительные сведения

Таблица 1. Предварительные сведения

N п/п	Описание параметра	Значение
1	Полное наименование МО	
2	Цель подключения	
3	Краткое наименование МО	
4	ИНН	

5	Количество подключаемых АРМ	
6	Наименования абонентских пунктов в сети ViPNet N 4960/IP-адреса АРМ	
7	Количество и наименования АВПО, установленных на АРМ в подключаемом сегменте ЗЛВС	
8	Количество и наименования 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 контроллера 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. Шаблон типового Соглашения о защищенном информационном взаимодействии

Приложение 2

к приказу

Министерства здравоохранения

Республики Крым

от 22.04.2019 N 725

ШАБЛОН ТИПОВОГО СОГЛАШЕНИЯ О ЗАЩИЩЕННОМ ИНФОРМАЦИОННОМ ВЗАИМОДЕЙСТВИИ N _____

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 N 149, и _____, именуемый в дальнейшем "Сторона 2", в

лице директора _____, действующего на основании Устава, утвержденного приказом Министерства здравоохранения Республики Крым от _____ N ___, 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 N 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 подписанном 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 информации по организации защищенного информационного взаимодействия с использованием процедур межсетевого обмена ViPNet.

3.2. Обмен электронными документами, их подпись и подтверждение целостности и подлинности документа осуществляются 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 создавалась 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 202__ 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/с: 03752202870) БИК: 043510001

Банк: ОТДЕЛЕНИЕ РЕСПУБЛИКА КРЫМ

р/сч.: 40201810635100000006

л/сч.: 03752202870

Министр здравоохранения

Республики Крым

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 средствами взаимного экспорта/импорта, о чем администраторы защищенных сетей уведомляют друг друга с помощью ПО ViPNet [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 N 4960 ООО "Информационные системы и Аутсорсинг" / _____/

Администратор безопасности сети N _____/ _____/

Сторона 1

Сторона 2:

Министр здравоохранения

Республики Крым

_____/ А.И. Голенко

Выберите элемент

_____/ _____/



**МІНІСТЕРСТВО
ОХОРОНИ ЗДОРОВ'Я
РЕСПУБЛІКИ КРИМ**

**МИНИСТЕРСТВО
ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ КРЫМ**

**КЪЫРЫМ
ДЖУМХУРИЕТИ
САГЪЛЫКЪ САКЪЛАВ
НАЗИР ЛИГИ**

пр.Кирова, 13, г.Симферополь, 295005. Тел.: 621-271 e-mail: minzdrav2014@mzdrav.rk.gov.ru
ОКПО 00182225, ОГРН 1149102018504, ИНН 9102012869, КПП 910201001

от 05.02.2020 № 01/419-01-А1
на № от

**Руководителям учреждений
здравоохранения,
подведомственным Министерству
здравоохранения Республики Крым**

В связи с частыми обращениями медицинских организаций в Министерство здравоохранения Республики Крым по вопросу ограничения доступа в Единой медицинской информационной системе здравоохранения Республики Крым (далее - ЕМИСЗ РК) к электронным медицинским картам пациентов психиатрического, наркологического, ВИЧ и фтизиатрического профиля, Министерство здравоохранения Республики Крым разъясняет следующее,

Согласно части 1 статьи 23 Конституции Российской Федерации каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (часть 1 статьи 24 Конституции Российской Федерации),

Частью первой статьи 13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее - Закон № 323-ФЗ) установлено, что сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну,

В соответствии с пунктом 4 Указа Президента Российской Федерации от 06.03.1997 № 188 к Перечню сведений конфиденциального характера, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами, отнесена врачебная тайна,

Таким образом, сведения о состоянии здоровья пациента относятся к охраняемой законом врачебной тайне,

Соблюдение врачебной тайны является одним из принципов охраны здоровья граждан (пункт 9 статьи 4 Закона № 323-ФЗ), Такое правовое

регулирование направлено на обеспечение защиты права гражданина на неприкосновенность частной жизни, личную тайну и препятствует бесконтрольному разглашению сведений личного характера.

Кроме того, согласно пункту 2 части 2 статьи 73 Закона № 323-ФЗ **медицинские работники обязаны соблюдать врачебную тайну.**

О том, что медицинские работники обязаны хранить врачебную тайну, говорится и в клятве врача (ст. 71 Закона № 323-ФЗ). Обязанность медицинских и фармацевтических работников, медицинских организаций соблюдать врачебную тайну прописана также в пп. 2 п. 2 ст. 73 и пп. 4 п. 1 ст. 79 Закона № 323-ФЗ.

Обмен информацией в ходе оказания медицинской помощи не квалифицируется как нарушение врачебной тайны. К примеру, без предварительного согласия пациента врач может предоставлять сведения о пациенте своему руководителю, также несущему ответственность за результаты лечения. **Однако если данная информация сообщается не с целью оказания медицинской помощи, а при беседе врачей, других медицинских работников или при общении с неспециалистами, то такое действие может быть квалифицировано как нарушение ст. 73 Закона № 323-ФЗ.**

Согласно разъяснениям, содержащимся в п. 43 Постановления Пленума ВС РФ от 17.03.2004 № 2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации», в случае оспаривания работником увольнения за разглашение врачебной тайны работодатель обязан представить доказательства, свидетельствующие о том, что информация, разглашенная работником, **относится к охраняемой законом тайне**, эта информация стала известна работнику **в связи с исполнением им трудовых обязанностей** и он **обязался не разглашать** такие сведения.

Подписывая трудовой договор, работник медицинской организации обязывается хранить врачебную тайну, ставшую ему известной при осуществлении своей деятельности.

Таким образом, вышеприведенными нормами права предусмотрен прямой запрет на обнародование врачебной тайны, за нарушение которого предусмотрено наказание, в том числе: увольнение с работы (*подпункт "в" пункта б части первой статьи 81 Трудового кодекса Российской Федерации: разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника*).

В пункте 4 статьи 13 Закона № 323-ФЗ содержится исчерпывающий перечень оснований, по которым допускается предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя:

- проведение медобследования и лечения гражданина, не способного выразить свою волю в результате своего состояния;
- угроза распространения инфекционных заболеваний, массовых отравлений

и поражений;

- запрос органов дознания и следствия, суда, прокуратуры, уголовно-исполнительной системы;

- оказание медпомощи несовершеннолетнему, больному наркоманией, а также несовершеннолетнему, не достигшему 15 лет, для информирования родителей или законного представителя;

- информирование органов внутренних дел о поступлении пациента, получившего вред в результате противоправных действий;

- проведение военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых предусмотрена военная и приравненная к ней служба;

- расследование несчастного случая на производстве и профзаболевания, несчастного случая с обучающимся во время пребывания в обучающей организации;

- обмен информацией медицинскими организациями при оказании медпомощи;

- учет и контроль в системе ОМС;

- контролирование качества и безопасности медицинской деятельности.

Таким образом, на основании пункта 8 части 4 статьи 13 Закона № 323-ФЗ, предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается при обмене информацией медицинскими организациями, **в том числе размещенной в медицинских информационных системах**, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных.

Из Концепции информационной безопасности государственной информационной системы ЕМИСЗ РК, являющейся приложением № 1 к приказу Министерства здравоохранения Республики Крым от 19.02.2018 №267 прямо следует: «В соответствии со ст. 79 Федерального закона от 21 ноября 2011 года № 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.

Концепция разработана в соответствии с постановлением Совета министров Республики Крым от 20 декабря 2016 года № 612 «О единой медицинской

информационной системе здравоохранения Республики Крым».

Так, разделом 7 Положения о государственной информационной системе «Единая медицинская информационная система здравоохранения Республики Крым», утвержденного вышеуказанным постановлением № 612 определены требования к защите персональных данных в ЕМИСЗ РК.

В соответствии с требованиями Федеральной службы по техническому и экспертному контролю ЕМИСЗ РК защищается средствами криптозащиты.

Дополнительно следует отметить, что медицинские работники и фармацевтические работники осуществляют свою деятельность в соответствии с законодательством Российской Федерации, руководствуясь принципами медицинской этики и деонтологии (часть 1 статьи 73 Закона №323-ФЗ).

Использование ЕМИСЗ РК способствует увеличению качества работы медицинских работников, а также предотвращает потерю данных истории болезни пациентов.

Кроме того, специальными нормами, регулирующими работу медицинских организаций по различным направлениям, в том числе: фтизиатрии и пульмонологии, психиатрии и неврологии, **не предусмотрены дополнительные ограничения в отношении доступа к группам диагнозов пациентов другими медицинскими организациями.**

На основании изложенного, сведения, содержащиеся в ЕМИСЗ РК могут быть доступными для всех медицинских организаций без ограничений со строгим соблюдением всех требований, предусмотренных действующим законодательством.

В целях предупреждения нарушений врачебной тайны, ставшей известной в процессе осуществления своей деятельности, руководители учреждений здравоохранения должны провести соответствующие разъяснения среди своих работников.

Министр

И. ЧЕМОДАНОВ