Экз. № 1

Областное государственное бюджетное учреждение здравоохранения «Медицинский информационно-аналитический центр Костромской области»

УТВЕРЖДАЮ

Директор

ОГБУЗ «МИАЦ»

_____ А.А. Майоров

«25» марта 2020 г.

РЕГЛАМЕНТ

подключения медицинских организаций Костромской области к ГИС Региональной медицинской системе Костромской области

Кострома

2020

РЕГЛАМЕНТ

подключения медицинских организаций Костромской области к ГИС «РМИС»
областного государственного бюджетного учреждения здравоохранения
«Медицинский информационно-аналитический центр Костромской области»

1 Перечень используемых терминов и определений

Ниже приведен перечень терминов и определений, используемых в настоящем Регламенте.

Внешняя информационная система (относительно ГИС «РМИС» ОГБУЗ «МИАЦ») – иная информационная система, с которой у ГИС «РМИС» ОГБУЗ «МИАЦ» установлено либо планируется установить информационное взаимодействие.

Медицинская организация – организация Костромской области, которая подключила или планирует подключить АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ», или внешние информационные системы.

2 Перечень используемых сокращений

АРМ	–	автоматизированное рабочее место
ГИС «РМИС»	–	государственная информационная система Региональная медицинская система Костромской области
ИТ	–	информационные технологии
НСД	–	несанкционированный доступ
ОГБУЗ «МИАЦ»	–	областное государственное бюджетное учреждение здравоохранения «Медицинский информационно-аналитический центр Костромской области»
ОС	–	операционная система
ПДн	–	персональные данные
ПО	–	программное обеспечение
СВТ	–	средство вычислительной техники
СрЗИ	–	средство защиты информации
СКЗИ	–	средство криптографической защиты информации

3 Введение

3.1 Настоящий Регламент определяет:

- порядок подключения АРМ, функционирующих в медицинских организациях Костромской области, к ГИС «РМИС» ОГБУЗ «МИАЦ»;
- порядок эксплуатации АРМ, подключенных к ГИС «РМИС» ОГБУЗ «МИАЦ»;
- порядок подключения внешних информационных систем к ГИС «РМИС» ОГБУЗ «МИАЦ».

3.2 Основной целью принятия настоящего Регламента является определение условий, выполнение которых при подключении АРМ и внешних информационных систем к ГИС «РМИС» позволит обеспечить соблюдение установленных требований по обеспечению безопасности ПДн, обрабатываемых в ГИС «РМИС».

4 Положение о возможности распространения аттестатов соответствия типовых АРМ ГИС «РМИС» ОГБУЗ «МИАЦ» на подключаемые АРМ

4.1 ГИС «РМИС» ОГБУЗ «МИАЦ» состоит из следующих сегментов:

- сегмент «Регистр онкологических больных»;
- сегмент «Регистр потребностей хронических больных»;
- сегмент «Регистр ИПРА»;
- сегмент «Корвет»;
- сегмент «Витакор»;
- сегмент «Визуализатор»;
- сегмент «Парус»;
- сегмент «ЦАМИ»;
- сегмент «Национальный радиационно-эпидемиологический регистр».

4.2 Совокупность перечисленных сегментов ГИС «РМИС» ОГБУЗ «МИАЦ» и подключенных к ним АРМ пользователей реализует полный технологический процесс обработки информации.

4.3 ГИС «РМИС» ОГБУЗ «МИАЦ» аттестуется по требованиям приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», при этом:

- сегмент «Парус» ГИС «РМИС» ОГБУЗ «МИАЦ» аттестуется по требованиям, предъявляемым к информационным системам 3 класса защищенности;
- остальные сегменты ГИС «РМИС» ОГБУЗ «МИАЦ» аттестуется по требованиям, предъявляемым к информационным системам 2 класса защищенности;
- АРМ, подключаемые к сегменту «Парус» ГИС «РМИС» ОГБУЗ «МИАЦ», аттестуются по требованиям, предъявляемым к информационным системам 3 класса защищенности.
- АРМ, подключаемые к остальным сегментам ГИС «РМИС» ОГБУЗ «МИАЦ», на которых обрабатывается ПДн менее чем 100 000 субъектов, аттестуются по требованиям, предъявляемым к информационным системам 3 класса защищенности, а на которых обрабатывается ПДн более чем 100 000 субъектов, аттестуются по требованиям, предъявляемым к информационным системам 2 класса защищенности.

4.4 Аттестация АРМ, подключаемых к ГИС «РМИС» ОГБУЗ «МИАЦ», осуществляется путем аттестации типовых АРМ и распространения действия аттестатов соответствия типовых АРМ ГИС «РМИС» ОГБУЗ «МИАЦ» на прочие АРМ при условии их соответствия типовым АРМ, прошедшим аттестационные испытания.

4.5 АРМ, подключаемое к ГИС «РМИС» ОГБУЗ «МИАЦ», считается соответствующим типовому АРМ, в отношении которого были проведены аттестационные испытания, если для указанного АРМ установлены одинаковые класс защищенности, угрозы безопасности информации,

реализованы одинаковые проектные решения по информационной системе и ее системе защиты информации.

4.6 Соответствие АРМ, подключаемого к ГИС «РМИС» ОГБУЗ «МИАЦ», типовому АРМ, в отношении которого были проведены аттестационные испытания, подтверждается в ходе приемочных испытаний подключаемого АРМ.

4.7 На АРМ, подключаемом к ГИС «РМИС» ОГБУЗ «МИАЦ», на которое распространяется аттестат соответствия, ОГБУЗ «МИАЦ» (оператором) обеспечивается соблюдение эксплуатационной документации на систему защиты информации подключаемого АРМ и организационно-распорядительных документов по защите информации.

5 Порядок подключения внешних информационных систем к ГИС «РМИС»

5.1 Основанием для проведения комплекса мероприятий по подключению внешней информационной системы к ГИС «РМИС» ОГБУЗ «МИАЦ» является заявка на подключение к ГИС «РМИС» (форма приведена в Приложении 1), подготовленная владельцем (оператором) подключаемой информационной системы и направленная в ОГБУЗ «МИАЦ» в форме официального письма на бумажном носителе или в электронном виде.

5.2 Обязательным условием при подключении внешней информационной системы к ГИС «РМИС» ОГБУЗ «МИАЦ» является наличие у подключаемой информационной системы аттестата соответствия.

5.3 Работники отдела ИТ ОГБУЗ «МИАЦ» обеспечивают согласование заявки с директором ОГБУЗ «МИАЦ». В случае отказа в подключении к ГИС «РМИС» в адрес заявителя направляется соответствующее уведомление с указанием причин отказа.

5.4 На основании согласованной заявки работники отдела ИТ ОГБУЗ «МИАЦ» организуют совместную с владельцем (оператором) внешней информационной системы работу по ее подключению к ГИС «РМИС».

5.5 Владелец (оператор) подключенной информационной системы должен своевременно проводить контроль за обеспечением уровня защищенности информации, содержащейся в этой информационной системе.

5.6 В случае, если владелец (оператор) подключенной информационной системы по результатам контроля за обеспечением уровня защищенности информации, содержащейся в этой информационной системе, принял решение о необходимости доработки (модернизации) ее системы защиты информации, то он уведомляет об этом работников отдела ИТ ОГБУЗ «МИАЦ». Информационное взаимодействие ГИС «РМИС» с внешней информационной системой прекращается до момента завершения доработки (модернизации) системы защиты информации, обрабатываемой во внешней информационной системе.

6 Порядок подключения АРМ к ГИС «РМИС»

6.1 Основанием для проведения комплекса мероприятий по подключению АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ» являются заявка на подключение (отключение) АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ» (форма приведена в Приложении 2) и заявка на изменение списка пользователей ГИС «РМИС» (форма приведена в Приложении 3), подготовленные медицинской организацией и

направленные в ОГБУЗ «МИАЦ» в форме официального письма на бумажном носителе или в электронном виде.

6.2 Работники отдела ИТ ОГБУЗ «МИАЦ» обеспечивают согласование заявок с директором ОГБУЗ «МИАЦ». В случае отказа в подключении к ГИС «РМИС» в адрес медицинской организации направляется соответствующее уведомление с указанием причин отказа.

6.3 На основании согласованных заявок работники отдела ИТ ОГБУЗ «МИАЦ» направляют в адрес медицинской организации требования, выполнение которых является обязательным условием при подключении АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ» (форма приведена в Приложении 4).

6.4 Медицинская организация выполняет обязательные требования по подключению АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ» своими силами или с привлечением сторонних организаций. При необходимости монтажа, установки и наладки СКЗИ заявитель для этой цели привлекает стороннюю организацию, имеющую лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации и лицензию ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя). Медицинская организация вправе самостоятельно осуществлять для собственных нужд юридического лица или индивидуального предпринимателя работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства. В случае привлечения медицинской организацией сторонней организации для выполнения работ по внедрению технических, программных и программно-технических средств защиты информации, не являющихся СКЗИ, привлекаемая организация должна иметь лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

6.5 Непосредственный руководитель работника, АРМ которого необходимо подключить к ГИС «РМИС» ОГБУЗ «МИАЦ», обеспечивает ознакомление пользователя с порядком эксплуатации АРМ и его обязанностями по выполнению требований по защите ПДн. Факт прохождения инструктажа подтверждается подписью пользователя в соответствующем журнале и (или) листе ознакомления с соответствующими документами.

6.6 По завершении работ по выполнению обязательных требований медицинская организация (либо привлекаемая для проведения данных работ сторонняя организация, имеющая лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации) проводят приемочные испытания подключаемого АРМ в соответствии с Программой и методиками, в ходе которых подтверждают соответствие такого АРМ типовому АРМ, в отношении которого были проведены аттестационные испытания. При положительной оценке результатов испытаний в Протоколе приемочных испытаний медицинская организация оформляет акт соответствия подключаемого АРМ (сегмента ГИС «РМИС») типовому АРМ, в отношении которого были проведены аттестационные испытания (аттестованному типовому сегменту ГИС «РМИС»), и направляет один экземпляр в ОГБУЗ «МИАЦ».

6.7 При получении от медицинской организации акта соответствия подключаемого АРМ типовому АРМ уполномоченные специалисты ОГБУЗ «МИАЦ» принимают решение о включении АРМ медицинской организации в состав ГИС «РМИС», утверждают оформленное в форме приказа решение в установленном порядке, после чего работники отдела ИТ ОГБУЗ «МИАЦ» обеспечивают логическое подключение АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ», в том числе передачу пользователю АРМ учетных данных для доступа к ресурсам ГИС «РМИС» способом, исключающим возможность ознакомления с ними или их использования посторонними лицами.

7 Порядок эксплуатации АРМ, подключенных к ГИС «РМИС» ОГБУЗ «МИАЦ»

7.1 Порядок эксплуатации АРМ, подключенных к ГИС «РМИС» ОГБУЗ «МИАЦ» состоит из следующих разделов:

- Порядок действий в случае нарушения работоспособности АРМ;
- Требования по размещению АРМ и допуску к работе на АРМ;
- Права и обязанности пользователя АРМ.

8 Порядок действий в случае нарушения работоспособности АРМ

8.1 О нарушении работоспособности АРМ, подключенного к ГИС «РМИС» ОГБУЗ «МИАЦ», пользователь указанного АРМ должен сообщить лицам, осуществляющим техническое обслуживание СВТ организации, которой принадлежит данное АРМ. Лица, осуществляющие техническое обслуживание СВТ, обследуют АРМ на предмет выявления причины его неработоспособности, и сообщают о результатах обследования работникам отдела ИТ ОГБУЗ «МИАЦ».

8.2 Лица, осуществляющие техническое обслуживание СВТ организации, которой принадлежит АРМ, подключенное к ГИС «РМИС» ОГБУЗ «МИАЦ», выполняют в рамках своих полномочий поручения работников отдела ИТ ОГБУЗ «МИАЦ», направленные на восстановление работоспособности данного АРМ.

8.3 Лицам, осуществляющим техническое обслуживание АРМ, подключенного к ГИС «РМИС» ОГБУЗ «МИАЦ», запрещается самовольно вносить какие-либо изменения в состав, размещение, конфигурацию программного и аппаратного обеспечения АРМ, в том числе устанавливать дополнительно любые программные и аппаратные средства[1], отключать СрЗИ (СКЗИ), установленные на АРМ. При необходимости внести изменения в программное или аппаратное обеспечение АРМ, подключенного к ГИС «РМИС» ОГБУЗ «МИАЦ», указанные лица извещают об этом работников отдела ИТ ОГБУЗ «МИАЦ». Работники отдела ИТ ОГБУЗ «МИАЦ» принимают решение о допустимости либо о недопустимости внесения таких изменений.

8.4 Работники отдела ИТ ОГБУЗ «МИАЦ» в случае внесения изменений в состав, размещение, конфигурацию программного и аппаратного обеспечения АРМ, подключенного к ГИС «РМИС» ОГБУЗ «МИАЦ», принимают решение о необходимости проведения приемочных испытаний такого АРМ, в ходе которых подтверждают его соответствие типовому АРМ, в отношении которого были проведены аттестационные испытания.

8.5 После получения от ОГБУЗ «МИАЦ» подтверждения о возможности эксплуатации АРМ (подтверждения его соответствия требованиям) пользователь возобновляет обработку ПДн на АРМ.

[1] За исключением служебных съемных машинных носителей информации, используемых работником в рамках выполнения его должностных обязанностей.

9 Требования по размещению АРМ и допуску к работе на АРМ

9.1 АРМ, подключенное к ГИС «РМИС» ОГБУЗ «МИАЦ», должно быть размещено в пределах контролируемой зоны в соответствии с ее границами, определенными организационно-распорядительными документами в организации, которой принадлежит это АРМ (далее – организация).

9.2 В организации должен быть определен порядок доступа в помещение с установленным АРМ, а также перечень лиц, имеющих право доступа в данное помещение.

9.3 В нерабочее время должна обеспечиваться охрана помещения с установленным АРМ.

9.4 При размещении средств отображения информации (мониторов) должна быть исключена возможность несанкционированного просмотра выводимой на них информации лицами, не имеющими права доступа к ней.

9.5 Допуск работников организации к работе на АРМ должен осуществляться в соответствии с должностными обязанностями работников или иными организационно-распорядительными документами, принятыми в организации.

9.6 В случае смены пользователя (либо изменения сведений о пользователе) АРМ непосредственный руководитель пользователя в течение 3 рабочих дней составляет заявку на изменение списка пользователей (по форме, приведенной в Приложении 3) и направляет ее в ОГБУЗ «МИАЦ» в форме официального письма на бумажном носителе или в электронном виде.

9.7 В случае принятия медицинской организацией решения об отключении АРМ от ГИС «РМИС» ОГБУЗ «МИАЦ» она составляет заявку на подключение (отключение) АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ» (форма приведена в Приложении 2) и направляет ее в ОГБУЗ «МИАЦ» в форме официального письма на бумажном носителе или в электронном виде.

10 Права и обязанности пользователя АРМ

10.1 Пользователь АРМ обязан:

10.1.1 хранить в тайне свои учетные данные (логин и пароль) для доступа к ресурсам ГИС «РМИС»;

10.1.2 вводить учетные данные для доступа к ресурсам ГИС «РМИС» в отсутствие лиц, которые потенциально могут увидеть процесс набора символов на клавиатуре;

10.1.3 немедленно прекратить обработку ПДн и поставить в известность работников отдела ИТ ОГБУЗ «МИАЦ» в случаях:

- возникновения подозрения о компрометации[1] пароля для доступа к ресурсам ГИС «РМИС»;
- обнаружения не предусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств.

[1] Под компрометацией пароля пользователя ГИС «РМИС» в настоящем Регламенте понимаются события, в результате которых личный пароль пользователя с высокой вероятностью стал доступным третьим лицам.

Возобновление обработки ПДн на АРМ производится после устранения причин, повлекших прекращение обработки ПДн, а также после подтверждения работниками отдела ИТ ОГБУЗ «МИАЦ» возможности продолжения эксплуатации АРМ;

10.1.4 поставить в известность лиц, ответственных за техническое обслуживание СВТ организации, в случае возникновения отклонений в нормальной работе программных или аппаратных средств АРМ, затрудняющих его эксплуатацию;

10.1.5 незамедлительно выполнять указания работников отдела ИТ ОГБУЗ «МИАЦ», а также при необходимости предоставлять им АРМ для проведения контрольных мероприятий.

10.2 Пользователю АРМ запрещается:

10.2.1 сообщать учетные данные для доступа к ресурсам ГИС «РМИС» любым третьим лицами либо предоставлять им возможность совершать действия от имени своей учетной записи;

10.2.2 хранить пароль, записанный на бумажном носителе, непосредственно на рабочем месте или в местах, откуда он может быть похищен. Хранение пользователем своего пароля на бумажном носителе допускается только в запираемом хранилище личного пользования (ящике, шкафу, сейфе) либо в запираемом хранилище непосредственного руководителя в опечатанном конверте;

10.2.3 использовать программные и аппаратные компоненты АРМ в неслужебных целях;

10.2.4 самовольно вносить какие-либо изменения в состав, размещение, конфигурацию программного и аппаратного обеспечения АРМ, в том числе устанавливать дополнительно любые программные и аппаратные средства[1], отключать СрЗИ (СКЗИ), установленные на АРМ;

10.2.5 привлекать лиц, не уполномоченных на осуществление технического обслуживания СВТ организации, для производства ремонта аппаратных элементов АРМ или установки (настройки) системного или прикладного ПО без согласования с работниками отдела ИТ ОГБУЗ «МИАЦ»;

10.2.6 оставлять без присмотра включенное АРМ, не активизировав временную блокировку экрана средствами ОС;

10.2.7 умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках ПО АРМ, а также установленных на АРМ СрЗИ (СКЗИ), которые позволяют преодолеть (обойти) механизмы СрЗИ, отключить их либо нарушить их функционирование, получить доступ к ПДн без прохождения процедур идентификации и аутентификации. Об обнаружении такого рода ошибок пользователь АРМ должен незамедлительно ставить в известность работников отдела ИТ ОГБУЗ «МИАЦ»;

10.2.8 осуществлять попытки НСД к ресурсам ГИС «РМИС», а также попытки нарушения их функционирования;

[1] За исключением служебных съемных машинных носителей информации, используемых работником в рамках выполнения его должностных обязанностей.

10.2.9 разглашать ПДн, обрабатываемые в ГИС «РМИС», ставшие известными пользователю в процессе выполнения им должностных обязанностей;

10.2.10 искажать (повреждать) информацию, обрабатываемую в ГИС «РМИС», а также уничтожать ее, если это не предусмотрено его должностными обязанностями.

10.3 Пользователь АРМ имеет право:

10.3.1 требовать от уполномоченных сотрудников ОГБУЗ «МИАЦ» смены учетных данных пользователя в случае их компрометации;

10.3.2 получать консультацию по вопросам защиты ПДн, обрабатываемых на АРМ, от сотрудников ОГБУЗ «МИАЦ», ответственных за организацию безопасной эксплуатации ГИС РМИС.

10.4 Пользователь АРМ несет персональную ответственность за:

10.4.1 надлежащее исполнение обязанностей, закрепленных в настоящем Регламенте;

10.4.2 все действия, совершенные с информационными ресурсами ГИС «РМИС» от имени его учетной записи, в том числе при использовании третьими лицами скомпрометированного пароля, если он не был своевременно сменен пользователем.

11 Порядок контроля выполнения требований, установленных настоящим Регламентом

11.1 Контроль выполнения требований, закрепленных настоящим Регламентом, проводится в рамках выполнения ОГБУЗ «МИАЦ» функции по обеспечению проведения контроля за обеспечением уровня защищенности информации, содержащейся в ГИС «РМИС».

11.2 Контроль за обеспечением уровня защищенности информации, содержащейся в ГИС «РМИС», проводится ОГБУЗ «МИАЦ» самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

11.3 Периодичность проведения контроля за обеспечением уровня защищенности информации, содержащейся в ГИС «РМИС», устанавливается ОГБУЗ «МИАЦ» в организационно-распорядительных документах по защите информации с учетом особенностей функционирования ГИС «РМИС», но не реже 1 раза в два года.

Приложение № 1
к регламенту подключения медицинских организаций Костромской области к ГИС «РМИС» областного государственного бюджетного учреждения здравоохранения «Медицинский информационно-аналитический центр Костромской области»

ОБРАЗЕЦ

Заявка на подключение внешней информационной системы к ГИС «РМИС» ОГБУЗ «МИАЦ»

Наименование владельца (оператора) подключаемой информационной системы:

_____

_____.

Контактное лицо:_____

(ФИО, должность, структурное подразделение)

_____

_____

тел.:_____, эл. почта:_____.

Название подключаемой информационной системы:_____

_____

_____.

Цель подключения:_____

_____

_____.

Сегменты ГИС «РМИС», к которым планируется подключить информационную систему:

☐ Регистр онкологических больных;

☐ Регистр потребностей хронических больных;

☐ Регистр ИПРА;

☐ Корвет;

☐ Витакор;

☐ Визуализатор;

☐ Парус;

☐ ЦАМИ;

☐ Национальный радиационно-эпидемиологический регистр.

Аттестат соответствия подключаемой информационной системы (при наличии):

_____

(номер, дата выдачи, наименование выдавшей организации)

_____

_____.

Должность руководителя организации _____ *И.О. Фамилия*

Приложение № 2
к регламенту подключения медицинских организаций Костромской области к ГИС «РМИС» областного государственного бюджетного учреждения здравоохранения «Медицинский информационно-аналитический центр Костромской области»

ОБРАЗЕЦ

Заявка на подключение (отключение) АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ»

Наименование организации:

_____

_____

_____.

Контактное лицо:_____

(ФИО, должность, структурное подразделение)

_____

_____

тел.:_____, эл. почта:_____.

№	Адрес здания и название/номер помещения, в котором расположено АРМ	Инвентарный номер АРМ	Форм-фактор АРМ	Условные номера[1] сегментов ГИС «РМИС»	Действие
1	*г. Кострома, ул. Самоковская, д. 7*	*3965421102*	*Стационарное*	*7*	*подключение*

[1] Условные номера сегментов ГИС «РМИС»:
1 - Регистр онкологических больных;
2 - Регистр потребностей хронических больных;
3 - Регистр ИПРА;
4 - Корвет;
5 - Витакор;
6 - Визуализатор;
7 - Парус;
8 - ЦАМИ;
9 - Национальный радиационно-эпидемиологический регистр.

2	*г. Кострома, мкр-н. Паново, д. 18*	*52875*	*Моноблок*	*1, 9*	*отключение*

Должность руководителя организации _____ *И.О. Фамилия*

Приложение № 3
к регламенту подключения медицинских организаций Костромской области к ГИС «РМИС» областного государственного бюджетного учреждения здравоохранения «Медицинский информационно-аналитический центр Костромской области»

ОБРАЗЕЦ

Заявка на изменение списка пользователей
ГИС «РМИС» ОГБУЗ «МИАЦ»

Наименование организации:

_____

_____

_____.

Контактное лицо:_____
(ФИО, должность, структурное подразделение)

_____

_____

тел.:_____, эл. почта:_____.

№	Фамилия, имя, отчество	Дата рождения	Должность	Условные номера[1] сегментов ГИС «РМИС»	Действие
1	*Иванов Иван Иванович*	*15.03.1969*	*консультант*	*7*	*Создание учетной записи*
2	*Петрова Полина*	*21.11.1991*	*начальник отдела*	*7*	*Изменение*

[1] Условные номера сегментов ГИС «РМИС»:
1 - Регистр онкологических больных;
2 - Регистр потребностей хронических больных;
3 - Регистр ИПРА;
4 - Корвет;
5 - Витакор;
6 - Визуализатор;
7 - Парус;
8 - ЦАМИ;
9 - Национальный радиационно-эпидемиологический регистр.

	Павловна		*кадров*		*учетных данных в связи со сменой фамилии; новая фамилия – Архипова*
3	*Семенов Семен Семенович*	*07.09.1985*	*секретарь*	*1, 9*	*Удаление учетной записи в связи с увольнением*

Должность руководителя организации _____ *И.О. Фамилия*

Приложение № 4
к регламенту подключения медицинских организаций Костромской области к ГИС «РМИС» областного государственного бюджетного учреждения здравоохранения «Медицинский информационно-аналитический центр Костромской области»

ТРЕБОВАНИЯ

к автоматизированным рабочим местам
ГИС «РМИС» ОГБУЗ «МИАЦ»

1 Общие сведения

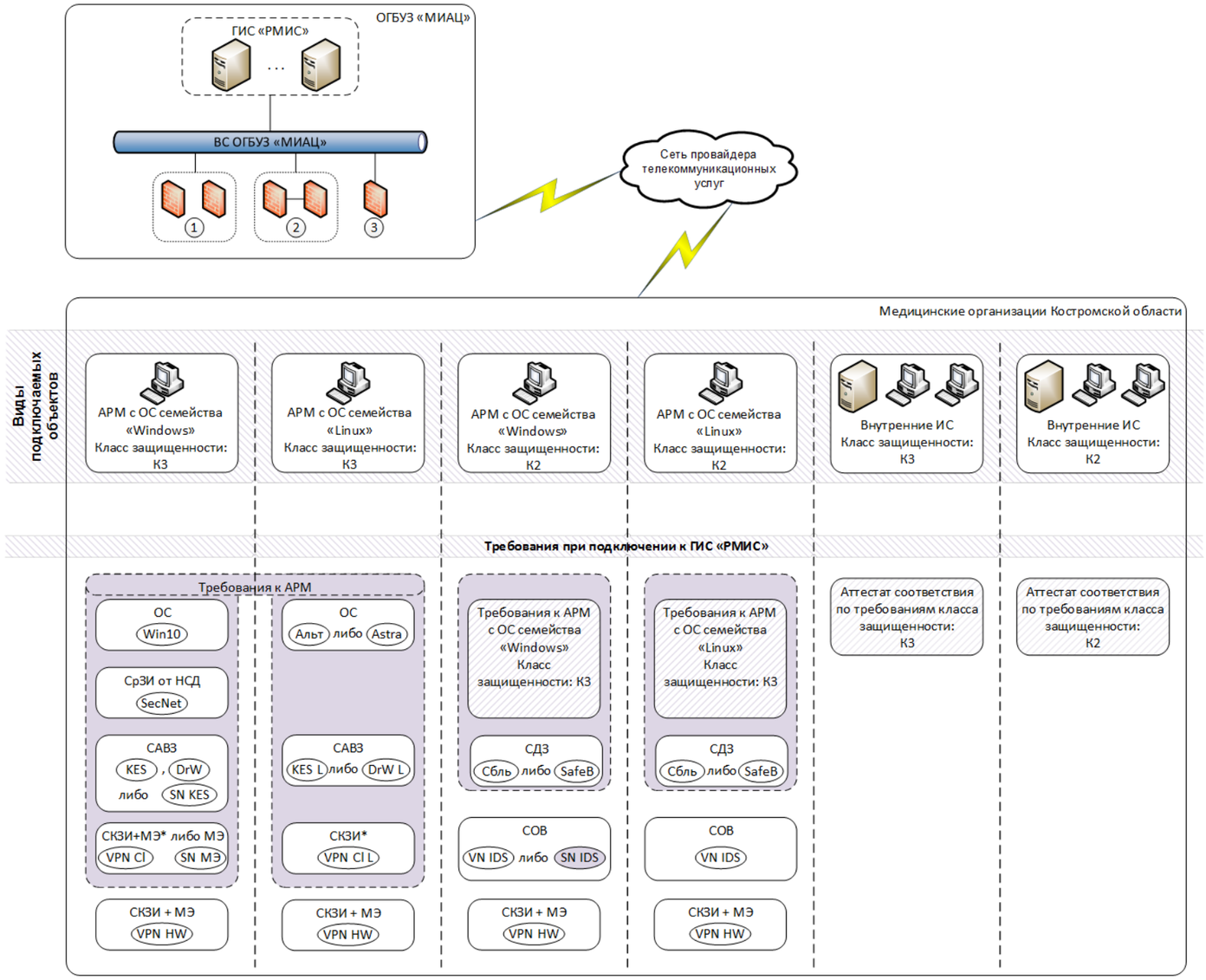
1.1 Медицинская организация при подключении АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ» должна выполнить настоящие Требования своими силами или с привлечением сторонних организаций. При необходимости монтажа, установки и наладки СКЗИ заявитель для этой цели привлекает стороннюю организацию, имеющую лицензию на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя). Медицинская организация вправе самостоятельно осуществлять для собственных нужд юридического лица или индивидуального предпринимателя работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства. По завершении работ по выполнению обязательных требований заявитель направляет в ОГБУЗ «МИАЦ» соответствующее уведомление.

1.2 АРМ, подключаемые к сегменту «Парус» ГИС «РМИС» ОГБУЗ «МИАЦ», подлежат аттестации по требованиям, предъявляемым к информационным системам 3 класса защищенности.

1.3 АРМ, подключаемые к остальным сегментам ГИС «РМИС» ОГБУЗ «МИАЦ», на которых обрабатывается ПДн менее чем 100 000 субъектов, подлежат аттестации по требованиям, предъявляемым к информационным системам 3 класса защищенности, а на которых обрабатывается ПДн более чем 100 000 субъектов, подлежат аттестации по требованиям, предъявляемым к информационным системам 2 класса защищенности.

1.4 АРМ должно отвечать требованиям, предъявляемым к нему производителями установленной ОС и применяемых средств защиты информации.

1.5 На рисунке 1 приведена общая схема подключения АРМ медицинских организаций к ГИС «РМИС» ОГБУЗ «МИАЦ».



Условные обозначения:

(1) - ПАК «ViPNet Coordinator HW1000» (сеть № 1955)

(2) - ПАК «ViPNet Coordinator HW1000» (ПАО «Ростелеком»)

(3) - ПАК «ViPNet Coordinator HW1000» (Администрация КО)

VPN HW - СКЗИ, МЭ ПАК «ViPNet Coordinator» (сеть ОГБУЗ «МИАЦ», сеть ПАО «Ростелеком», сеть Администрации КО, сеть медицинской организации КО)

Win10 - операционная система «Windows 10»

Альт - операционная система «Альт Линукс»

Astra - операционная система «Astra Linux Special Edition»

SecNet - средство защиты от несанкционированного доступа «Secret Net Studio»

KES - средство антивирусной защиты «Kaspersky Endpoint Security» (для Windows)

KES L - средство антивирусной защиты «Kaspersky Endpoint Security» (для Linux)

DrW - средство антивирусной защиты «Dr.Web Desktop Security Suite» (для Windows)

DrW L - средство антивирусной защиты «Dr.Web Desktop Security Suite» (для Linux)

SN KES - модуль антивирусной защиты (технология Kaspersky) в составе ПО «Secret Net Studio»

SN МЭ - модуль межсетевого экранирования в составе ПО «Secret Net Studio»

VPN Cl - средство криптографической защиты информации «ViPNet Client» (для Windows)

VPN Cl L - средство криптографической защиты информации «ViPNet Client» (для Linux)

Сбль - аппаратно-программный модуль доверенной загрузки «Соболь»

SafeB - программное средство доверенной загрузки «SafeBoot»

VN IDS - система обнаружения вторжений «ViPNet IDS»

SN IDS - модуль обнаружения вторжений в составе ПО «Secret Net Studio»

* - необходимо, при выполнении одного из условий:
1) контролируемая зона медицинской организации определена по ограждающим конструкциям кабинетов;
2) в точке подключения к сети провайдера телекоммуникационных услуг не установлен сертифицированный межсетевой экран (уровня сети)

Рис. 1. Общая схема подключения АРМ медицинских организаций к ГИС «РМИС» ОГБУЗ «МИАЦ»

2 Требования к составу АРМ

2.1 Общие требования к составу АРМ, подлежащих аттестации по требованиям, предъявляемым к информационным системам классов защищенности К3, К2.

2.1.1 Для защиты АРМ должны быть установлены последние сертифицированные версии СрЗИ. По истечении сроков действия сертификатов соответствия ФСТЭК России / ФСБ России либо при выявлении уязвимостей в установленных версиях СрЗИ медицинские организации, в состав которых входят подключаемые АРМ, должны провести работы по обновлении версий данных СрЗИ.

2.1.2 Допускается использование следующего системного ПО:

- ОС «Windows 10»;
- ОС «Альт Линукс»;
- ОС «Astra Linux Special Edition».

2.1.3 При использовании ОС «Windows 10» на АРМ необходимо установить СрЗИ от НСД «Secret Net Studio».

2.1.4 В зависимости от ОС на АРМ необходимо установить одно из следующих средств антивирусной защиты:

- ПО «Kaspersky Endpoint Security» (для Windows);
- ПО «Dr.Web Desktop Security Suite» (для Windows);
- модуль антивирусной защиты (технология Kaspersky) в составе ПО «Secret Net Studio»;
- ПО «Kaspersky Endpoint Security» (для Linux);
- ПО «Dr.Web Desktop Security Suite» (для Linux).

2.1.5 В зависимости от ОС, а также в случае выполнения одного из следующих условий:

- контролируемая зона медицинской организации определена по ограждающим конструкциям кабинетов (то есть если канал связи от АРМ до ПАК «ViPNet Coordinator HW» выходит за пределы контролируемой зоны);
- в точке подключения к сети провайдера телекоммуникационных услуг не установлен сертифицированный межсетевой экран (уровня сети),

на АРМ необходимо установить одно из следующих СКЗИ:

- ПО «ViPNet Client» (для Windows);
- ПО «ViPNet Client» (для Linux).

2.2 Дополнительные требования к составу АРМ, подлежащих аттестации по требованиям, предъявляемым к информационным системам класса защищенности К2.

2.2.1 На АРМ необходимо установить одно из следующих средств доверенной загрузки:

– ПАК «Соболь»;

– ПО «SafeBoot».

2.3 Типы подключаемых АРМ.

2.3.1 Выделяются следующие типы подключаемых АРМ в зависимости от классов защищенности, установленных ОС и СрЗИ, приведённые ниже (Таблица 1).

Таблица 1 – Типы подключаемых АРМ

Тип №	**Системное ПО**	**СрЗИ от НСД**	**Средство антивирусной защиты**	**СКЗИ[1]**	**МЭ**	**СОВ**	**Средство доверенной загрузки**
Класс защищенности К3							
1	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Kaspersky Endpoint Security» (для Windows)	ПО «ViPNet Client» (для Windows)	–	–	–
2	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Kaspersky Endpoint Security» (для Windows)	–	Модуль «Персональный МЭ» в составе ПО «Secret Net Studio»	–	–
3	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Dr.Web Desktop Security Suite» (для Windows)	ПО «ViPNet Client» (для Windows)	–	–	–
4	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Dr.Web Desktop Security Suite» (для Windows)	–	Модуль «Персональный МЭ» в составе ПО «Secret Net Studio»	–	–
5	ОС «Windows 10»	ПО «Secret Net Studio»	Модуль антивирусной защиты (технология Kaspersky)	ПО «ViPNet Client» (для Windows)	–	–	–

[1] Необходимо, при выполнении одного из условий:
1) контролируемая зона медицинской организации определена по ограждающим конструкциям кабинетов (то есть если канал связи от АРМ до ПАК «ViPNet Coordinator» выходит за пределы контролируемой зоны);
2) в точке подключения к сети провайдера телекоммуникационных услуг не установлен сертифицированный межсетевой экран (уровня сети).

			в составе ПО «Secret Net Studio»				
6	ОС «Windows 10»	ПО «Secret Net Studio»	Модуль антивирусной защиты (технология Kaspersky) в составе ПО «Secret Net Studio»	–	Модуль «Персональный МЭ» в составе ПО «Secret Net Studio»	–	–
7	ОС «Альт Линукс»	–	ПО «Kaspersky Endpoint Security» (для Linux)	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	–	–
8	ОС «Альт Линукс»	–	ПО «Kaspersky Endpoint Security» (для Linux)	–	МЭ в составе сертифицированной ОС	–	–
9	ОС «Альт Линукс»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	–	–
10	ОС «Альт Линукс»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	–	МЭ в составе сертифицированной ОС	–	–
11	ОС «Astra Linux Special Edition»	–	ПО «Kaspersky Endpoint Security» (для Linux)	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	–	–
12	ОС «Astra Linux Special Edition»	–	ПО «Kaspersky Endpoint Security» (для Linux)	–	МЭ в составе сертифицированной ОС	–	–
13	ОС «Astra Linux Special Edition»	–	ПО «Dr.Web Desktop Security Suite» (для	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	–	–

			Linux)				
14	ОС «Astra Linux Special Edition»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	–	МЭ в составе сертифицированной ОС	–	–
Класс защищенности К2							
15	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Kaspersky Endpoint Security» (для Windows)	ПО «ViPNet Client» (для Windows)	–	Модуль СОВ[1]	ПАК «Соболь»
16	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Kaspersky Endpoint Security» (для Windows)	ПО «ViPNet Client» (для Windows)	–	Модуль СОВ[7]	ПО «SafeBoot»
17	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Kaspersky Endpoint Security» (для Windows)	–	Модуль «Персональный МЭ» в составе ПО «Secret Net Studio»	Модуль СОВ[7]	ПАК «Соболь»
18	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Kaspersky Endpoint Security» (для Windows)	–	Модуль «Персональный МЭ» в составе ПО «Secret Net Studio»	Модуль СОВ[7]	ПО «SafeBoot»
19	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Dr.Web Desktop Security Suite» (для Windows)	ПО «ViPNet Client» (для Windows)	–	Модуль СОВ[7]	ПАК «Соболь»
20	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Dr.Web Desktop Security Suite» (для Windows)	ПО «ViPNet Client» (для Windows)	–	Модуль СОВ[7]	ПО «SafeBoot»

[1] Для АРМ класса защищенности К2 необходимо использовать систему обнаружения вторжений либо уровня сети, либо уровня узла в составе ПО «Secret Net Studio».

21	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Dr.Web Desktop Security Suite» (для Windows)	–	Модуль «Персональный МЭ» в составе ПО «Secret Net Studio»	Модуль СОВ[7]	ПАК «Соболь»
22	ОС «Windows 10»	ПО «Secret Net Studio»	ПО «Dr.Web Desktop Security Suite» (для Windows)	–	Модуль «Персональный МЭ» в составе ПО «Secret Net Studio»	Модуль СОВ[7]	ПО «SafeBoot»
23	ОС «Windows 10»	ПО «Secret Net Studio»	Модуль антивирусной защиты (технология Kaspersky) в составе ПО «Secret Net Studio»	ПО «ViPNet Client» (для Windows)	–	Модуль СОВ[7]	ПАК «Соболь»
24	ОС «Windows 10»	ПО «Secret Net Studio»	Модуль антивирусной защиты (технология Kaspersky) в составе ПО «Secret Net Studio»	ПО «ViPNet Client» (для Windows)	–	Модуль СОВ[7]	ПО «SafeBoot»
25	ОС «Windows 10»	ПО «Secret Net Studio»	Модуль антивирусной защиты (технология Kaspersky) в составе ПО «Secret Net Studio»	–	Модуль «Персональный МЭ» в составе ПО «Secret Net Studio»	Модуль СОВ[7]	ПАК «Соболь»
26	ОС «Windows 10»	ПО «Secret Net Studio»	Модуль антивирусной защиты (технология Kaspersky) в составе ПО «Secret Net Studio»	–	Модуль «Персональный МЭ» в составе ПО «Secret Net Studio»	Модуль СОВ[7]	ПО «SafeBoot»
27	ОС «Альт Линукс»	–	ПО «Kaspersky Endpoint Security»	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной	Модуль СОВ[7]	ПАК «Соболь»

			(для Linux)		ОС		
28	ОС «Альт Линукс»	–	ПО «Kaspersky Endpoint Security» (для Linux)	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПО «SafeBoot»
29	ОС «Альт Линукс»	–	ПО «Kaspersky Endpoint Security» (для Linux)	–	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПАК «Соболь»
30	ОС «Альт Линукс»	–	ПО «Kaspersky Endpoint Security» (для Linux)	–	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПО «SafeBoot»
31	ОС «Альт Линукс»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПАК «Соболь»
32	ОС «Альт Линукс»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПО «SafeBoot»
33	ОС «Альт Линукс»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	–	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПАК «Соболь»
34	ОС «Альт Линукс»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	–	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПО «SafeBoot»
35	ОС «Astra Linux Special Edition»	–	ПО «Kaspersky Endpoint Security» (для Linux)	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПАК «Соболь»
36	ОС «Astra Linux Special	–	ПО «Kaspersky Endpoint	ПО «ViPNet Client» (для	МЭ в составе сертифици	Модуль СОВ[7]	ПО «SafeBoot»

	Edition»		Security» (для Linux)	Linux)	рованной ОС		
37	ОС «Astra Linux Special Edition»	–	ПО «Kaspersky Endpoint Security» (для Linux)	–	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПАК «Соболь»
38	ОС «Astra Linux Special Edition»	–	ПО «Kaspersky Endpoint Security» (для Linux)	–	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПО «SafeBoot»
39	ОС «Astra Linux Special Edition»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПАК «Соболь»
40	ОС «Astra Linux Special Edition»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	ПО «ViPNet Client» (для Linux)	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПО «SafeBoot»
41	ОС «Astra Linux Special Edition»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	–	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПАК «Соболь»
42	ОС «Astra Linux Special Edition»	–	ПО «Dr.Web Desktop Security Suite» (для Linux)	–	МЭ в составе сертифицированной ОС	Модуль СОВ[7]	ПО «SafeBoot»

3 Требования к средствам защиты информации, применяемым на уровне вычислительной сети медицинской организации

3.1 Для защиты вычислительных сетей медицинских организаций должны быть установлены последние сертифицированные версии СрЗИ. По истечении сроков действия сертификатов соответствия ФСТЭК России / ФСБ России либо при выявлении уязвимостей в установленных версиях СрЗИ медицинские организация должны провести работы по обновлении версий данных СрЗИ.

3.2 АРМ, подключаемые к ГИС «РМИС» ОГБУЗ «МИАЦ», необходимо физически и (или) логически выделить в отдельный сегмент вычислительной сети медицинской организации (далее – защищаемый сегмент) и обеспечить защиту его периметра.

3.2.1 Для защиты периметра защищаемого сегмента необходимо использовать сертифицированное ФСТЭК России средство межсетевого экранирования (для класса защищенности К3 – не ниже 6 класса защиты, для класса защищенности К2 – не ниже 5 класса защиты).

3.2.2 Для обеспечения защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче в рамках ГИС «РМИС» по сетям провайдеров телекоммуникационных услуг необходимо применять технологию «ViPNet».

3.3 Требования по межсетевому экранированию защищаемого сегмента и по защите информации, передаваемой в рамках ГИС «РМИС» по сетям провайдеров телекоммуникационных услуг, могут быть выполнены путем установки на границе защищаемого сегмента средства межсетевого экранирования и СКЗИ ПАК «ViPNet Coordinator HW».

3.3.1 ПАК «ViPNet Coordinator HW», устанавливаемый на границе защищаемого сегмента, может относится к одной из следующих ViPNet-сетей:

- ViPNet-сеть ОГБУЗ «МИАЦ» (№ 1955);
- ViPNet-сеть ПАО «Ростелеком»;
- ViPNet-сеть Администрации КО;
- ViPNet-сеть медицинской организации.

3.4 При подключении к ГИС «РМИС» ОГБУЗ «МИАЦ» в отношении АРМ, подлежащих аттестации по требованиям, предъявляемым к информационным системам 2 класса защищенности, необходимо реализовать группу мер по обнаружению вторжений.

3.4.1 Для реализации данных мер защиты необходимо применять один из следующих вариантов систем обнаружения вторжений:

- модуль обнаружения и предотвращения вторжений в составе ПО «Secret Net Studio»;
- ПАК «ViPNet IDS».

4 Требования к параметрам и настройке средств защиты информации

4.1 Средства защиты информации должны быть установлены и настроены в соответствии с требованиями эксплуатационных документов на данные средства, а также с учетом требований проектного решения на построение системы защиты информации ГИС «РМИС» ОГБУЗ «МИАЦ».

4.2 ОГБУЗ «МИАЦ» предоставляет медицинской организации требования к параметрам и настройке устанавливаемых средств защиты информации. Медицинская организация в обязательном порядке выполняет указанные требования.

4.3 Медицинская организация по завершении установки и настройки средств защиты информации должна провести анализ защищенности АРМ, подключаемого к ГИС «РМИС» ОГБУЗ «МИАЦ», в ходе которого проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, правильность установки и настройки СрЗИ, технических средств и программного обеспечения, а также корректность СрЗИ информации при их взаимодействии с техническими средствами и программным обеспечением.

5 Требования по размещению АРМ и допуску к работе на АРМ

5.1 АРМ, подключенное к ГИС «РМИС» ОГБУЗ «МИАЦ», должно быть размещено в пределах контролируемой зоны в соответствии с ее границами, определенными организационно-распорядительными документами в медицинской организации, которой принадлежит это АРМ.

5.2 В медицинской организации должен быть определен порядок доступа в помещение с установленным АРМ, а также перечень лиц, имеющих право доступа в данное помещение.

5.3 В нерабочее время должна обеспечиваться охрана помещения с установленным АРМ.

5.4 При размещении средств отображения информации (мониторов) должна быть исключена возможность несанкционированного просмотра выводимой на них информации лицами, не имеющими права доступа к ней.

5.5 Допуск работников организации к работе на АРМ должен осуществляться в соответствии с должностными обязанностями работников или иными организационно-распорядительными документами, принятыми в медицинской организации.

5.6 В случае смены пользователя (либо изменения сведений о пользователе) АРМ непосредственный руководитель пользователя в течение 3 рабочих дней составляет заявку на изменение списка пользователей (по форме, приведенной в Приложении 3) и направляет ее в ОГБУЗ «МИАЦ» в форме официального письма на бумажном носителе или в электронном виде.

5.7 В случае принятия медицинской организацией решения об отключении АРМ от ГИС «РМИС» ОГБУЗ «МИАЦ» она составляет заявку на подключение (отключение) АРМ к ГИС «РМИС» ОГБУЗ «МИАЦ» (форма приведена в Приложении 2) и направляет ее в ОГБУЗ «МИАЦ» в форме официального письма на бумажном носителе или в электронном виде.