ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ КОСТРОМСКОЙ ОБЛАСТИ

ПРИКАЗ

от «25» 09 2023 года № 1040

г. Кострома

Об утверждении Регламента подключения медицинских информационных систем или автоматизированных рабочих мест медицинских организаций к Государственной информационной системе «Региональная медицинская информационная система Костромской области».

Во исполнение требований Федерального закона от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», приказа Минздрава России от 24 декабря 2018 г. №911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций», в целях включения медицинских организаций частной формы собственности, медицинских организаций, функции и полномочия учредителей в отношении которых осуществляют Правительство Российской Федерации или федеральные органы исполнительной власти, а так же медицинские организации, созданные определенными ведомствами или организациями для предоставления медицинской помощи своим работникам и их семьям, в единый цифровой контур здравоохранения,

ПРИКАЗЫВАЮ:

1. Утвердить Регламент подключения медицинских информационных систем и автоматизированных рабочих мест медицинских организаций к Государственной информационной системе «Региональная медицинская информационная система Костромской области» согласно приложению №1 к настоящему приказу.
2. Контроль за исполнением данного приказа оставляю за собой.
3. Настоящий приказ вступает в силу с момента его подписания.

Директор департамента Н.В.Гирин

Приложение №1
УТВЕРЖДЕНО
приказом департамента
здравоохранения
Костромской области
от «25» 09 2023 г.
№ 1070/

РЕГЛАМЕНТ
подключения медицинских информационных систем
или автоматизированных рабочих мест медицинских организаций
к Государственной информационной системе «Региональная медицинская информационная система Костромской области»

г. Кострома, 2023

1. Перечень используемых терминов и сокращений

В настоящем документе использованы следующие сокращения и термины с соответствующими определениями.

Медицинская организация	Организация Костромской области, которая подключила или планирует подключить медицинскую информационную систему или автоматизированное рабочее место к ГИС «РМИС»
ЕГИСЗ	Единая государственная информационная система здравоохранения
ГИС «РМИС»	Государственная информационная система «Региональная медицинская информационная система Костромской области»
МО	Медицинская организация частной формы собственности, медицинская организация, функции и полномочия учредителей, в отношении которых осуществляют Правительство РФ или федеральные органы исполнительной власти, а так же медицинские организации, созданные определенными ведомствами или организациями для предоставления медицинской помощи своим работникам и их семьям.
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ОГБУЗ «МИАЦ»	Областное государственное бюджетное учреждение здравоохранения «Медицинский информационно-аналитический центр Костромской области»
МИС	Медицинская информационная система
АРМ	Автоматизированное рабочее место
РЭМД	Реестр электронных медицинских документов
СЭМД	Структурированные электронные медицинские документы
ВСПД	Ведомственная сеть передачи данных, обеспечивающая защиту трафика в соответствии с требованиями регуляторов в сфере информационной безопасности
ПДн	Персональные данные

СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации

2. Введение

2.1. Настоящий Регламент подключения медицинских информационных систем и автоматизированных рабочих мест медицинских организаций к Государственной информационной системе «Региональная медицинская информационная система Костромской области» (далее – Регламент) определяет порядок подключения медицинских информационных систем и (или) автоматизированных рабочих мест медицинских организаций частной формы собственности, медицинских организаций, функции и полномочия учредителей, в отношении которых осуществляют Правительство Российской Федерации или федеральные органы исполнительной власти, а так же медицинские организации, созданные определенными ведомствами или организациями для предоставления медицинской помощи своим работникам и их семьям (далее – МИС (АРМ) МО) к ГИС «РМИС».

2.2. Основной целью принятия Регламента является определение условий, выполнение которых при подключении МИС (АРМ) МО к ГИС «РМИС» позволит обеспечить соблюдение установленных требований по обеспечению безопасности ПДн и иной информации, обрабатываемой в ГИС «РМИС».

2.3. Необходимость подключения МИС (АРМ) МО к ГИС «РМИС» обусловлена требованиями Минздрава России о предоставлении информации в подсистемы ЕГИСЗ.

3. Общие положения

3.1. Основанием для проведения комплекса мероприятий по подключению МИС (АРМ) МО к ГИС «РМИС» является заявка на подключение МИС (АРМ) МО к ГИС «РМИС» (форма приведена в Приложении №1 к Регламенту), подготовленная владельцем (оператором) подключаемой МИС (АРМ) МО и направленная в департамент здравоохранения Костромской области в форме официального письма за подписью руководителя организации.

3.2. Обязательным условием при подключении МИС (АРМ) МО к ГИС «РМИС» является наличие у подключаемой МИС (АРМ) МО аттестата соответствия требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах не ниже чем для 2 класса защищенности.

3.3. Работники отдела информационных технологий ОГБУЗ «МИАЦ» обеспечивают согласование заявки, полученной от департамента здравоохранения Костромской области, с директором ОГБУЗ «МИАЦ». В случае отказа в подключении к ГИС «РМИС» в адрес заявителя направляется соответствующее уведомление с указанием причин отказа.

3.4. На основании согласованной заявки работники отдела ИТ ОГБУЗ «МИАЦ» организуют совместную с владельцем (оператором) МИС (АРМ) МО работу по ее подключению к ГИС «РМИС».

3.5. Владелец (оператор) подключенной МИС (АРМ) МО должен своевременно проводить контроль за обеспечением уровня защищенности информации, содержащейся в этой МИС (АРМ) МО.

3.6. В случае, если владелец (оператор) подключенной МИС (АРМ) МО по результатам контроля за обеспечением уровня защищенности информации, содержащейся в этой МИС (АРМ) МО, принял решение о необходимости доработки (модернизации) ее системы защиты информации, то он уведомляет об этом ОГБУЗ «МИАЦ». Информационное взаимодействие ГИС «РМИС» с МИС (АРМ) МО прекращается до момента завершения доработки (модернизации) системы защиты информации, обрабатываемой в МИС (АРМ) МО.

4. Описание интеграционных профилей

4.1. Для отправки СЭМД из МИС МО в РЭМД ЕГИСЗ, МИС МО должна осуществлять формирование СЭМД в соответствии с форматами, размещенными на портале оперативного взаимодействия участников ЕГИСЗ (https://portal.egisz.rosminzdrav.ru/materials).

4.2. МИС МО должна иметь интеграционный сервис соответствующий федеральным форматам РЭМД ЕГИСЗ (https://portal.egisz.rosminzdrav.ru/materials/1879).

5. Описание построения взаимодействия и требования по подключению

5.1. Для организации подключения МИС (АРМ) МО к ГИС «РМИС», МО необходимо организовать защищенный канал передачи данных в соответствии с требованиями регуляторов в сфере защиты информации от МИС (АРМ) МО до ГИС «РМИС».

Организация защищенного канала связи может быть реализована:

– путем организации подключения (межсетевого взаимодействия) к защищенной сети передачи данных оператором которой является Государственное автономное учреждение «Агентство цифровых технологий Костромской области»;

– путем организации межсетевого взаимодействия с сетью ViPNet №1955 оператором которой является ОГБУЗ «МИАЦ».

Пропускная способность организуемого канала связи определяется МО в зависимости из потребностей информационного обмена.

МО самостоятельно определяет тип и характеристики производительности конечного оборудования.

5.2. МИС (АРМ) МО подключаемые к защищенной сети передачи данных ОГБУЗ «МИАЦ» должны соответствовать требованиям по информационной безопасности и иметь аттестат соответствия по требованиям приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» предъявляемым к информационным системам 2 класса защищенности, выданный организацией, имеющей лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

Без наличия данного аттестата ключевые документы на средства криптографической защиты информации не предоставляются и подключение не производится.

5.3. Для организации подключения к защищенной сети передачи данных МО подает заявку в ОГБУЗ «МИАЦ» к которой прилагается:

– заявка на подключение к защищенной сети передачи данных с указанием варианта подключения – через Государственное автономное учреждение «Агентство цифровых технологий Костромской области» либо ОГБУЗ «МИАЦ».

– заявка на предоставление ключевых документов на СКЗИ (при выборе в качестве подключения сеть Государственного автономного учреждение «Агентство цифровых технологий Костромской области» заявка дополнительно направляется в Государственное автономное учреждение «Агентство цифровых технологий Костромской области»);

– серийный и (или) учетный номера СКЗИ (при выборе в качестве подключения сеть Государственного автономного учреждение «Агентство цифровых технологий Костромской области» заявка дополнительно направляется в Государственное автономное учреждение «Агентство цифровых технологий Костромской области»);

– схема организации связи (при выборе в качестве подключения сеть Государственного автономного учреждение «Агентство цифровых технологий Костромской области» заявка дополнительно направляется в Государственное автономное учреждение «Агентство цифровых технологий Костромской области»);

– заверенную копию аттестата соответствия МИС (АРМ) МО по требованиям приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» предъявляемым к информационным системам 2 класса защищенности, выданный организацией, имеющей лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации;

– заверенную копию лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации организации, выдавшей аттестат соответствия требованиям информационной безопасности;

– заверенную копию лицензии на оказание медицинских услуг;

– заверенный руководителем список пользователей, которые будут назначены ответственными за работу в ГИС «РМИС»;

– заверенную руководителем копию или выписку из приказа о назначении ответственных лиц (ответственного за обеспечение безопасности ПДн, ответственного за организацию обработки ПДн, ответственного пользователя СКЗИ);

– заверенную руководителем копию или выписку из порядка доступа работников в защищаемые помещения;

– заверенную руководителем копию или выписку из журнала учета жестких магнитных носителей информации.

5.4. Настройка СКЗИ осуществляется силами МО в соответствии с эксплуатационной документацией на СКЗИ.

Оператор защищенной сети предоставляет МО ключевые документы.

МО самостоятельно или силами подрядной организации осуществляет ввод ключевых документов в программный или программно-аппаратный комплекс криптографической защиты информации.

О вводе ключевых документов в средство криптографической защиты информации МО в течение 7 рабочих дней сообщает в адрес организации выдавшей ключевые документы и направляет Акт об инсталляции средства криптографической защиты информации.

5.5. Оператор защищенной сети связи, при необходимости, осуществляет донастройку собственных СКЗИ и сообщает организации Заявителю о возможности осуществления информационного взаимодействия.

5.6. ОГБУЗ «МИАЦ», оставляет за собой право осуществления контроля за выполнением требований по информационной безопасности и приостановки взаимодействия в случае наличия нарушений (несоответствия требованиям) до полного их устранения.

5.7. Для организации подключения МИС (АРМ) МО к ГИС «РМИС», МО необходимо быть зарегистрированной в федеральном регистре медицинских организаций и выполнить следующее:

– в случае подключения МИС МО к ГИС «РМИС» необходимо провести интеграцию МИС МО и «РМИС ВИТАКОР»;

– в случае подключения АРМ МО к ГИС «РМИС» необходимо приобрести лицензию на право использования программного обеспечения «РМИС ВИТАКОР» у ЗАО Витакор;

– присоединится к договору поручения на обработку персональных данных с ОГБУЗ «МИАЦ»;

– заключить договор на сопровождение с ОГБУЗ «МИАЦ».

Нормативные правовые акты

1. Федеральный закон от 21.11.2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
2. Федеральный закон от 26.07.2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
3. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
4. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных»;
5. Федеральный закон от 27.12.2002 г. №184-ФЗ «О техническом регулировании»;
6. Указ Президента Российской Федерации от 05.12.2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
7. Указ Президента Российской Федерации от 17.03.2008 г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
8. Постановление Правительства Российской Федерации от 01.06.2021 г. №852 «О лицензировании медицинской деятельности (за исключением указанной деятельности, осуществляемой медицинскими организациями и другими организациями, входящими в частную систему здравоохранения, на территории инновационного центра «Сколково») и признании утратившими силу некоторых актов Правительства Российской Федерации»;
9. Постановление Правительства Российской Федерации от 09.02.2022 г. №140 «О единой государственной информационной системе в сфере здравоохранения»;
10. Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
11. Концепция информационной безопасности в сфере здравоохранения, утвержденная протоколом президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 19.03.2022 г. №7;
12. Приказ Минздрава России от 24.12.2018 г. №911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций»;

13. Приказ ФСТЭК России от 11.02.2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

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

15. Приказ ФСТЭК России от 21.12.2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

16. Приказ ФСТЭК России от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

17. Приказ ФСТЭК России от 29.04.2021 г. №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;

18. Приказ ФСБ России от 09.02.2005 г. №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

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

20. Приказ ФАПСИ от 13.06.2001 г. №152 «Об утверждении Инструкции 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».

Приложение №1
к Регламенту

ОБРАЗЕЦ

ЗАЯВКА
на подключение МИС (АРМ) МО
к ГИС «РМИС»

Наименование владельца и оператора подключаемой информационной системы (автоматизированного рабочего места):

_____

Физический адрес нахождения информационной системы (автоматизированного рабочего места)

_____

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

_____

_____

тел.:_____, эл. почта:_____

Название подключаемой информационной системы (автоматизированного рабочего места): _____

_____

Цель подключения:_____

_____

Аттестат соответствия подключаемой информационной системы (автоматизированного рабочего места):

_____
(номер, дата выдачи, наименование выдавшей организации)

_____ _____ _____
(должность руководителя организации) (подпись) (И.О. Фамилия)