ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ
КОСТРОМСКОЙ ОБЛАСТИ

ПРИКАЗ

№ 1442 от 05.11.2026

г. Кострома

О внесении изменений
в приказ департамента здравоохранения Костромской области №1070
от 25 сентября 2023 года «Об утверждении Регламента подключения
медицинских информационных систем и автоматизированных рабочих мест
медицинских организаций частной системы здравоохранения к Государственной
информационной системе «Региональная медицинская информационная система
Костромской области»

В связи с изменениями Федерального закона от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», принятием приказа ФСТЭК России от 11.04.2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» и приказа Федеральной службы безопасности Российской Федерации от 22.08.2026 № 321 "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных", в целях приведения в соответствие Регламента включения медицинских организаций частной системы здравоохранения в единый цифровой контур здравоохранения в соответствие с указанными требованиями,

ПРИКАЗЫВАЮ:

1. Изложить Приложение №1 приказа №1070 от 25 сентября 2023 года «Об утверждении Регламента подключения медицинских информационных систем и автоматизированных рабочих мест медицинских организаций частной

системы здравоохранения к Государственной информационной системе «Региональная медицинская информационная система Костромской области» в новой редакции согласно приложению к настоящему приказу.

2. Контроль за исполнением данного приказа оставляю за собой.

3. Настоящий приказ вступает в силу с даты его подписания.

Исполняющий обязанности
директора департамента А.Н. Мавренкова

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

[redacted]

Подписант: Мавренкова Анна Николаевна
Дата и время подписания: 05.11.2026 14.36
Должность: Первый заместитель директора департамента

Приложение

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

г. Кострома, 2026

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 к ГИС «РМИС»
ЕГИСЗ	Единая государственная информационная система здравоохранения
ГИС «РМИС»	Государственная информационная система «Региональная медицинская информационная система Костромской области»
МО ЧСЗ	Медицинская организация частной системы здравоохранения
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 частной системы здравоохранения 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 системы здравоохранения (далее – МИС (АРМ) МО ЧСЗ) к ГИС «РМИС».

2.2. Основной целью принятия Регламента является определение условий, выполнение которых при подключении МИС (АРМ) МО ЧСЗ 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 ЧСЗ к ГИС «РМИС» обусловлена требованиями Минздрава России о предоставлении информации в подсистемы ЕГИСЗ для медицинских организаций частной системы здравоохранения.

3. Общие положения

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

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

3.3. Работники отдела ИТ 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 ЧСЗ работу по ее подключению к ГИС «РМИС».

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

3.6. В случае, если владелец (оператор) подключенной МИС (АРМ) МО ЧСЗ по результатам контроля за обеспечением уровня защищенности информации, содержащейся в этой МИС (АРМ) МО ЧСЗ, 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 ЧСЗ прекращается до момента завершения доработки (модернизации) системы защиты информации, обрабатываемой в МИС (АРМ) МО ЧСЗ.

4. Описание интеграционных профилей

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

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

4.3. Информационное взаимодействие МО ЧСЗ с системами ОМС реализуется в соответствии с форматами передачи сведений и протоколами взаимодействия в сфере обязательного медицинского страхования (https://www.ffoms.gov.ru/documents/interaction/, https://portal.egisz.rosminzdrav.ru/materials).

5. Описание построения взаимодействия и требования по подключению

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

Организация защищенного канала связи реализуется путем подключения к защищенной сети передачи данных оператором которой является государственное автономное учреждение «Агентство цифровых технологий Костромской области» используя программное обеспечение или программно-аппаратный комплекс криптографической защиты;

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

МО ЧСЗ самостоятельно определяет тип и характеристики производительности оконечного оборудования.

5.2. МИС (АРМ) МО ЧСЗ подключаемые к защищенной сети передачи данных ОГБУЗ «МИАЦ» должны соответствовать требованиям по информационной безопасности и иметь аттестат соответствия по требованиям приказа ФСТЭК России от 11.04.2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» и приказа 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» предъявляемым к информационным системам не ниже 2 класса защищенности и 2 уровня защищенности, выданный организацией, имеющей лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

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

– заявка на подключение к защищенной сети передачи данных с указанием МАК-адреса и IP-адреса объекта информатизации;

– серийный и (или) учетный номера СКЗИ приобретенного по рекомендациям государственным автономным учреждением «Агентство цифровых технологий Костромской области»;

– акт установки и настройки СЗИ;

– заверенная копия аттестата соответствия МИС (АРМ) МО ЧСЗ по требованиям приказа ФСТЭК России от 11.04.2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» и приказа 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» предъявляемым к информационным системам не ниже 2 класса защищенности и 2 уровня защищенности, выданный организацией, имеющей лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации;

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

– заверенная копия лицензии на оказание медицинских услуг;

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

– заверенная руководителем копя или выписка из приказа о назначении ответственных лиц (ответственного за обеспечение безопасности ПДн, ответственного за организацию обработки ПДн, ответственного пользователя СКЗИ);

– заверенная руководителем копия или выписка из порядка доступа работников в защищаемые помещения;

– заверенная руководителем копия или выписка из журнала учета жестких магнитных носителей информации.

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

5.5. Оператор защищенной сети, 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 ЧСЗ к ГИС «РМИС», МО ЧСЗ необходимо быть зарегистрированной в федеральном регистре медицинских организаций и выполнить следующее:

– 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 «РМИС ВИТАКОР» 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 11.04.2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

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».

21. приказ Федеральной службы безопасности Российской Федерации от 22.08.2026 № 321 "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5-1 статьи 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации,

информационных технологиях и о защите информации" с использованием шифровальных (криптографических) средств"

Приложение №1
к Регламенту

ОБРАЗЕЦ

ЗАЯВКА
на подключение МИС (АРМ) МО ЧСЗ
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)