Согласовано

Заместитель министра здравоохранения

Ростовской области

_____Р.Р. Банацкий

«___» октября 2023 года

Утверждаю

И.о. начальника ГБУ РО «МИАЦ»

_____С.А. Жиляков

«4» октября 2023 года

Временный регламент

информационного взаимодействия с централизованными подсистемами государственной информационной системы в сфере здравоохранения Ростовской области

(версия № 03/2023)

г. Ростов-на-Дону

2023

Перечень сокращений

ГИСЗ РО	государственная информационная система в сфере здравоохранения Ростовской области
ИС	информационная или автоматизированная система Участника, взаимодействующая с централизованными подсистемами
Оператор	государственное бюджетное учреждение Ростовской области «Медицинский информационно-аналитический центр»
Регламент	временный регламент информационного взаимодействия с централизованными подсистемами государственной информационной системы в сфере здравоохранения Ростовской области
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
СЗИ	средство защиты информации
СКЗИ	средство криптографической защиты информации
Участник	министерство здравоохранения Ростовской области, подведомственные министерству здравоохранения Ростовской области организации
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЦП	централизованные подсистемы, входящие в состав ГИСЗ РО

1. Общие положения

Настоящий Регламент определяет порядок взаимодействия ЦП с информационными (автоматизированными) системами Участника, а также требования к их защите.

Централизованные подсистемы, перечень которых представлен в Приложении № 1 к Регламенту, включены в состав государственной информационной системы в сфере здравоохранения Ростовской области и введены в опытную эксплуатацию приказом министерства здравоохранения Ростовской области от 25.05.2022 № 932.

В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11.02.2013 № 17, актом определения класса защищенности ГИСЗ РО от 15.09.2022 данной информационной системе присвоен **1 класс защищенности (К1).**

В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, актом определения уровня защищенности персональных данных при их обработке в ГИСЗ РО от 12.04.2023 данной информационной системе установлен **2 уровень защищенности (2 УЗ).**

Для подключения к ЦП Участник должен выполнить требования по подключению к ЦП, описанные в настоящем Регламенте.

2. Требования к организации подключения

Организация подключения Участника к ЦП осуществляется в соответствии с требованиями:

нормативных правовых актов Российской Федерации в сфере защиты информации (в том числе персональных данных);

нормативных и методических документов уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения защиты информации (ФСТЭК России, ФСБ России, Роскомнадзор);

настоящего Регламента.

Подключение Участника к ЦП производится Оператором после выполнения двух обязательных мероприятий:

– предоставление доступа Участника к ЦП

– регистрация Участника в ЦП

Предоставление доступа Участника к ЦП выполняется после уведомления Оператора о выполнении технических требований с приложением подтверждающих документов (пункт 5.1 настоящего Регламента).

Регистрация Участника в ЦП осуществляется путем получения установленным порядком учетной записи (пункт 5.2 настоящего Регламента).

После выполнения указанных мероприятий Участник допускается к обработке информации в ЦП.

3. Требования к организационному обеспечению подключения к ЦП

Обеспечение защиты информации в ходе эксплуатации ИС Участника осуществляется в соответствии с организационно-распорядительной, эксплуатационной документацией на систему защиты информации ИС Участника и нормативными правовыми документами Российской Федерации в области защиты информации.

В рамках организации взаимодействия Участником должны быть выполнены следующие основные мероприятия:

– назначено должностное лицо (лица), ответственное за информационное взаимодействие с ЦП (в том числе за информационную безопасность этого взаимодействия), разработаны функциональные обязанности с персональной ответственностью каждого лица;

– заведены учеты:

используемых СКЗИ и СЗИ, ключевых документов, эксплутационной и технической документации к ним;

лиц, допущенных к работе с СКЗИ;

лиц, допущенных к работе с конфиденциальной информацией (в том числе с персональными данными);

съемных носителей информации, используемых для обработки конфиденциальной информации (в том числе персональных данных);

– разработаны локальные распорядительные документы в области защиты конфиденциальной информации (в том числе персональных данных) и криптографической защите информации;

– обеспечен контроль за исполнением законодательства, нормативных правовых актов и распорядительных документов по правилам работы с ИС Участника, по обеспечению информационной безопасности и защите конфиденциальной информации (в том числе персональных данных).

4. Требования к техническому обеспечению подключения к ЦП

Для организации защищённого информационного обмена Оператора и Участника необходимо обеспечивать криптографическую защиту каналов связи, проходящих через неконтролируемую зону, в том числе по открытым общедоступным сетям.

Оператор не несет ответственности за используемые Участником каналы связи (в том числе принадлежащие Участнику на правах собственности, аренды или любом другом законном основании). При отсутствии у Участника канала связи, подключение к ЦП не представляется возможным даже при выполнении всех требований Регламента.

Оператор для организации криптографической защиты каналов связи при взаимодействии информационных систем использует продуктовые линейки криптографического оборудования компаний ООО «Код безопасности» и ОАО «ИнфоТеКС». Все подключаемые к ЦП Участники должны использовать СКЗИ, совместимые с имеющимися у Оператора, (типа «Континент» или ViPNet).

Используемые Оператором СКЗИ имеют сертификат соответствия ФСБ России до уровня КС3 включительно. При подключении к ЦП, криптографическое оборудование Участника должно соответствовать уровню КС3.

Квалификация работников, обеспечивающих сопровождение и обеспечение защиты информации ИС Участника должна позволять устанавливать, настраивать, использовать и диагностировать (в рамках функциональных обязанностей) все используемые для целей Регламента СЗИ и СКЗИ, за исключением первичной установки, наладки, инсталляции,

монтажа и ввода в эксплуатацию СКЗИ (указанные мероприятия производит только лицензиат ФСБ России).

Установленные СКЗИ и СЗИ Участника должны иметь действующие сертификаты соответствия ФСТЭК и/или ФСБ России.

5. Порядок организации взаимодействия Участника с Оператором

5.1. Порядок предоставления доступа Участника к ЦП

Участник уведомляет Оператора о намерении подключиться к ЦП путем предоставления заявки (Приложение № 2 к Регламенту) установленным порядком.

К заявке прилагаются:

– заверенная (подписью руководителя и печатью) копия технического паспорта информационной системы, планируемой для подключения к централизованным подсистемам (актуализированного на дату обращения);

– документ, подтверждающий соответствие информационной системы Участника требованиям защиты информации (заверенная (подписью руководителя и печатью) копия заключения о соответствии или аттестата соответствия). При подготовке данных сведений необходимо учитывать требования, изложенные в п. 18.7 Приказа ФСТЭК России от 11.02.2013 № 17, в частности, представлять заверенную (подписью руководителя и печатью) копию документа, подтверждающего проведение периодического контроля за обеспечением уровня защищенности информации в системе согласно установленных временных показателей и присвоенных классов защищенности;

– сведения об инфраструктуре медицинской организации, используемой для информационного взаимодействия с ЦП (Приложение № 3 к Регламенту) с датой, подписью, расшифровкой подписи руководителя (профильного заместителя) и печатью Участника.

– файл конфигурации ресурсов организации и собственный сертификат защищенного соединения со шлюзом доступа в ЦОД, сгенерированный ответственным пользователем СКЗИ (администратором безопасности) в соответствии с мероприятиями, изложенными на стр. 66 RU.88338853.501430/022 90 3 «Руководства администратора Континент, Версия 3.9» (только при использовании аппаратуры Континент);

– фамилия, инициалы и контактный телефон ответственного за подключение ИС к ЦП.

На основании предоставленных документов Оператор в течение **семи рабочих дней** принимает решение о возможности подключения ИС Участника к ЦП и уведомляет Участника о принятом решении. В случае положительного решения, в течение **30 (тридцати) рабочих дней**, осуществляется подключения Участника к ЦП.

Если Оператору ЦП недостаточно информации, изложенной в предоставленных документах от Участника для оценки корректности сделанных в них выводов, он может запросить у Участника дополнительные документы или информацию, в том числе акты об установке и настройке СЗИ, СКЗИ, документов о праве собственности СЗИ, СКЗИ, а также информацию о лицензиатах, выпустивших аттестат соответствия (заключение о соответствии) информационной системы Участника.

Для контроля эффективности исполненных мер по защите информации в ИС Участника, Оператор оставляет за собой право осуществления выездной контрольной проверки, в части касающейся исполнения требований нормативных правовых актов Российской Федерации в области защиты информации.

5.2. Порядок регистрации Участника в ЦП

Для получения доступа к ЦП, Участник предоставляет сведения о работниках, ответственных за внедрение ЦП в организации, и заявку на получение доступа к ЦП Оператору установленным порядком.

Сведения об ответственных работниках предоставляются по установленной форме (Приложении № 4 к Регламенту).

Заявка предоставляется по установленной форме (Приложение № 5 к Регламенту) с датой, подписью, расшифровкой подписи руководителя (профильного заместителя) и печатью Участника.

Оператор в течении пяти рабочих дней со дня получения заявки регистрирует Участника и уведомляет его о выполнении заявки в ответном письме.

Если Участнику для работы с ЦП необходимо получение доступа к веб-интерфейсу ЦП, Участник предоставляет Оператору заявку на предоставление работникам Участника прав роли «Администратор ЦП».

Заявка предоставляется по установленной форме (Приложение № 6 к Регламенту) с датой, подписью, расшифровкой подписи руководителя (профильного заместителя) и печатью Участника.

Оператор в течении пяти рабочих дней со дня получения заявки регистрирует учетные записи «Администратор ЦП» и уведомляет Участника о выполнении заявки в ответном письме.

После получения ответа о готовности учетных записей, Участник направляет своего представителя к Оператору по адресу: 344029, г. Ростов-на-Дону, проспект Сельмаш, д. 14, каб. № 11. Время посещения согласовать по телефону: +7 (863) 200-18-33.

Представителю Участника, получающему Акт, содержащий сведения об учетных записях, необходимо при себе иметь следующие документы:

– документ, удостоверяющий личность;

– доверенность на действия от имени Участника, в свободной форме, с подписью руководителя и печатью Участника;

– подписанные оригиналы заявок (Приложения № 4, 5, 6, 7 к Регламенту).

Работники, получившие права роли «Администратор ЦП», самостоятельно регистрируют учетные записи для медицинских и иных работников Участника.

Для отзыва доступа учетной записи «Администратор ЦП» Участник предоставляет Оператору заявку на отключение доступа пользователя «Администратор ЦП» по форме, содержащей данные об учетных записях пользователей, доступ которых необходимо отключить.

Заявка предоставляется по установленной форме (Приложение № 7 к Регламенту) с датой, подписью, расшифровкой подписи руководителя (профильного заместителя) и печатью Участника.

Оператор в течении пяти рабочих дней со дня получения заявки блокирует учетные записи пользователей и уведомляем Участника о выполнении заявки в ответном письме..

6. Ответственность за нарушение требований

Ответственность за нарушение требований настоящего Регламента возлагается на Участника.

В случае выявления нарушений требований настоящего Регламента и других нарушений, способных повлиять на безопасность информации,

обрабатываемой в ЦП, Оператор **прекращает взаимодействие с Участником путем временного отключения Участника без его уведомления** (до устранения нарушений).

7. Перечень нормативных правовых актов, устанавливающих требования к обеспечению безопасности обработки информации

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
3. Руководящий документ. Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 01.10.2012 № 1119);
4. «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 10.03.2022 № 7;
5. Руководящий документ. Состав и содержание 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 (утверждены приказом ФСБ России от 10.07.2014 № 378);
6. Руководящий документ. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утвержден приказом ФСТЭК России от 11.02.2013 № 17);
7. Руководящий документ. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утвержден приказом ФСТЭК России от 18.02.2013 № 21).

8. Руководящий документ. «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» (утвержден приказом ФАПСИ от 13.07.2001 г. № 152).

8. Справочная информация

В случае наличия на затребованных документах (аттестат соответствия или заключение о соответствии) ограничительной пометки «Для служебного пользования» снятие копий, их учет, заверение и дальнейшую передачу в ГБУ РО «МИАЦ» осуществлять:

либо в соответствии с приказом Министра здравоохранения Российской Федерации от 14.07.2020 № 700н «Об упорядочении обращения с информацией ограниченного распространения», распоряжением губернатора Ростовской области от 09.06.2019 № 221 «Об утверждении инструкции о порядке обращения с информацией ограниченного распространения» и приказом министра здравоохранения Ростовской области от 09.04.2021 № 530 «Об утверждении инструкции по делопроизводству»;

либо после снятия установленным порядком ограничительной пометки «Для служебного пользования» (избыточно нанесенной на указанные документы) и дальнейшего обращения с ними как с обычными документами.

Заместитель директора
ГБУ РО «МИАЦ» В.С. Чистяков

Начальник отдела защиты информации
ГБУ РО «МИАЦ» А.В. Шарыгин

Начальник отдела развития цифрового здравоохранения
ГБУ РО «МИАЦ» А.В. Тарасдаров

Приложение № 1
к Регламенту

Перечень централизованных подсистем, входящих в состав государственной информационной системы в сфере здравоохранения Ростовской области

1. Централизованная подсистема «Управления потоками пациентов»
2. Централизованная подсистема «Региональная интегрированная электронная медицинская карта»
3. Централизованная подсистема «Центральный архив медицинских изображений»
4. Централизованная подсистема «Управление скорой и неотложной медицинской помощью»
5. Централизованная подсистема «Управление льготным лекарственным обеспечением»
6. Централизованная подсистем «Телемедицинские консультации»
7. Централизованная подсистема «Лабораторные исследования»
8. Централизованная подсистема «Организация оказания медицинской помощи больным онкологическими заболеваниями»
9. Централизованная подсистема «Организация оказания медицинской помощи больным сердечно-сосудистыми заболеваниями»
10. Централизованная подсистема «Организация оказания медицинской помощи по профилям «Акушерство и гинекология» и «Неонатология» (Мониторинг беременных)»

Приложение № 2
к Регламенту

Угловой штамп МО*

И.о начальника
ГБУ РО «МИАЦ»
С.А.Жилякову

Заявка на подключение к ЦП

Прошу зарегистрировать и подключить

_____*

(наименование учреждения)

к централизованной подсистеме (подсистемам)

_____*

(наименование централизованных подсистем)

государственной информационной системы здравоохранения в сфере Ростовской области.

К заявке прилагаю:

копию аттестата (заключения) о соответствии информационной системы требованиям защиты информации;

сведения об инфраструктуре медицинской организации, используемой для информационного взаимодействия с ЦП;

файл конфигурации и собственный сертификат защищенного соединения (только для АПКШ Континент, ЦУС);

контактные данные ответственного за подключение ИС к ЦП.

Руководитель МО* /_____*/

(Фамилия И.О.)

Внизу страницы ОБЯЗАТЕЛЬНО указать ответственное лицо заполнившее заявку с номером контактного телефона*

*- отмеченные поля ОБЯЗАТЕЛЬНЫ для заполнения.

Приложение 3
к Регламенту

Угловой штамп МО*

И.о. начальника
ГБУ РО «МИАЦ»
С.А.Жилякову

Сведения об инфраструктуре медицинской организации, используемой для информационного взаимодействия с ЦП

№ п/п	Фактический адрес	Тип корпуса (здания)	Тип СКЗИ	Модификация СКЗИ	Версия прошивки (исполнение аппаратной платформы)

Руководитель МО* /_____*/
(Фамилия И.О.)

Внизу страницы ОБЯЗАТЕЛЬНО указать ответственное лицо заполнившее заявку с номером контактного телефона*
*- *отмеченные поля ОБЯЗАТЕЛЬНЫ для заполнения.*

Приложение 4
к Регламенту

Угловой штамп МО*

И.о начальника
ГБУ РО «МИАЦ»
С.А.Жилякову

Контактные данные работников медицинской организации, ответственных за эксплуатацию в организации централизованных подсистем.

Наименование медицинской организации: _____

Специалист по организационным вопросам			
ФИО	Должность	Телефон	E-mail
Специалист по техническим вопросам			
ФИО	Должность	Телефон	E-mail

Руководитель МО* /_____*/
(Фамилия И.О.)

Внизу страницы ОБЯЗАТЕЛЬНО указать ответственное лицо заполнившее заявку с номером контактного телефона*
**- отмеченные поля ОБЯЗАТЕЛЬНЫ для заполнения.*

Приложение 5
к Регламенту

Угловой штамп МО*

И.о начальника
ГБУ РО «МИАЦ»
С.А.Жилякову

Заявка на предоставление доступа к продуктивной версии централизованной подсистемы, входящей в состав ГИСЗ РО

Прошу предоставить доступ к продуктивной версии централизованной подсистемы _____, входящей в состав государственной информационной системы в сфере здравоохранения Ростовской области.

Наименование медицинской организации	**OID МО из ФРМО**	**Наименование МИС МО**	**Наименование разработчика прикладного программного обеспечения МИС МО**

Руководитель МО* /_____*/
(Фамилия И.О.)

Внизу страницы ОБЯЗАТЕЛЬНО указать ответственное лицо заполнившее заявку с номером контактного телефона*
*- *отмеченные поля ОБЯЗАТЕЛЬНЫ для заполнения.*

Приложение 6
к Регламенту

Угловой штамп МО*

И.о начальника
ГБУ РО «МИАЦ»
С.А.Жилякову

Заявка на предоставление права роли «Администратор ЦП» в продуктивной версии централизованной подсистемы ГИСЗ РО

Прошу предоставить права роли «Администратор ЦП» в централизованную подсистему _____ следующим пользователям:
(наименование централизованной подсистемы)

ФИО (полностью)	**Должность**	**Контактный телефон**	**Адрес электронной почты (уникальный в пределах заявки)**	**OID МО из ФРМО**

Руководитель МО* /_____*/
(Фамилия И.О.)

Внизу страницы ОБЯЗАТЕЛЬНО указать ответственное лицо заполнившее заявку с номером контактного телефона*
**- отмеченные поля ОБЯЗАТЕЛЬНЫ для заполнения.*

Приложение 7
к Регламенту

Угловой штамп МО*

И.о начальника
ГБУ РО «МИАЦ»
С.А.Жилякову

Заявка на отзыв права роли «Администратор ЦП» в продуктивной версии централизованной подсистемы ГИСЗ РО

Прошу предоставить права роли «Администратор ЦП» в централизованную подсистему _____ следующим пользователям:
(наименование централизованной подсистемы)

ФИО (полностью)	**Должность**	**Контактный телефон**	**Адрес электронной почты (уникальный в пределах заявки)**	**OID МО из ФРМО**

Руководитель МО* /_____*/
(Фамилия И.О.)

Внизу страницы ОБЯЗАТЕЛЬНО указать ответственное лицо заполнившее заявку с номером контактного телефона*
**- отмеченные поля ОБЯЗАТЕЛЬНЫ для заполнения.*