УТВЕРЖДЕН
приказом ГБУЗ «ЧОМИАЦ»
от 22.08.2025 № 62

Регламент работы Ключевого центра государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр»

I. Общие положения

1.1. Настоящий Регламент работы Ключевого центра государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр» (далее соответственно – Регламент, ГБУЗ «ЧОМИАЦ») определяет порядок изготовления, выдачи, и использования дистрибутивов ключевой и справочной информации для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области (далее соответственно – дистрибутив ключей, защищенная сеть).

1.2. Ключевой центр ГБУЗ «ЧОМИАЦ» – центр в области изготовления, выдачи и использования дистрибутивов ключей для обеспечения подключения к защищенной сети, функционирующий в соответствии с положениями настоящего Регламента.

1.3. Защищенная сеть функционирует на базе продуктов ViPNet и имеет номер 1464.

1.4. Структурным подразделением ГБУЗ «ЧОМИАЦ», обеспечивающим работу Ключевого центра и выполняющим функции администратора защищенной сети, является отдел защиты информации.

1.5. Настоящий Регламент является договором присоединения в порядке статьи 428 Гражданского кодекса Российской Федерации. Организация, обратившаяся в Ключевой центр или имеющая подключение к защищенной сети, считается присоединившейся к настоящему Регламенту (далее – Организация). Факт присоединения к Регламенту является полным принятием условий настоящего Регламента и всех приложений к нему. Регламент публикуется на сайте miac74.ru.

1.6. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится ГБУЗ «ЧОМИАЦ» в одностороннем порядке. Уведомление Организаций о внесении изменений (дополнений) в Регламент осуществляется путем помещения новой редакции Регламента на сайт miac74.ru.

1.7. Формы документов для совершения действий, предусмотренных настоящим Регламентом, в доступном для редактирования формате помещены на сайт miac74.ru в разделе «Проекты» / «Ведомственная сеть передачи данных».

1.8. Документы для совершения действий, предусмотренных настоящим Регламентом, должны соответствовать следующим требованиям:

1) текст документов должен быть легко читаемым;

2) документы не должны иметь подчисток или приписок, зачеркнутых слов либо иных неоговоренных исправлений;

3) документы не должны быть исполнены карандашом или с помощью легко удаляемых с бумажного носителя красителей;

4) документы не должны иметь повреждения, которые не позволяют однозначно истолковать их содержание.

1.9. Подключение Организации к защищенной сети возможно только после получения Организацией разрешения от администратора защищенной сети.

1.10. Выданные Ключевым центром дистрибутивы ключей предназначены исключительно для средств криптографической защиты информации ViPNet, сертифицированным ФСБ России и используемым для подключения к защищенной сети (далее – СКЗИ).

1.11. Сведения о Ключевом центре.

Адрес:	г. Челябинск, ул. Кузнецова, д. 2А, к. 8, каб. 209
Часы работы:	понедельник-пятница с 8:00 до 16:30, перерыв с 12:00 до 12:30
Телефон:	+7 351 240-12-12 (доб. 2)
E-mail:	itsecurity@miac74.ru
Сайт:	miac74.ru

II. Права и обязанности сторон

2.1. Организация обязана:

1) приказом назначить ответственного за организацию подключения к защищенной сети (далее – администратор безопасности) из числа работников Организации, имеющего необходимый уровень квалификации для обеспечения защиты информации с использованием СКЗИ;

2) при расторжении с администратором безопасности трудового договора (или переводе его на другую должность) издать новый приказ о назначении администратора безопасности из числа работников Организации;

3) выполнять требования настоящего Регламента и 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, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 (далее – Инструкция ФАПСИ);

4) уведомлять Ключевой центр об изменении своих реквизитов в течение одного рабочего дня с даты их изменения.

2.2. Администратор безопасности обязан:

1) допускать пользователей к работе с СКЗИ только после их ознакомления с Инструкцией ФАПСИ и обучением правилам работы с СКЗИ, предусмотренным документацией к используемым СКЗИ;

2) выполнять требования настоящего Регламента, Инструкции ФАПСИ, документации к используемым СКЗИ и контролировать выполнение этих требований пользователями СКЗИ;

3) уведомлять Ключевой центр об изменении адресов установки СКЗИ в течение одного рабочего дня с даты их изменения;

4) немедленно уведомлять Ключевой центр о прекращении использования пользователем СКЗИ подключения к защищенной сети или прекращении допуска пользователя к работе с СКЗИ;

5) отключать сетевые узлы ViPNet в соответствии с пунктом 5.1 настоящего Регламента в течение 10 рабочих дней с даты прекращения использования пользователем СКЗИ подключения к защищенной сети или прекращения допуска пользователя к работе с СКЗИ;

6) немедленно уведомлять Ключевой центр о компрометации ключей сетевых узлов ViPNet.

2.3. Представитель администратора безопасности обязан:

1) обеспечивать соблюдение мер, исключающих доступ посторонних лиц к дистрибутивам ключей и СКЗИ, их несанкционированное копирование, а также непреднамеренные утрату или уничтожение при доставке дистрибутивов ключей и СКЗИ администратору безопасности;

2) немедленно сообщать администратору безопасности о фактах утраты дистрибутивов ключей и СКЗИ при их доставке администратору безопасности;

3) передавать полученные в Ключевом центре дистрибутивы ключей и СКЗИ лично администратору безопасности.

2.4. Ключевой центр имеет право:

1) отключать сетевые узлы ViPNet или ограничивать им доступ к защищенной сети в случае нарушения Организацией, администратором

безопасности (или его представителем), пользователем СКЗИ требований настоящего Регламента, а также при отсутствии активности сетевых узлов в течении 180 календарных дней с даты последней зарегистрированной активности или даты выдачи дистрибутива ключей;

2) запрашивать у Организации копии лицензий на право использования продуктов ViPNet или иных документов, подтверждающих право использования продуктов ViPNet;

3) запрашивать у Организации сведения и документы, подтверждающие наличие у администратора безопасности необходимого уровня квалификации для обеспечения защиты информации с использованием СКЗИ;

4) запрашивать у Организации сведения и документы, подтверждающие выполнение требований настоящего Регламента, Инструкции ФАПСИ, документации к используемым СКЗИ при использовании подключения к защищенной сети.

2.5. Ключевой центр обязан по запросу Организации предоставить мотивированный отказ в случае принятия Ключевым центром решения об отказе в совершении действий, предусмотренных настоящим Регламентом, в течение трех рабочих дней с даты получения такого запроса.

III. Порядок приема в Ключевом центре

3.1. Под приемом в Ключевом центре в настоящем Регламенте понимается посещение администратором безопасности (или его представителем) Ключевого центра для осуществления действий, предусмотренных настоящим Регламентом.

3.2. Прием в Ключевом центре осуществляется по предварительной записи по номеру телефона + 7 351 240-12-12 (доб. 2).

3.3. Если на прием в Ключевой центр прибудет представитель администратора безопасности, то он должен представить доверенность, подтверждающую его полномочия (Приложение 1).

3.4. При первичном приеме в Ключевом центре администратор безопасности (или его представитель) должен предоставить:

1) согласие на обработку персональных данных:

а) при личном обращении администратора безопасности – Приложение 2;

б) при обращении представителя администратора безопасности – Приложение 3;

2) заверенную установленным образом копию приказа о назначении администратора безопасности (Приложение 4). Отметка о заверении копии приказа проставляется под реквизитом «подпись» и должна содержать:

а) слова «Копия верна»;

б) должность лица, заверившего копию;

в) собственноручную подпись лица, заверившего копию;

г) инициалы и фамилию лица, заверившего копию;

д) дату заверения копии не старше 30 календарных дней;

е) печать организации или кадрового подразделения;

3) копию второй и третьей страниц паспорта гражданина Российской Федерации администратора безопасности, заверенную им. Отметка о заверении копии паспорта должна содержать:

а) слова «Копия верна»;

б) собственноручную подпись администратора безопасности;

в) инициалы и фамилию администратора безопасности;

г) дату заверения копии не старше 30 календарных дней.

3.5. При каждом приеме в Ключевом центре администратор безопасности (или его представитель) представляет оригинал своего паспорта гражданина Российской Федерации.

3.6. Администратор безопасности в случае перевода его на другую должность перед совершением действий, предусмотренных настоящим Регламентом, должен предоставить в Ключевой центр новую копию приказа с актуальной должностью согласно подпункту 2 пункта 3.4 настоящего Регламента.

IV. Получение дистрибутива ключей

4.1. Для получения дистрибутива ключей на приеме в Ключевом центре администратор безопасности (или его представитель) предоставляет заявление на получение дистрибутива ключей (Приложение 5).

4.2. Заявление на получение дистрибутива ключей действительно в течение 30 календарных дней с момента его подписания руководителем Организации.

4.3. Решение о выдаче дистрибутива ключей или об отказе в выдаче дистрибутива ключей принимается Ключевым центром после проверки предоставленных для получения дистрибутива ключей документов.

4.4. В случае принятия решения о выдаче дистрибутива ключей Ключевой центр изготавливает дистрибутив ключей и выдает его на оптическом диске администратору безопасности или его представителю в течение одного рабочего дня.

4.5. При выдаче дистрибутива ключей Ключевой центр обеспечивает подписание получателем дистрибутива ключей необходимых учетных документов.

4.6. Носители с дистрибутивами ключей учитываются и хранятся в соответствии с требованиями Инструкции ФАПСИ и документацией к используемым СКЗИ. Хранение дистрибутивов ключей на неучтенных носителях и передача дистрибутивов ключей по незащищенным каналам связи недопустимы.

V. Отключение сетевого узла ViPNet

5.1. Для отключения сетевого узла ViPNet от защищенной сети на приеме в Ключевом центре администратор безопасности (или его представитель) предоставляет заявление о прекращении использования подключения к защищенной сети (Приложение 6).

5.2. Решение об отключении сетевого узла ViPNet или об отказе в отключении сетевого узла ViPNet принимается Ключевым центром после проверки предоставленных для отключения сетевого узла ViPNet документов в течение одного рабочего дня с момента их предоставления.

5.3. В случае принятия решения об отключении сетевого узла ViPNet от защищенной сети Ключевой центр в течение одного рабочего дня осуществляет отключение.

VI. Уведомление о компрометации ключей

6.1. Для уведомления о компрометации ключей сетевых узлов ViPNet необходимо направить на электронную почту Ключевого центра скан-копию заявления о компрометации ключей (Приложение 7).

6.2. Решение о проведении мероприятий при компрометации ключей принимается Ключевым центром после проверки достоверности сведений в предоставленном заявлении о компрометации ключей в течение одного рабочего часа с момента предоставления заявления.

6.3. В случае принятия решения о проведении мероприятий при компрометации ключей Ключевой центр немедленно проводит соответствующие мероприятия.