Министерство здравоохранения Омской области
Бюджетное учреждение здравоохранения Омской области
«КЛИНИЧЕСКИЙ ДИАГНОСТИЧЕСКИЙ ЦЕНТР»
(БУЗОО «КДЦ»)

ПРИКАЗ

30 ноября 2022 г. № 257

г. Омск

О назначении лиц, ответственных
за обеспечение информационной безопасности

В целях обеспечения информационной безопасности в БУЗОО «КДЦ», а также распределения ответственности и выполнения требований Федеральных законов, нормативно-правовых и нормативно-методических актов в области защиты информации,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки защищаемой информации (далее – защищаемая информация) в БУЗОО «КДЦ» заместителя главного врача по ОМР.
2. Возложить на заместителя главного врача по ОМР следующие обязанности:
   - контроль оформления (ведения) и своевременного уточнения списка лиц, доступ которых к защищаемой информации, обрабатываемой в БУЗОО «КДЦ», необходим для выполнения служебных обязанностей, а также списка лиц, имеющих право бесконтрольного пребывания в помещениях, в которых производится обработка защищаемой информации;
   - контроль выполнения сотрудниками, допущенными к обработке защищаемой информации, предъявляемых требований к безопасности информации;
   - контроль эффективности принимаемых организационных мер по обеспечению безопасности защищаемой информации в соответствии с утвержденными документами, определяющими требования к организации обработки защищаемой информации;
   - выявление фактов несоблюдения условий обработки защищаемой информации, использования нерегламентированных программных и технических средств, способных привести к нарушению конфиденциальности обрабатываемых данных, а также иных нарушений, приводящих к снижению уровня защищенности;
   - контроль доведения до сведения сотрудников, допущенных к обработке защищаемой информации, положений законодательства Российской Федерации о защите информации, локальных актов по вопросам обработки защищаемой информации;
   - контроль организации приема, обработки и учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных, осуществление контроля за обработкой таких обращений.
3. Утвердить и ввести в действие Инструкцию ответственного за организацию обработки защищаемой информации (Приложение 1 к данному Приказу).
4. Назначить администратором информационной безопасности (далее – администратор безопасности) начальника отдела АСУ.
5. Возложить на начальника отдела АСУ следующие обязанности:

– организация эксплуатации и контроля работоспособности технических и программных средств ИС, в которых обрабатывается защищаемая информация, в том числе средств и систем защиты информации в соответствии с установленными организационно-техническими требованиями по защите информации и эксплуатационными документами;

– контроль обслуживания и ремонта технических средств ИС, в которых обрабатывается защищаемая информация;

– контроль за осуществлением резервного копирования (восстановления) баз данных и документов, содержащих обрабатываемую защищаемую информацию;

– контроль за работой пользователей ИС, своевременное выявление и регистрация попыток несанкционированного доступа к защищаемой информации;

– обучение лиц, использующих средства защиты информации, применяемые в ИС, правилам работы с ними.

6. Утвердить и ввести в действие Инструкцию администратора информационной безопасности (Приложение 2 к данному Приказу).

7. Создать Комиссию по вопросам информационной безопасности БУЗОО «КДЦ» (Приложение 3 к данному Приказу).

8. Утвердить и ввести в действие Положение о Комиссии по вопросам информационной безопасности БУЗОО «КДЦ» (Приложение 4 к данному Приказу).

9. Комиссии по вопросам информационной безопасности, в срок до_____ 202__ года, провести работы по выявлению информационных систем БУЗОО «КДЦ» и определению класса защищенности выявленных информационных систем и уровня защищенности обрабатываемых в них персональных данных.

10. Создать Комиссию по вопросам обеспечения безопасности критической информационной инфраструктуры БУЗОО «КДЦ» (Приложение 5 к данному Приказу).

11. Утвердить и ввести в действие Положение о Комиссии по вопросам обеспечения безопасности критической информационной инфраструктуры БУЗОО «КДЦ» (Приложение 6 к данному Приказу).

12.Назначить ответственным за обеспечение безопасности критической информационной инфраструктуры БУЗОО «КДЦ» заместителя главного врача по организационно-методической работе.

13.Утвердить и ввести в действие Инструкцию ответственного за обеспечение безопасности критической информационной инфраструктуры БУЗОО «КДЦ» (Приложение 7 к данному Приказу).

14.Признать утратившими силу приказ от 06.06.2018г. №29 «О создании комиссии по категорированию объектов критической информационной инфраструктуры в БУЗОО «КДЦ». п.п.1-8 приказа № 37 от 17.04.20119г. «О внесении изменений в приказ №23 от 10.04.2017г. « Об организации работы с персональными данными».

15.Ведущему документоведу ознакомить всех заинтересованных должностных лиц под роспись в трехдневный срок с момента регистрации.

16.Контроль за исполнением настоящего Приказа оставляю за собой.

Главный врач Н.И. Орлова

Исп. Бодрова Т.В.
2-17

ПРИЛОЖЕНИЕ 1
к Приказу
от 30.11.2022 г. № 257

ИНСТРУКЦИЯ
ответственного за организацию обработки защищаемой информации

Обозначения и сокращения по тексту

БУЗОО «КДЦ», Оператор	–	Бюджетное учреждение здравоохранения Омской области «Клинический диагностический центр»;
Ответственный (ответственное лицо)	–	Должностное лицо, ответственное за организацию обработки защищаемой информации;
Администратор безопасности	–	Администратор информационной безопасности
Защищаемая информация	–	Информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну (в т.ч. персональные данные);
ИС	–	Информационные системы БУЗОО «КДЦ»;
НСД	–	несанкционированный доступ;
ПО	–	программное обеспечение;
СКЗИ	–	средство криптографической защиты информации;

1. Общие положения

1.1. В настоящем документе определяются права, обязанности, а также ответственность должностного лица, ответственного за организацию обработки защищаемой информации в БУЗОО «КДЦ».

1.2. Лицо, ответственное за организацию обработки защищаемой информации (далее – Ответственный; ответственное лицо) – должностное лицо, отвечающее за организацию обработки защищаемой информации с использованием средств автоматизации и без использования таких средств, а также осуществляющее контроль доступа к защищаемой информации.

1.3. Ответственный назначается на должность из числа штатных сотрудников БУЗОО «КДЦ» приказом руководителя БУЗОО «КДЦ», и подотчетен ему.

1.4. Лицо, ответственное за организацию обработки персональных данных в своей работе должен руководствоваться настоящей инструкцией и следующими основными законодательными и нормативными правовыми актами Российской Федерации:

- Трудовой кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- локальные акты БУЗОО «КДЦ» в области защиты информации.

2. Должностные обязанности

2.1. В соответствии с ч. 4 ст. 22.1 Федерального закона № 152-ФЗ, Ответственный обязан:

– осуществлять внутренний контроль соблюдения сотрудниками организации Законодательства Российской Федерации о защите информации, контроль выполнения сотрудниками, допущенными к обработке защищаемой информации, предъявляемых требований к безопасности информации.

– доводить до сведения сотрудников БУЗОО «КДЦ» положения законодательства по защите информации, локальных актов по вопросам информационной безопасности, требований к защите данных.

– выявлять факты несоблюдения условий обработки защищаемой информации, использования нерегламентированных программных и технических средств, способных привести к нарушению конфиденциальности обрабатываемых данных, а также иных нарушений, приводящих к снижению уровня защищенности.

– контролировать процесс разработки и поддержания в актуальном состоянии списка лиц, допущенных к обработке защищаемой информации, эффективность принимаемых организационных мер по обеспечению безопасности защищаемой информации в соответствии с утвержденными документами, определяющими требования к организации обработки защищаемой информации.

– организовывать прием и отработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.2. На ответственное лицо возлагается задача по организации выполнения требований законодательства при обработке персональных данных.

2.3. Требования ответственного лица, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми сотрудниками БУЗОО «КДЦ».

3. Должностные права

3.1. Ответственное лицо имеет право:

– запрашивать у сотрудников организации информацию, необходимую для реализации своих полномочий.

– требовать от сотрудников организации, являющихся пользователями информационных систем, выполнения установленной технологии обработки защищаемой информации, инструкций и других локальных актов по обеспечению безопасности защищаемой информации.

– участвовать в разработке мероприятий по совершенствованию безопасности защищаемой информации.

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности.

– принимать меры по приостановлению или прекращению обработки защищаемой информации, осуществляемой с нарушением требований законодательства Российской Федерации.

– вносить руководителю БУЗОО «КДЦ» предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки защищаемой информации или нарушения режима конфиденциальности.

– вносить руководителю БУЗОО «КДЦ» предложения о совершенствовании правового, технического и организационного регулирования обеспечения защиты

информации.

4. Ответственность

4.1. Ответственное лицо несет персональную ответственность за качество проводимых им работ, связанных с выполнением им своих должностных обязанностей.

4.2. За нарушение настоящей Инструкции Ответственное лицо может быть привлечено к дисциплинарной или иной предусмотренной законодательством ответственности.

5. Прием обращений субъектов персональных данных

5.1. Ответственное лицо обязано организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей в журнале учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных и осуществлять контроль приема и обработку таких обращений и запросов.

5.2. Запрос может содержать:

- номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словестное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором;
- подпись субъекта ПДн или его законного представителя.

5.3. В случае отсутствия в запросе, по крайней мере, одного пункта из п. 3.2, прием обращения производится по усмотрению ответственного лица.

ЛИСТ ОЗНАКОМЛЕНИЯ

с инструкцией ответственного за организацию обработки защищаемой информации

№	Фамилия И.О.	Должность, структурное подразделение	Подпись, дата

ПРИЛОЖЕНИЕ 2
к Приказу
от 30.11.2022 г. № 257

ИНСТРУКЦИЯ
администратора информационной безопасности

Обозначения и сокращения по тексту

БУЗОО «КДЦ», Оператор	–	Бюджетное учреждение здравоохранения Омской области «Клинический диагностический центр»;
Ответственный (ответственное лицо)	–	Должностное лицо, ответственное за организацию обработки защищаемой информации;
Администратор безопасности	–	Администратор информационной безопасности
АРМ	–	автоматизированное рабочее место;
Защищаемая информация	–	Информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну (в т.ч. персональные данные);
ИС	–	Информационные системы БУЗОО «КДЦ»;
МЭ	–	межсетевой экран;
НСД	–	несанкционированный доступ;
ПО	–	программное обеспечение;
СЗИ	–	средства защиты информации;
СКЗИ	–	средство криптографической защиты информации;

1. Общие положения

1.1. Настоящая инструкция определяет права и обязанности должностного лица, ответственного за обеспечение информационной безопасности, обрабатываемых в информационных системах (далее – администратора безопасности), и содержит перечень административных задач, описание правил и процессов обслуживания технических и программно-технических средств ИС БУЗОО «КДЦ».

1.2. Администратор безопасности назначается приказом руководителя БУЗОО «КДЦ» и отвечает за обеспечение безопасности защищаемой информации при ее обработке в ИС БУЗОО «КДЦ»;

1.3. Администратор безопасности по вопросам обеспечения безопасности защищаемой информации подчиняется непосредственно руководителю БУЗОО «КДЦ»;

1.4. Назначенных администраторов безопасности должно быть **не менее двух**.

1.5. Администратор безопасности отвечает за поддержание установленного уровня защищенности информации;

1.6. Администратор безопасности осуществляет методическое руководство деятельности пользователей ИС, допущенных к обработке защищаемой информации;

1.7. Требования администратора безопасности, связанные с выполнением им своих

обязанностей, обязательны для исполнения всеми пользователями ИС;

1.8. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИС, состояния и поддержания установленного уровня защищенности информации, обрабатываемой в ИС;

1.9. Настоящая инструкция не исключает обязательного выполнения требований других действующих нормативных документов по вопросам обеспечения защиты информации.

1.10. Администратор безопасности обеспечивает нормальное функционирование защитных механизмов ИС;

1.11. Квалификация администратора безопасности должна позволять решать возложенные на него задачи по администрированию средств защиты информации ИС.

1.12. В случае болезни, отпуска и иных причин длительного отсутствия, администратор безопасности передает свои обязанности замещающему его лицу.

2. Уровень подготовки администратора

2.1. Администратор безопасности должен знать:

- законодательные и нормативные правовые акты, методические и нормативные материалы по вопросам, связанным с обеспечением информационной безопасности и локальные нормативные и методические акты по защите информации;
- структуру ИС БУЗОО «КДЦ», категории защищаемой информации, категории субъектов доступа и объектов доступа;
- порядок использования и технологический процесс, обработки и хранения защищаемой информации;
- методы и средства защиты и контроля защищаемой информации, способы выявления каналов утечки информации, способы организации противодействия угрозам информационной безопасности;
- принципы функционирования, методику обслуживания и устранения неисправностей программно-технических средств ИС;
- принципы работы регистрации (журналирования) событий ОС и СЗИ;
- основы сетевого администрирования;
- основы администрирования используемых в ИС, операционных систем, средств защиты информации и программного обеспечения;
- основные технологии реализации компьютерных атак;
- принцип работы с базами уязвимостей (БДУ ФСТЭК России, CWE и др.);
- правила и нормы охраны труда.

3. Задачи, права и обязанности администратора безопасности

3.1. Администратор безопасности отвечает за согласование настроек программно-технических и программных средств защиты информации, а также контроль действий привилегированных пользователей (администраторов ИС), и **решает следующие задачи**:

- поддержание необходимого уровня защищенности ИС и обрабатываемой в ИС защищаемой информации;
- осуществление методического руководства деятельности пользователей ИС, допущенных к обработке защищаемой информации;
- определение и подтверждение необходимости и достаточности принимаемых мер по защите информации в ИС;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по

каналам связи защищаемой информации;

– проведение совещательных мероприятий и инструктажей, направленных на повышение уровня знаний пользователей ИС и администраторов ИС в области информационной безопасности;

– организация установки, настройки и контроля выполнения правил эксплуатации и функционирования средств защиты информации ИС;

– сопровождение средств защиты информации (СЗИ) и основных технических средств и систем (ОТСС) ИС;

– обеспечение штатного функционирования защитных механизмов ИС и периодическое обновление СЗИ ИС;

– оперативное реагирование на нарушения требований по информационной безопасности (ИБ) в ИС и участие в их прекращении;

– осуществление внутреннего контроля соблюдения сотрудниками организации Законодательства Российской Федерации о защите информации;

– осуществление контроля использования машинных носителей информации (включая съёмные МНИ);

– осуществление анализа журналов регистрации событий, создание их архивных копий и обеспечение надёжного хранения этих копий. При обнаружении предпосылок и фактов несанкционированного доступа к защищаемым ресурсам ИС администратор безопасности принимает необходимые меры;

– проведение периодического контроля работоспособности, параметров настройки и правильности функционирования ПО и средств защиты информации ИС (не реже чем раз в 90 дней);

– осуществление контроля поддержания в актуальном состоянии перечня учётных записей пользователей ИС и назначенных им привилегий;

– осуществление контроля за созданием, присвоением и уничтожением идентификаторов субъектов доступа и устройств ИС;

– осуществление контроля за соблюдением парольных политик пользователями ИС;

– осуществление контроля защищенности аппаратных средств ИС;

– осуществление контроля за сроками действия сертификатов соответствия требованиям по безопасности информации на средства защиты информации, используемые в составе системы защиты информации ИС;

– разработка планов проведения мероприятий по анализу защищённости ИС;

– произведение анализа программных и технических средств на наличие уязвимостей с использованием общедоступных источников и данных производителя, а также инструментальных средств анализа защищенности;

– организация мероприятий по устранению обнаруженных в результате анализа уязвимостей;

– организация проведения периодического контроля принятых мер по защите информации;

– осуществление своевременной корректировки разрешительной системы доступа (изменение списка пользователей, изменение прав доступа пользователей ИС);

– осуществление прекращения обработки защищаемой информации, как в целом, так и от отдельных пользователей ИС, в случае выявления нарушений установленного порядка работ или нарушения функционирования средств защиты информации и ИС.

3.2. В рамках выполнения основных задач администратор безопасности **осуществляет**:

– текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;

– текущий контроль технологического процесса автоматизированной обработки защищаемой информации;

– участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности защищаемой информации;

– управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС;

– управление СЗИ в ИС, в том числе параметрами настройки программного обеспечения (ПО), включая ПО СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;

– установку обновлений ПО, включая ПО СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;

– централизованное управление системой защиты информации;

– регистрацию и анализ событий в ИС, связанных с защитой информации (далее – события безопасности);

– информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации и отдельных СЗИ, а также их обучение;

– сопровождение функционирования системы защиты информации ИС в ходе ее эксплуатации;

– поддержание конфигурации ИС и системы защиты информации (структуры системы защиты информации, состава, мест установки и параметров настройки СЗИ, ПО и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИС и системы защиты информации);

– управление изменениями базовой конфигурации ИС и системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИС и системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИС и системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИС и системы защиты информации, сохранение данных об изменениях базовой конфигурации ИС и системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИС и системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС и системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность Организации;

– контроль безотказного функционирования технических средств, обнаружение и локализацию отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;

– мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

– отслеживание попыток использования ИС вне установленного рабочего времени;

– определение параметров настройки ПО, включая ПО СЗИ, состава и конфигурации технических средств и ПО до внесения изменений в базовую конфигурацию ИС и системы защиты информации;

– методическую помощь всем пользователям ИС по вопросам обеспечения безопасности информации.

3.3. Администратор безопасности **имеет право**:

– отключать от ресурсов ИС работников, осуществивших НСД к защищаемым ресурсам ИС или нарушивших другие требования по ИБ;

– давать работникам обязательные для исполнения указания и рекомендации по вопросам информационной безопасности;

– контролировать исполнение пользователями правил парольной политики, правил работы в ИС, соблюдение внутренних регламентов по защите информации;

– инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИС;

– осуществлять контроль информационных потоков, генерируемых пользователями ИС при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа;

– запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное ПО и аппаратное обеспечение;

– участвовать в приемке новых программных средств обработки информации, новых ИС, порталов, web-сервисов и т.д.

– вырабатывать предложения по дальнейшему усовершенствованию принятой политики безопасности, выбору используемого в ИС ПО, СЗИ и аппаратного обеспечения.

3.4. Администратор безопасности **обязан:**

– знать и выполнять требования нормативных документов (в том числе локальных) по защите информации, регламентирующих порядок обеспечения безопасности информации, обрабатываемой в ИС;

– осуществлять управление изменениями конфигурации системы защиты информации, проводить анализ потенциального воздействия планируемых изменений ИС, осуществлять документирование данных о таких изменениях;

– осуществлять периодический мониторинг (контроль) защищенности ИС;

– своевременное информировать лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС;

– выявлять, анализировать уязвимости системы защиты информации ИС и оперативно устранять вновь выявленные уязвимости;

– осуществлять контроль выполнения мер по защите технических средств;

– оказывать помощь пользователям ИС в части применения СЗИ и консультировать по вопросам введенного режима защиты;

– в случае отказа работоспособности технических средств и ПО ИС, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

– в случае выявления нарушений режима безопасности защищаемой информации, а также возникновения внештатных и аварийных ситуаций, немедленно докладывать об этом ответственному лицу и принимать необходимые меры с целью ликвидации их последствий;

3.4.1. При выявлении факта/попытки НСД администратор безопасности обязан:

– прекратить доступ к ИС со стороны выявленного участка НСД;

– доложить руководителю и/или ответственному за обеспечение безопасности информации о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

– проанализировать характер НСД;

– совместно с ответственным лицом осуществить действия по выяснению причин,

приведших к НСД;

– предпринять меры по предотвращению подобных инцидентов в дальнейшем.

К попыткам НСД относятся:

– сеансы работы с ИС незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;

– действия третьего лица, пытающегося получить доступ (или получившего доступ) к ИС с использованием учетной записи администратора или другого пользователя ИС, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

4. Ответственность администратора безопасности

4.1 Администратор безопасности несет персональную ответственность:

– За качество выполнения обязанностей, установленных данной Инструкцией;

– За качество проводимых работ по контролю действий пользователей, состояние и поддержание необходимого уровня защищенности информации, содержащейся в ИС;

– За разглашение данных, ставших известными ему по роду работы.

4.2 За нарушение настоящей Инструкции Ответственное лицо может быть привлечено к дисциплинарной или иной предусмотренной законодательством ответственности.

ЛИСТ ОЗНАКОМЛЕНИЯ
с инструкцией администратора информационной безопасности

№	Фамилия И.О.	Должность, структурное подразделение	Подпись, дата

ПРИЛОЖЕНИЕ 3
к Приказу
от 30.11.2022 г. № 257

СОСТАВ
комиссии по вопросам информационной безопасности БУЗОО «КДЦ».

Для регулирования вопросов, связанных с информационной безопасностью в БУЗОО «КДЦ», назначается комиссия в составе:

Председатель комиссии:

Бодрова Т.В.	Заместитель главного врача по организационно-методической работе

Члены комиссии:

Савельев А.В.	Начальник отдела автоматизированных систем управления
Иванов С.В.	Ведущий программист
Кунгурова Л.А.	Системный администратор

В случае отсутствия Бодровой Т.В обязанности председателя комиссии возлагать на начальника отдела автоматизированных систем управления Савельева А.В.

ПРИЛОЖЕНИЕ 5
к Приказу
от 30.11.2022 г. № 257

СОСТАВ

комиссии по вопросам обеспечения безопасности критической информационной инфраструктуры Бюджетное учреждение здравоохранения Омской области «Клинический диагностический центр»

Для регулирования вопросов, связанных с обеспечением безопасности критической информационной инфраструктуры Бюджетное учреждение здравоохранения Омской области «Клинический диагностический центр», а также в целях исполнения Федерального закона РФ от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», назначается комиссия в составе:

Председатель комиссии:

Бодрова Т.В.	Заместитель главного врача по организационно-методической работе

Члены комиссии:

Кунгурова Л.А.	Системный администратор
Савельев А.В.	Начальник отдела автоматизированных систем управления
Барсуков А.С.	Главный бухгалтер
Каракулов П.В.	Начальник отдела эксплуатации медицинской техники
Шефлер М.Е.	Начальник кадрово-правовой службы
Апресов Д.С.	Начальник планово - экономического отдела

В случае отсутствия Бодровой Т.В. обязанности председателя комиссии возлагать на системного администратора Кунгурову Л.А.

ПРИЛОЖЕНИЕ 6
к Приказу
от 30.11.2022 г. № 254

ПОЛОЖЕНИЕ
о Комиссии по вопросам обеспечения безопасности критической информационной инфраструктуры БУЗОО «КДЦ»

Обозначения и сокращения по тексту

БУЗОО «КДЦ»	– Бюджетное учреждение здравоохранения Омской области «Клинический диагностический центр»;
Ответственный (ответственное лицо)	– Должностное лицо, ответственное за обеспечение безопасности критической информационной инфраструктуры
Администратор безопасности	– Администратор информационной безопасности
ИС	– Информационные системы БУЗОО «КДЦ»
Категорирование	– Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения (Источник: Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации, статья 7, пункт 1)
КИИ	– Критическая информационная инфраструктура
ОКИИ	– Объекты критической информационной инфраструктуры: Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры (Источник: Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», статья № 2, пункт 7).

1. Общие положения

1.1. Настоящее Положение определяет структуру, основные задачи и порядок работы Комиссии по вопросам обеспечения безопасности критической информационной инфраструктуры Бюджетное учреждение здравоохранения Омской области «Клинический диагностический центр» (далее – Комиссия).

1.2. Комиссия назначается приказом руководителя БУЗОО «КДЦ».

1.3. Комиссия создается для достижения следующих целей:

– исполнение требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также иных положений нормативных правовых актов в сфере КИИ;

– укрепление безопасности ОКИИ в организации путем непосредственного участия руководства и выделения необходимых ресурсов;

– координация внедрения мероприятий по управлению информационной безопасностью ОКИИ.

1.4. Комиссия осуществляет свою деятельность в соответствии с действующими федеральными законами, постановлениями и решениями Правительства Российской Федерации, методическими и руководящими документами органов уполномоченных в сфере технической защиты информации, приказами и указаниями руководства БУЗОО «КДЦ», данным Положением и иными внутренними организационными распорядительными документами, регулирующими вопросы защиты ОКИИ.

1.5. Организационно Комиссия состоит из председателя и членов Комиссии.

1.6. Комиссия является постоянно действующим коллегиальным органом, действующим в интересах БУЗОО «КДЦ».

1.7. В состав комиссии в обязательном порядке должны включаться администратор безопасности и ответственное лицо.

1.8. Членами Комиссии назначаются:

1. работники, являющиеся специалистами в области выполняемых функций или осуществляемых видов деятельности, и в области информационных технологий и связи, а также специалисты по эксплуатации основного технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учёту опасных веществ и материалов;
2. работники, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов критической информационной инфраструктуры;
3. работники подразделения по защите государственной тайны (в случае, если объект КИИ обрабатывает информацию, составляющую государственную тайну);
4. работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций.

1.9. Решения Комиссии, принимаемые в соответствии с ее компетенцией, после подписания протокола заседания Председателем Комиссии носят с учётом действующих в БУЗОО «КДЦ» организационно-распорядительных и внутренних нормативных документов обязательный характер для членов Комиссии, структурных подразделений, должностных лиц и работников БУЗОО «КДЦ».

1.10. Определения **ролей:**

Наименование роли	Определение роли
Председатель Комиссии	Должностное лицо, согласно приказу об утверждении / изменении состава Комиссии
Члены Комиссии	Должностные лица, согласно приказу об утверждении / изменении состава Комиссии
Приглашенные лица на заседание Комиссии	Приглашенные лица для участия в заседании Комиссии

2. Основные задачи Комиссии

2.1. Принятие решения о принадлежности БУЗОО «КДЦ» к субъектам КИИ.

2.2. Категорирование ОКИИ.

2.3. Определение концептуальных подходов к обеспечению защиты ОКИИ.

2.4. Утверждение и пересмотр политики информационной безопасности и соответствующих обязанностей по ее выполнению в части защиты ОКИИ.

2.5. Анализ и мониторинг инцидентов нарушения безопасности ОКИИ.

2.6. Утверждение основных проектов в области обеспечения безопасности ОКИИ.

2.7. Согласование конкретных функций и обязанностей в области информационной безопасности ОКИИ в рамках организации.

2.8. Согласование конкретных методик и процедур обеспечения безопасности ОКИИ.

2.9. Оценка адекватности и координация внедрения конкретных мероприятий по управлению безопасностью КИИ для новых ОКИИ.

2.10. По решению председателя Комиссии могут рассматриваться и другие вопросы, возникшие в ходе работ по обеспечению безопасности ОКИИ.

3. Порядок работы Комиссии

3.1. Периодичность созыва Комиссии определяется ее председателем, но не может быть реже 1 раза в год.

3.2. Для оперативного решения вопросов связанных с обеспечением безопасности ОКИИ могут проводиться внеочередные созывы Комиссии. Инициатива о внеочередном созыве Комиссии может поступать от руководителя БУЗОО «КДЦ», председателя Комиссии, ответственного лица или администратора безопасности.

3.3. Решения Комиссии принимаются открытым голосованием и считаются принятыми, если они поддержаны большинством присутствующих членов Комиссии.

3.4. Решения Комиссии утверждаются руководителем организации и доводятся до исполнителей и других заинтересованных лиц в части, их касающейся.

3.5. Протоколы и решения Комиссии хранятся у председателя Комиссии, в соответствии с требованиями, предъявленными к защищенному документообороту.

3.6. Для включения в повестку дня заседания Комиссии внепланового вопроса лицо, инициирующее рассмотрение вопроса, не менее чем за 5 рабочих дней до предлагаемой даты заседания Комиссии направляет в адрес Председателя Комиссии служебную записку с указанием перечня вопросов, подлежащих рассмотрению.

К служебной записке прилагается пояснительная записка с обоснованием целесообразности рассмотрения Комиссией данного вопроса и другие материалы, необходимые Комиссии для рассмотрения вопроса повестки дня, и предложения по списку приглашенных лиц, не являющихся членами Комиссии.

3.7. Заседания Комиссии, как правило, проводятся в очной форме. В отдельных случаях по решению Председателя Комиссии, когда дискуссия по рассматриваемому вопросу маловероятна (например, утверждение Плана работ или Отчёта об его исполнении), допускается проведения заседания в заочной форме. Для проведения заочного заседания в составе документов включается опросный лист для голосования с проектом решения по вопросам повестки дня заседания Комиссии, а члены Комиссии участвуют в голосовании посредством представления к назначенной дате проведения заседания заполненных опросных листов с отражением своей позиции по каждому рассматриваемому вопросу заседания.

3.8. Заседание Комиссии считается правомочным (имеет кворум), если в нём приняли участие (представили опросные листы при проведении заседания в заочной форме) не менее половины списочного состава членов Комиссии. Не допускается делегирование членом Комиссии своих полномочий иным лицам.

3.9. Каждый член Комиссии обладает одним голосом. Передача голоса одним членом Комиссии другому члену Комиссии не допускается. Решение Комиссии принимается простым большинством голосов членов Комиссии, принявших участие в заседании. При равенстве голосов решающим является голос председательствующего.

3.10. Рассмотренные на заседании Комиссии вопросы и принятые по ним решения в течение 2 (двух) рабочих дней, начиная со дня, следующего за днем заседания, оформляются избранным на заседании секретарем Комиссии в виде проекта протокола заседания, который направляется посредством корпоративной электронной почты на согласование членам Комиссии, принявшим участие в заседании.

3.11. В протоколе заседания Комиссии указываются:

- дата заседания Комиссии и форма заседания (очная/заочная);
- фамилии и инициалы присутствующих на заседании (представивших опросные листы при проведении заседания в заочной форме) членов Комиссии, включая Председателя Комиссии, и приглашённых лиц;

- в случае председательства на заседании Заместителя Председателя Комиссии – основания, на которых он выполняет данную функцию;
- формулировка каждого из рассматривавшийся вопросов;
- рассмотренные на заседании материалы и информация, включая пояснительные записки и объяснения виновных в нарушениях, положенные в основу принимаемых решений;
- фамилии и инициалы выступивших на заседании лиц, и краткое изложение их выступлений;
- пояснительная (обосновывающая) часть принятого решения;
- принятые решения по каждому вопросу;
- результаты голосования с обязательным указанием фамилий и инициалов лиц, проголосовавших против принятых решений или воздержавшихся от голосования;
- фамилии и инициалы лица, протоколировавшего заседание.

К Протоколу прилагаются все рассмотренные на заседании материалы и изложенные по желанию в письменной форме мнения членов Комиссии, не согласившихся с её решением.

3.12. Члены Комиссии согласованием в корпоративной электронной почте в течение 2 (двух) рабочих дней подтверждают правильность отражения в проекте протокола заседания высказанную ими позицию по рассмотренным вопросам очного/заочного заседания. В случае отсутствия обратной связи в обозначенный срок протокол считается согласованным.

3.13. На последнем заседании календарного года члены Комиссии рассматривают отчёт о результатах выполнения Плана работы Комиссии на календарный год, который после утверждения Председателем Комиссии рассылается всем членам Комиссии (и, при необходимости, руководителям структурных подразделений организации) на ознакомление.

3.14. Ежегодно не позднее 20 января текущего года Председатель Комиссии представляет служебной запиской на ознакомление руководителю БУЗОО «КДЦ» отчёт о результатах выполнения Плана работы Комиссии за прошедший год.

4. Функции и права Председателя и членов Комиссии

4.1. В функции Председателя Комиссии входит:

- организация работы Комиссии, утверждение Плана работы Комиссии на календарный год, а также Отчёта о его исполнении;
- созыв заседания Комиссии, назначение или утверждение предложенной инициатором рассмотрения вопроса даты заседания Комиссии, утверждение повестки дня заседания Комиссии, ведение её очных заседаний;
- согласование списка приглашаемых для участия в заседаниях Комиссии лиц;
- утверждение решений Комиссии путём подписания протоколов заседаний Комиссии;
- выполнение функции члена Комиссии;
- контроль исполнения решений и рекомендаций, отражённых в протоколах Комиссии.

4.2. Председатель Комиссии имеет право:

- запрашивать и получать от всех структурных подразделений организации необходимую для выполнения функций Комиссии информацию, в пределах компетенции Комиссии;
- приглашать на заседания Комиссии работников структурных подразделений организации, контрагентов, экспертов, консультантов для рассмотрения отдельных вопросов, требующих их участия;
- осуществлять иные права, предусмотренные законодательством Российской Федерации, иными внутренними документами БУЗОО «КДЦ» и настоящим Положением.

4.3. В функции членов комиссии входит:

- изучение вопросов и материалов повестки дня заседания Комиссии и формирование позиции по вопросам повестки;

- принятие личного участия в заседаниях Комиссии, голосование по вопросам повестки дня заседания Комиссии;
- по поручению Председателя Комиссии подготовка, в рамках своей компетенции, тематических материалов, докладов, экспертных заключений, Отчётов по вопросам заседания Комиссии;
- направление в адрес Председателя Комиссии своих предложений об участии в работе Комиссии заинтересованных сотрудников или сторонних организаций.

4.4. Члены Комиссии имеют право:

- вносить вопросы в пределах компетенции Комиссии в повестку дня заседаний Комиссии и представлять по ним материалы;
- привлекать к формированию позиции по вопросам повестки дня заседания Комиссии работников подразделений в рамках своего функционального направления;
- выносить предложения о приглашении для участия в заседаниях Комиссии работников структурных подразделений организации, контрагентов, экспертов, консультантов для рассмотрения отдельных вопросов, требующих их участия;
- выступать на заседаниях Комиссии по вопросам повестки дня, а также с соответствующими инициативами о принятии решений по вопросам повестки дня заседаний Комиссии;
- в письменной форме излагать своё мнение, при его несогласии с решением Комиссии, которое подлежит обязательному приобщению к протоколу заседания Комиссии;
- осуществлять иные права, предусмотренные законодательством Российской федерации, иными внутренними документами БУЗОО «КДЦ» и настоящим Положением.

ЛИСТ ОЗНАКОМЛЕНИЯ

с положением о Комиссии по вопросам обеспечения безопасности критической информационной инфраструктуры БУЗОО «КДЦ»

№	Фамилия И.О.	Должность, структурное подразделение	Подпись, дата

ПРИЛОЖЕНИЕ 7
к Приказу
от 30.11.2022 г. № 257

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности критической информационной инфраструктуры БУЗОО «КДЦ»

Обозначения и сокращения по тексту

БУЗОО «КДЦ», Субъект КИИ	–	Бюджетное учреждение здравоохранения Омской области «Клинический диагностический центр»
Администратор безопасности	–	Администратор информационной безопасности
ИС	–	Информационные системы БУЗОО «КДЦ»
Категорирование	–	Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения (Источник: Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации, статья 7, пункт 1)
КИИ	–	Критическая информационная инфраструктура
ОКИИ	–	Объекты критической информационной инфраструктуры: Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры (Источник: Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», статья № 2, пункт 7).

1. Общие положения

1.1. В настоящем документе определяются права, обязанности, а также ответственность должностного лица, ответственного за обеспечение безопасности критической информационной инфраструктуры в БУЗОО «КДЦ».

1.2. Лицо, ответственное за обеспечение безопасности критической информационной инфраструктуры (далее – Ответственный; ответственное лицо) – должностное лицо, отвечающее за организацию работ по обеспечению безопасности объектов КИИ, не являющихся значимыми, принадлежащих БУЗОО «КДЦ», а также осуществляющее контроль доступа к таким ОКИИ.

1.3. Ответственный назначается на должность из числа штатных сотрудников БУЗОО «КДЦ» приказом руководителя БУЗОО «КДЦ», и подотчетен ему.

1.4. Лицо, ответственное за обеспечение безопасности КИИ в своей работе должен руководствоваться настоящей инструкцией и следующими основными законодательными и нормативными правовыми актами Российской Федерации:

– Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Постановление Правительства № 127 от 08.02.2018 г. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

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

– Приказ ФСТЭК России № 236 от 21.12.2017 г. «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

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

– Приказ ФСБ России от 24.07.2018 №367 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»;

– Приказ ФСБ России от 24.07.2018 №368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

– локальные акты БУЗОО «КДЦ» в области защиты информации, а также в области обеспечения безопасности КИИ.

2. Должностные обязанности

2.1. Ответственный обязан:

– осуществлять разработку предложений по совершенствованию организационно-распорядительных документов по безопасности ОКИИ и представление их руководителю субъекта критической информационной инфраструктуры (уполномоченному лицу).

– осуществлять поддержание в актуальном состоянии организационно-распорядительных документов БУЗОО «КДЦ» по безопасности объектов КИИ.

– осуществлять анализ угроз безопасности информации в отношении объектов критической информационной инфраструктуры и выявление уязвимостей в них;

– осуществлять планирование, разработку, совершенствование и внедрение мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры БУЗОО «КДЦ»;

– принимать участие в реагировании на инциденты безопасности, связанные с ОКИИ;

– организовывать проведение оценки соответствия объектов критической информационной инфраструктуры требованиям по безопасности;

– осуществлять подготовку предложений по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности ОКИИ;

– осуществлять внутренний контроль соблюдения сотрудниками Организации Законодательства Российской Федерации о защите ОКИИ, контроль выполнения сотрудниками, допущенными к работе с ОКИИ, предъявляемых требований к безопасности

ОКИИ;

– осуществлять контроль своевременного проведения категорирования в случаях изменения ОКИИ, в результате которого такие объекты перестали соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости (или отсутствие такой категории), либо внедрение новых ИС, ИТКС, АСУ ТП, потенциально являющимися ОКИИ;

– доводить до сведения сотрудников БУЗОО «КДЦ» положения законодательства по защите КИИ, локальных актов по вопросам информационной безопасности ОКИИ, требований к защите таких объектов.

– выявлять факты несоблюдения условий обеспечения безопасности ОКИИ, использования нерегламентированных программных и технических средств, способных привести к нарушению конфиденциальности обрабатываемых данных, а также иных нарушений, приводящих к снижению уровня защищенности ОКИИ.

2.2. На ответственное лицо возлагается задача по организации выполнения требований законодательства по защите объектов КИИ, не отнесенных к значимым (без категории значимости).

2.3. Требования ответственного лица, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми сотрудниками БУЗОО «КДЦ».

3. Должностные права

3.1. Ответственное лицо имеет право:

– запрашивать у сотрудников организации информацию, необходимую для реализации своих полномочий.

– требовать от сотрудников организации, являющихся пользователями ОКИИ, выполнения требований локальных актов по обеспечению безопасности ОКИИ.

– участвовать в разработке мероприятий по совершенствованию безопасности ОКИИ.

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ОКИИ.

– вносить руководителю организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении ОКИИ.

– вносить руководителю организации предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ОКИИ.

4. Ответственность

4.1. Ответственное лицо несет персональную ответственность за качество проводимых им работ, связанных с выполнением им своих должностных обязанностей.

4.2. За нарушение настоящей Инструкции Ответственное лицо может быть привлечено к дисциплинарной или иной предусмотренной законодательством ответственности.

Лист согласования

Проекта приказа
«О назначении лиц, ответственных
за обеспечение информационной безопасности

Должность, ФИО	Подпись	Дата	Замечания
Финансовый директор Толкачев С.М.		24.11.2022г	—
Заместитель главного врача по медицинской части Смяловский В.Э.		23.11.22	
Заместитель главного врача по лечебной работе Брейль А.П.		24.11.22	
Заместитель главного врача по КЭР Урлапова Г.П.		24.11.22.	
Заместитель главного врача по ОМР Бодрова Т.В.		16.11.22.	
Начальник кадрово-правовой службы Шефлер М.Е.		22.11.2022	
Главный бухгалтер Барсуков А.С.		17.11.22г	
Главная медсестра Мысикова Г.П.		22.11.22	

ЛИСТ ОЗНАКОМЛЕНИЯ к Приказу №357 от «30» 11 2022 г.

О назначении лиц, ответственных за обеспечение информационной безопасности

Должность	*Подпись*	*Расшифровка подписи*	*Дата*
Зам. главного врача по медицинской части		Смяловский В.Э.	05.12.22
Зам. главного врача по лечебной работе		Брейль А.П.	02.12.22.
Зам. главного врача по ОМР		Бодрова Т.В.	30.11.22г
Зам. главного врача по КЭР		Урлапова Г.П.	
Начальник кадрово-правовой службы		Шефлер М.Е.	02.12.2022
Главная медицинская сестра		Мысикова Г.П.	02.12.22
Главный бухгалтер		Барсуков А.С.	02.12.22
Финансовый директор		Толкачев С.М.	30.11.2022г
Начальник организационно-методического отдела		Немчинова И.П.	30.11.2022г
Старшая сестра организационно-методического отдела		Бахта С.А.	02.12.2022
Заведующий централизованной микробиологической лабораторией		Андреева Г.А.	02.12.2022
И.о.заведующей Централизованной лабораторией		Фень А.В.	02.12.2022
Начальник отдела АСУ		Савельев А.В.	30.11.2022
Заведующий дневным стационаром		Предвечная И.К.	30.11.2022
Заведующий круглосуточным стационаром		Самсонов К.Ю.	30.11.22
Заведующая консультативным отделом		Бычковская И.С.	30.11.22
Заведующая отделом ультразвуковой диагностики		Ерофеева А.Л.	30.11.22г.
Заведующий отделом ФМИ		Потапов В.В.	30.11.2022

Заведующий эндоскопическим отделом		Кириченко Н.П.	30.11.22г
Заведующий группой анестезиологии-реанимации		Гладких В.А.	30.11.2022г.
Начальник отдела ЭМТ		Каракулов П.В.	30.11.2022
Заведующий аптекой		Баженова Н.А.	30.11.2022
Руководитель контрактной службы		Демьяненко Т.А.	30.11.2022
Начальник хозяйственного отдела		Сарин В.А.	30.11.2022г.
Старшая медсестра дневного стационара		Дятлова Е.В.	30.11.2022г
Старшая медсестра отдела ФМИ		Волосатова М.А.	30.11.22
Старшая медсестра отдела РМИ		Старостина А.В.	30.11.22.
Старшая медсестра отдела УЗД		Чайка О.В.	30.11.22г
Старшая медсестра эндоскопического отдела		Перешивко И.Н.	30.11.22
Старшая медсестра консультативного отдела		Гришкова Е.С.	30.11.2022г
Старшая медсестра круглосуточного стационара	Чернышева	Чернышева О.А.	30.11.2022
Старшая лаборант централизованной микробиологической лаборатории		Цеханович Т.Н.	30.11.2022г.
Старшая лаборант централизованной лаборатории		Кропочева Н.М.	30 11 22