Министерство здравоохранения

Ростовской области

Государственное бюджетное учреждение Ростовской области

«Центр медицинской реабилитации №1»

в г. Таганроге

ПРИКАЗ

№ 205.1- ОД от 03 декабря 2021г.

О внесении изменений

в приказ о защите информации

В связи с кадровыми изменениями,

# приказываю:

1. Назначить ответственным за информатизацию, в том числе за организацию защиты информации и обработки персональных данных в автоматизированной системе (далее -АС) ГБУ РО «ЦМР №1» в г. Таганроге, заместителя главного врача по общим вопросам Янченко А.В.
2. Назначить администратором информационной безопасности АС ГБУ РО «ЦМР №1» в г. Таганроге ведущего инженера-программиста Балкизова Т.В.
3. Назначить ответственным пользователем средств криптографической защиты информации (СКЗИ) АС ГБУ РО «ЦМР №1» в г. Таганроге ведущего инженера-программиста Балкизова Т.В.
4. Утвердить:

4.1. Инструкцию ответственного за информатизацию, в том числе за организацию защиты информации и обработки персональных данных в АС ГБУ РО «ЦМР №1» в г. Таганроге, согласно приложению 1.

4.2. Инструкцию администратора информационной безопасности АС ГБУ РО «ЦМР №1» в г. Таганроге, согласно приложению 2.

4.3. Инструкцию администратора информационной безопасности по организации защищенного автоматизированного рабочего места в АС ГБУ РО «ЦМР №1» в г. Таганроге, согласно приложению 3.

5. Сотрудникам, указанным в п.1-3 настоящего приказа, руководствоваться инструкциями, указанными в п.4 настоящего приказа в части касающейся.

6. Контроль за исполнением настоящего приказа оставляю за собой.

И.о.главного врача С.Г. Беседовский

Томашевич О.Б.

(88634) 477016

«СОГЛАСОВАНО» Балкизов Т.В.

|  |
| --- |
| **Приложение № 1**  **к приказу**  **от 03.12.2021 г. № 205.1-ОД** |

ИНСТРУКЦИЯ

**ответственного за информатизацию, в том числе за организацию защиты информации и обработки персональных данных в автоматизированной системе ГБУ РО «Центр медицинской реабилитации № 1» в г. Таганроге**

1. **Общие положения**
   1. Настоящая Инструкция определяет основные права и обязанности специалиста ответственного за информатизацию, в том числе организацию защиты информации и обработки персональных данных в автоматизированной системе (АС) ГБУ РО «Центр медицинской реабилитации № 1» в г. Таганроге (ГБУ РО «ЦМР № 1» в г. Таганроге).
   2. Ответственный за организацию защиты информации и обработки персональных данных назначается приказом руководителя ГБУ РО «ЦМР №1» в г. Таганроге на основании Федерального Закона «О персональных данных» №152-ФЗ от 27 июля 2006 года.
2. **Обязанности ответственного за организацию защиты информации и обработки персональных данных**
   1. Организация технологического процесса обработки персональных данных и иной конфиденциальной информации в соответствии с локальными и внешними нормативно-правовыми актами.
   2. Организация ознакомления сотрудников под роспись с локальными и внешними нормативно-правовыми актами, регулирующими обработку персональных данных и иной конфиденциальной информации.
   3. Организация заключения соглашения между ГБУ РО «ЦМР № 1» в г. Таганроге и работниками о соблюдении требований обращения с защищаемой информацией.
   4. Уведомление уполномоченного органа по защите прав субъектов персональных данных о намерении ГБУ РО «ЦМР № 1» в г. Таганроге осуществлять обработку персональных данных в качестве оператора.
   5. Планирование и координация работ по внедрению организационных и технических мер обеспечения безопасности персональных данных и иной конфиденциальной информации.
   6. Контроль за деятельностью администратора информационной безопасности.
   7. Организация периодического контроля за исполнением сотрудниками организационных и технических мер обеспечения информационной безопасности при обработке персональных данных и иной конфиденциальной информации.
   8. Организация периодического контроля за соблюдением правил обработки защищаемой информации и эффективности принятых мер защиты информации с последующим анализом результатов контроля.
   9. Рассмотрение предложений и принятие решений по устранению недостатков и предупреждению нарушений в области обеспечения информационной безопасности, осуществление контроля за устранением нарушений.
   10. Рассмотрение предложений и принятие решений по внесению изменений в конфигурацию информационной системы и экстренной модификации ПО.
   11. Утверждение предложений по совершенствованию технологического процесса обработки защищаемой информации.
   12. Осуществление непосредственного контроля за соблюдением установленного законодательством порядка рассмотрения запросов субъектов персональных данных
   13. Организация повышения квалификации, осведомленности сотрудников в области защиты персональных данных и иной конфиденциальной информации.
   14. Изучение отчетов и прочих материалов о состоянии работ по обеспечению безопасности персональных данных в АИС ГБУ РО «ЦМР № 1» в г. Таганроге.
   15. Участие в комиссии по уничтожению защищаемой информации и хранение актов об уничтожении защищаемой информации.
   16. Руководство рабочей группой по расследованию событий и инцидентов информационной безопасности.
3. **Права ответственного за организацию защиты информации и обработки персональных данных**

Ответственный за организацию защиты информации и обработки персональных данных имеет право:

* 1. Запрашивать и получать необходимые материалы для выполнения возложенных на него обязанностей.
  2. Осуществлять контроль за реализацией организационных и распорядительных документов по организации обработки и обеспечению безопасности персональных данных.
  3. Рассматривать предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области технической защиты конфиденциальной информации.
  4. Принимать решение о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) защищаемой информации.
  5. Привлекать в установленном порядке необходимых специалистов, в том числе сотрудников ГБУ РО «ЦМР №1» в г.Таганроге для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

1. **Ответственность специалиста ответственного за организацию защиты информации и обработки персональных данных**
   1. Ответственный за организацию защиты информации и обработки персональных данных несет персональную ответственность за:

* правильность и объективность принимаемых решений;
* правильное и своевременное выполнение организационных и распорядительных документов, принятых руководством ГБУ РО «ЦМР № 1» в г. Таганроге по вопросам обработки и защиты персональных данных и иной конфиденциальной информации;
* выполнение возложенных на него обязанностей, предусмотренных организационно-распорядительной документацией ГБУ РО «ЦМР № 1» в г. Таганроге;
* качество проводимых работ по обеспечению безопасности персональных данных и иной конфиденциальной информации в соответствии с функциональными обязанностями.

|  |
| --- |
| **Приложение № 2**  **к приказу**  **от 03.12.2021 г. № 205.1-ОД** |

ИНСТРУКЦИЯ

**администратора информационной безопасности автоматизированной системы ГБУ РО «Центр медицинской реабилитации № 1» в г. Таганроге**

1. **Общие положения**

1.1.Настоящая Инструкция определяет основные права и обязанности администратора информационной безопасности (далее – Администратор ИБ) автоматизированной системы (АС) ГБУ РО «Центр медицинской реабилитации № 1» в г. Таганроге (ГБУ РО «ЦМР № 1» в г. Таганроге).

* 1. Администратор ИБ назначается из числа штатных сотрудников ГБУ РО «ЦМР № 1» в г. Таганроге и отвечает за реализацию требований и мер по защите информации, обрабатываемой в АИС ГБУ РО «ЦМР № 1» в г. Таганроге.

1. **Обязанности администратора информационной безопасности**
   1. Настройка средств защиты информации и контроль таких настроек в соответствии с требованиями по безопасности.
   2. Выявление (анализ) возможных уязвимостей системы защиты информации в процессе эксплуатации АИС ГБУ РО «ЦМР № 1» в г. Таганроге, их нейтрализация и(или) внесение предложений по их нейтрализации.
   3. Установка, настройка и поддержание в исправном состоянии технических и программных средств системы защиты информации АИС ГБУ РО «ЦМР № 1» в г. Таганроге.
   4. Регистрация пользователей с присвоением/изменением полномочий по доступу в АИС ГБУ РО «ЦМР № 1» в г. Таганроге.
   5. Контроль соответствия действий пользователей с утвержденной технологией обработки и защиты информации.
   6. Ведение копий программных компонентов средств защиты информации, их периодическое обновление (при необходимости) и контроль работоспособности.
   7. Резервирование критических компонентов системы (файлов конфигураций, данных и т.п).
   8. Выполнение работ по масштабированию и изменению состава АИС ГБУ РО «ЦМР № 1» в г. Таганроге установленным порядком.
   9. Проведение периодического контроля эффективности принятых мер защиты информации в АИС ГБУ РО «ЦМР № 1» в г. Таганроге.
   10. Формирование предложений по устранению недостатков и предупреждению нарушений в области обеспечения информационной безопасности, осуществление контроля за устранением нарушений.
   11. Инструктаж и обучение в пределах своей компетенции сотрудников в области технической защиты персональных данных и иной конфиденциальной информации при ее обработке в АИС ГБУ РО «ЦМР № 1» в г. Таганроге.
2. **Права администратора информационной безопасности**

Администратор ИБ имеет право:

* 1. Запрашивать и получать необходимые материалы для выполнения возложенных обязанностей.
  2. Осуществлять контроль за реализацией и работой системы защиты АИС ГБУ РО «ЦМР № 1» в г. Таганроге.
  3. Формировать предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.
  4. Принимать решение о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) защищаемой информации.
  5. Привлекать в установленном порядке необходимых специалистов из числа сотрудников ГБУ РО «ЦМР № 1» в г. Таганроге для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

1. **Ответственность администратора информационной безопасности**
   1. Администратор ИБ несет персональную ответственность за:

* правильность и объективность принимаемых решений;
* правильное и своевременное выполнение организационных и распорядительных документов, принятых руководством ГБУ РО «ЦМР № 1» в г. Таганроге по вопросам обработки и защиты информации в АИС ГБУ РО «ЦМР № 1» в г. Таганроге;
* выполнение возложенных на него обязанностей, предусмотренных настоящей инструкцией;
* качество проводимых работ по обеспечению безопасности конфиденциальной информации, в том числе персональных данных в соответствии с функциональными обязанностями.

|  |  |
| --- | --- |
| **Приложение № 8**  **к приказу**  **от 03.12.2021 г. № 205.1-ОД** | |
|  |

ИНСТРУКЦИЯ

**администратора информационной безопасности по организации защищенного автоматизированного рабочего места в автоматизированной системе ГБУ РО «Центр медицинской реабилитации № 1» в г. Таганроге**

1. **Общие положения**

1.1.Настоящая Инструкция определяет порядок организации защищенного автоматизированного рабочего места (ЗАРМ) в автоматизированной системе (АС) ГБУ РО «Центр медицинской реабилитации № 1» в г. Таганроге (ГБУ РО «ЦМР № 1» в г. Таганроге).

* 1. В качестве ЗАРМ в АС ГБУ РО «ЦМР № 1» в г. Таганроге используются бездисковые терминалы и мобильные устройства.

1. **Организация рабочего места**
   1. Подключение ЗАРМ сотрудников к АС ГБУ РО «ЦМР № 1» в г. Таганроге осуществляет администратор информационной безопасности АС ГБУ РО «ЦМР № 1» в г. Таганроге (далее, администратор ИБ), на основании распоряжения (приказа) руководителя ГБУ РО «ЦМР № 1» в г. Таганроге.
   2. Типовое ЗАРМ состоит из:
   * системного блока;
   * клавиатуры;
   * манипулятора типа «мышь»;
   * принтера;
   * считывателя;
   * монитора;
   * web-камера;
   * гарнитура (микрофон с наушниками)

или

* + мобильного устройства.
  1. К работе в АС ГБУ РО «ЦМР № 1» в г. Таганроге допускаются сотрудники, в том числе и находящиеся на испытательном сроке, которые:
  + замещают должности которые предусматривают осуществление обработки персональных данных либо осуществление доступа к персональным данным и иной конфиденциальной информации*;*
  + прошли инструктаж по работе в АС ГБУ РО «ЦМР № 1» в г. Таганроге у администратора ИБ;
  + ознакомились под роспись с «Основными положениями законодательства Российской Федерации в области защиты информации»;
  + ознакомились под роспись с локальной организационно-распорядительной документацией по организации обработки защищаемой информации, в части их касающейся.

1. **Защита помещений и технических средств**
   1. Доступ в режимные помещения, где расположены компоненты АС ГБУ РО «ЦМР № 1» в г. Таганроге в нерабочее время должен быть заблокирован дверью, закрытой на ключ.
   2. В рабочее время доступ в помещение контролируется ответственным персоналом, находящимся в помещении. При отсутствии персонала, нахождение посторонних лиц в режимном помещении запрещается, а дверь должна быть закрыта на ключ.
   3. Все работы по обслуживанию ЗАРМ проводятся только под контролем администратора ИБ.
   4. Размещение дисплеев, клавиатур, принтеров должно исключать их несанкционированный просмотр посторонними лицами и посетителями. Окна режимных помещений рекомендуется оснастить жалюзи;
   5. Размещение и режим эксплуатации устройств вывода аудиоинформации должно исключать несанкционированное прослушивание информации, в частности рабочие места предназначенные для оказания телемедицинских консультаций должны быть расположены в отдельных помещениях, а вывод аудио информации должен осуществляться в гарнитуру пользователя в случае невозможности исключения несанкционированного прослушивания информации оргмерами.
   6. Передача мобильных устройств третьим лицам запрещена.
2. **Порядок действий администратора при организации рабочего места**
   1. Перед установкой (выдачей или заменой) ЗАРМ, администратор ИБ должен убедиться, что пользователями выполнены все условия (раздел 2.3 настоящей инструкции).
   2. После успешной загрузки ЗАРМ администратор создает учетную запись пользователя и производит настройку ППО, задает первоначальное значение пароля и доводит до его пользователя.
   3. При организации мобильного ЗАРМ администратор устанавливает VPN клиент и антивирусное средство с функцией централизованного управления, затем создает учетную запись пользователя на сервере доступа мобильных устройств, задает первоначальное значение пароля и доводит до его пользователя
   4. При необходимости администратор ИБ производит обучающую демонстрацию работы для пользователя.
   5. В завершение работ, администратор ИБ оформляет акт ввода в эксплуатацию защищенного автоматизированного рабочего места, форма которого приведена в Приложении 1, к настоящей инструкции, с выполнением следующих условий:
   * акт составляется комиссией, в которую должен входить администратор ИБ, ответственный пользователь, начальник структурного подразделения эксплуатирующего рабочее место, ответственный за организацию защиты информации и обработки персональных данных.
   * в акте указывается наименование режимного помещения, в котором расположено подключаемое\изменяемое автоматизированное рабочее место, а также характеристики этого рабочего места (для бездисковых терминалов).
   1. На основании акта, администратор ИБ вносит изменение в матрицу доступа.
   2. При расформировании автоматизированного рабочего места администратором ИБ выполняются действия обратные указанному порядку, а в акте подключения защищенного автоматизированного рабочего места делается соответствующая отметка о расформировании.

|  |  |
| --- | --- |
|  | Приложение 1 к Инструкции администратора информационной безопасности по организации защищенного автоматизированного рабочего места в автоматизированной системе ГБУ РО «Центр медицинской реабилитации № 1» в г. Таганроге |

## *АКТ № \_\_\_\_*

ввода в эксплуатацию защищенного автоматизированного рабочего места АС ГБУ РО «ЦМР № 1» в г. Таганроге

Комиссией в составе:

Председатель комиссии – ответственный за организацию защиты информации и обработки персональных данных, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

Члены комиссии:

* Администратор ИБ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* Ответственный пользователь защищенного автоматизированного рабочего места, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

произведен ввод в эксплуатацию защищенного автоматизированного рабочего места (ЗАРМ) **\_\_\_\_\_\_\_\_\_**, в составе, указанном в таблице 1 и расположенного в режимном помещении \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (для бездисковых терминалов).

Таблица 1.

| **№**  **п/п** |  | **Наименование (модель) технических средств**  **и систем объекта информатизации** | **Заводской (серийный)**  **или инвентарный номер** | **Сетевой адрес (MAC)** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Ввод в эксплуатацию произведен в полном соответствии с «Инструкцией администратору информационной безопасности по организации защищенного автоматизированного рабочего места в автоматизированной системе ГБУ РО «Центр медицинской реабилитации № 1» в г. Таганроге.
2. Требования по защите технических средств и режимных помещений выполнены в полном объеме.
3. Все необходимое программное обеспечение и периферийное оборудование функционирует в штатном режиме.

Председатель комиссии:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_