

**ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«СТОМАТОЛОГИЧЕСКАЯ ПОЛИКЛИНИКА №2»
МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ КРАСНОДАРСКОГО КРАЯ**

ПРИКАЗ

«09» 01 2025 г.

№ 114

г. Краснодар

**О назначении ответственного за организацию обработки
персональных данных и других ответственных лиц**

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и принятыми в соответствии с ним нормативными правовыми актами, п р и к а з ы в а ю:

1. Утвердить:

1) Должностную инструкцию ответственного за организацию обработки персональных данных в государственном автономном учреждении здравоохранения "Стоматологическая поликлиника №2" министерства здравоохранения Краснодарского края (приложение 1);

2) Функциональные обязанности администратора информационной безопасности государственного автономного учреждения здравоохранения "Стоматологическая поликлиника №2" министерства здравоохранения Краснодарского края (приложение 2);

3) Функциональные обязанности администратора информационных систем государственного автономного учреждения здравоохранения "Стоматологическая поликлиника №2" министерства здравоохранения Краснодарского края (приложение 3);

2. Назначить ответственным за организацию обработки персональных данных из числа сотрудников государственного автономного учреждения здравоохранения "Стоматологическая поликлиника №2" министерства здравоохранения Краснодарского края специалиста по защите информации в компьютерных системах и сетях Тосунова А.С.

3. Ответственному за организацию обработки персональных данных:

1) организовать сбор и хранение в личных делах сотрудников обязательств сотрудников государственного автономного учреждения здравоохранения "Стоматологическая поликлиника №2" министерства здравоохранения Краснодарского края (далее – Учреждение), непосредственно осуществляющих обработку персональных данных, в случае расторжения с ними трудового договора прекратить обработку персональных данных, ставшие известные им в связи с исполнением должностных обязанностей;

2) организовать сбор и хранение в личных делах сотрудников Учреждения согласий на обработку персональных данных, иных субъектов персональных данных;

3) в случаях, когда предоставление персональных данных является обязательным в соответствии с федеральным законом и (или) постановлением Правительства Российской Федерации, организовать процедуру разъяснения субъекту персональных данных юридических последствий отказа предоставления своих персональных данных;

4) провести оценку возможного вреда, который может быть причинён субъектам персональных данных, в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых Учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

5) организовать проведение первичного инструктажа и (или) обучение по вопросам обработки персональных данных со всеми сотрудниками Учреждения, непосредственно осуществляющими обработку персональных данных;

6) организовать проведение первичного инструктажа и (или) обучение по вопросам обработки персональных данных со всеми принимаемыми на работу сотрудниками, в должностные инструкции которых будет входить обработка персональных данных;

7) организовать проведение внепланового инструктажа и (или) обучение по вопросам обработки персональных данных с сотрудниками Учреждения, непосредственно осуществляющими обработку персональных данных, при значительных изменениях законодательства Российской Федерации, регулирующего сферу взаимоотношений, возникающих при обработке персональных данных, в том числе требований к защите персональных данных, документов, определяющих политику Учреждения в отношении обработки персональных данных, локальных актов. Решение о необходимости внепланового инструктажа принимает ответственный за организацию обработки персональных данных Учреждения в каждом отдельном случае;

8) обеспечить контроль ведения и хранение журнала ознакомления и (или) обучения. Хранение журнала осуществлять в местах, исключающих доступ к журналу посторонних лиц. Хранить журнал в течение 5 лет после завершения ведения.

4. Назначить ответственным за обеспечение безопасности информационных систем (далее – Администратор информационной безопасности) из числа сотрудников государственного автономного учреждения здравоохранения "Стоматологическая поликлиника №2" министерства здравоохранения Краснодарского края специалиста по защите информации в компьютерных системах и сетях Тосунова А.С.

5. Назначить ответственным за техническое обслуживание информационных систем из числа сотрудников государственного автономного учреждения здравоохранения "Стоматологическая поликлиника №2" министерства здравоохранения Краснодарского края начальника отдела информационных технологий Линиченко С.Н.

6. Администратору информационной безопасности:

1) участвовать в проведении классификации и (или) установлении уровня защищённости информации, содержащиеся в информационных системах Учреждения;

2) определить актуальные угрозы безопасности информации и разработать «Модель угроз безопасности информации в информационных системах», а также, в случае необходимости, её согласование с регуляторами в области информационной безопасности (в пределах их компетенций). В случае применения средств криптографической защиты информации в информационных системах, разработать совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определить на этой основе и с учётом типа актуальных угроз требуемый класс средств криптографической защиты информации («Модель нарушителя»);

3) организовать учёт машинных носителей информации;

4) организовать проведение инструктажей сотрудников, работающих с защищаемой информацией в информационных системах (далее – Пользователи ИС), по темам: правила работы в информационных системах, защита информации в информационной системе, положения законодательства в сфере защиты информации, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников Учреждения в вопросах информационной безопасности;

5) организовать доступ Пользователей ИС к ресурсам информационных систем, в соответствии с утвержденным главным врачом перечнем лиц, допущенных к работе с информационными системами. Блокировать учётные записи, вносить изменения в полномочия и добавлять новых Пользователей ИС;

6) оказывать помощь Пользователям ИС, в части применения средств защиты от несанкционированного доступа и других средств защиты, входящих в состав информационных систем;

7) участвовать в составе постоянно действующей комиссии по реагированию на инциденты информационной безопасности, расследованиях причин инцидентов безопасности и внесение по результатам таких расследований предложений по совершенствованию систем безопасности.

7. Назначить комиссию по установлению уровня защищённости персональных данных в информационных системах персональных данных в составе, согласно приложению 4 к настоящему приказу.

8. Комиссии по установлению уровня защищённости персональных данных в информационных системах персональных данных в своей работе руководствоваться требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». В месячный

срок, с даты подписания данного приказа, а также, при изменении состава и (или) условий обработки персональных данных в информационных системах, комиссия предоставляет главному врачу на утверждение по результатам работ акты об установлении уровня защищённости персональных данных в информационных системах персональных данных Учреждения.

9. Назначить комиссию по классификации государственных и (или) муниципальных информационных систем по требованиям защиты информации, не составляющей государственную тайну в составе, согласно приложению 5 к настоящему приказу.

10. Комиссии по классификации государственных и (или) муниципальных информационных систем по требованиям защиты информации, не составляющей государственную тайну в своей работе руководствоваться приложением 1 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденный приказом ФСТЭК России от 11 февраля 2013 г. № 17. При обработке в государственной (муниципальной) информационной системе информации, содержащей персональные данные, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». В месячный срок, с даты подписания данного приказа, а также, при изменении состава и (или) условий обработки информации в информационных системах, комиссия предоставляет главному врачу на утверждение по результатам работ акты о классификации государственных и (или) муниципальных информационных систем Учреждения.

11. Для анализа инцидентов информационной безопасности, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий, планирования и принятия мер по предотвращению повторного возникновения инцидентов, назначить постоянно действующую комиссию по работе с инцидентами в составе, согласно приложению 6 к настоящему приказу.

12. Председателю комиссии по работе с инцидентами информационной безопасности:

1) председателю и постоянно действующей комиссии по работе с инцидентами в своей работе руководствоваться «Положением по работе с инцидентами информационной безопасности» Учреждения;

2) при необходимости привлекать к работе с комиссией сотрудников Учреждения, а также определять необходимость и выступать с инициативой о привлечении третьих лиц, не являющихся сотрудниками Учреждения, к работе с данной комиссией;

3) регистрировать в соответствующем журнале все инциденты информационной безопасности. Допускается ведение журнала в электронном виде;

4) обеспечить хранение журнала в местах, исключающих к нему доступ посторонних лиц. Хранить журнал в течение 5 лет после завершения ведения.

13. Назначить комиссию по уничтожению персональных данных субъектов персональных данных, согласно приложению 7 к настоящему приказу.

Комиссии по уничтожению персональных данных субъектов персональных данных руководствоваться требованиями, указанными в приложении 1 к настоящему приказу и утверждённым приказом Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций № 179 от 28 октября 2022 г. «Об утверждении Требований к подтверждению уничтожения персональных данных».

14. Назначить комиссию по оценке вреда субъектам персональных данных в составе, согласно приложению 8 к настоящему приказу.

Комиссии по оценке вреда субъектам персональных данных руководствоваться требованиями, утверждённые приказом Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций № 178 от 27 октября 2022 г. «Об утверждении Требований к оценке вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

15. Контроль за выполнением настоящего приказа оставляю за собой.

16. Приказ вступает в силу со дня его подписания.

Главный врач



В.Н. Жигаленко