

УТВЕРЖДЕНО

Приказом ГБУ КО «РЦЦ»

от « 16 » июня 2023 г.

№ 115

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных в
государственном бюджетном учреждении Калининградской области
«Региональный перинатальный центр»

г. Калининград
2023 г.

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в государственном бюджетном учреждении Калининградской области «Региональный перинатальный центр» определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн). Настоящие Правила разработаны в соответствии с:

- Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных»;
- 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»;
- Приказом ФСТЭК России №17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах»;
- Приказом ФСТЭК России №21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Внутренний контроль в государственном бюджетном учреждении Калининградской области «Региональный перинатальный центр» может осуществляться:

- Ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – Ответственный за обеспечение безопасности ПДн в ИСПДн);
- Ответственным за организацию обработки ПДн;
- Комиссией по обеспечению защиты персональных данных в государственном бюджетном учреждении Калининградской области «Региональный перинатальный центр» (далее – Комиссия);
- организациями, имеющими лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

1.3. Формы внутреннего контроля:

– текущий контроль, осуществляемый Ответственным за организацию обработки ПДн и Ответственным за обеспечение безопасности ПДн в ИСПДн;

– периодический контроль, осуществляемый Комиссией;

– внеплановый контроль, осуществляемый Комиссией;

– комплексный контроль над выполнением установленных требований к защите персональных данных, организусмый государственным бюджетным учреждением Калининградской области «Региональный перинатальный центр» и проводимый организацией, имеющей лицензию ФСТЭК на осуществление деятельности по технической защите конфиденциальной информации.

1.4. Проверки, проводимые в рамках внутреннего контроля соответствия обработки персональных данных установленным требованиям, в государственном бюджетном учреждении Калининградской области «Региональный перинатальный центр» (далее – проверки) могут быть плановые и внеплановые.

1.4.1 Плановые проверки проводятся на основании утвержденного главным врачом государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр» ежегодного Плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям (Приложение №1).

1.4.2 Внеплановые проверки проводятся на основании решения Комиссии, которое может быть принято в следующих случаях:

– по результатам расследования инцидента информационной безопасности;

– по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

– выявления фактов незаконного разглашения (распространения) персональных данных.

Внеплановые проверки также проводятся на основании поступившего в государственном бюджетном учреждении Калининградской области «Региональный перинатальный центр» письменного заявления субъекта ПДн о нарушениях правил обработки персональных данных. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

2. Порядок проведения плановых и внеплановых проверок

2.1. Для проведения плановых проверок лицо, ответственное за организацию обработки ПДн, разрабатывает План осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям на текущий год (далее – План осуществления внутреннего контроля), который согласовывается с Комиссией и утверждается главным врачом.

2.2. Общий срок проведения проверки не должен превышать пятнадцати рабочих дней. При необходимости срок проведения проверки может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных проверок.

2.3. Плановые и внеплановые проверки проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн в ИСПДн.

2.4. Ответственный за обеспечение безопасности ПДн в ИСПДн не позднее чем за три рабочих дня до начала проведения проверки уведомляет всех работников, допущенных к обработке ПДн, и направляет им для ознакомления План осуществления внутреннего контроля. При проведении внеплановых проверок уведомление не требуется.

2.5. В целях осуществления внутреннего контроля, в зависимости от его целей, могут выполняться следующие проверки:

- соответствие полномочий пользователя ИСПДн утвержденным правилам доступа;
- соблюдение пользователями ИСПДн требований Регламента по обеспечению информационной безопасности персональных данных в информационных системах персональных данных;
- соблюдение Инструкции о порядке доступа в помещения, в которых осуществляется обработка персональных данных;
- порядок и условия применения средств защиты информации;
- состояние учета машинных носителей персональных данных;
- наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.
- проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- технические мероприятия, связанные с штатным и нештатным функционированием средств защиты;

- технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации;
- соблюдение пользователями информационных систем персональных данных правил работы со съёмными носителями персональных данных;
- соблюдение правил хранения и работы с бумажными носителями персональных данных.

2.6. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

2.7. Проверки могут осуществляться как непосредственно на рабочих местах исполнителей, участвующих в обработке персональных данных, так и путем направления запросов и рассмотрения документов, необходимых для осуществления внутреннего контроля.

2.8. Проверка должна быть завершена не позднее чем через 15 рабочих дней с даты начала проверки.

3. Права и обязанности лиц, осуществляющих внутренний контроль

3.1. Права Ответственного за организацию обработки ПДн, Ответственного за обеспечение безопасности ПДн в ИСПДн и Комиссии при проведении внутреннего контроля:

- запрашивать у руководителя информацию и (или) документы, необходимые для осуществления внутреннего контроля;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить главному врачу государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр» предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить главному врачу предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

3.2. Лица, осуществляющие внутренний контроль, должны обеспечивать конфиденциальность ставших им известными в ходе проведения мероприятий внутреннего контроля персональных данных. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

4. Результат проведения внутреннего контроля

4.1. По итогам проведения плановых и внеплановых контрольных мероприятий лицо (Комиссия) разрабатывает отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- заключение по итогам проведения внутреннего контрольного мероприятия.

4.2. Отчет передается на рассмотрение главному врачу государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр».

4.3. Результаты проведенных проверок оформляются в виде Акта внутреннего контроля (Приложение № 2), который подписывается членами Комиссии.

4.4. Мероприятия по контролю над соблюдением режима защиты персональных данных фиксируются в Журнале (Приложение 3).

4.5. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости председатель Комиссии докладывает главному врачу.

Приложение № 1

к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите персональных
данных

ПЛАН

осуществления внутреннего контроля соответствия обработки
персональных данных установленным требованиям в
государственном бюджетном учреждении Калининградской области
«Региональный перинатальный центр»

№	Тема проверки	Нормативный правовой документ, предъявляющий требования	Срок проведения	Исполнитель

Приложение № 2
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите персональных
данных

Акт
внутреннего контроля соответствия обработки персональных данных
требованиям к защите персональных данных в
государственном бюджетном учреждении Калининградской области
«Региональный перинатальный центр»

Предмет контроля:

Выявленные нарушения:

Меры по устранению нарушений:

Предложения комиссии:

Подписи членов комиссии:

_____	_____
(подпись)	(фамилия, имя, отчество)
_____	_____
(подпись)	(фамилия, имя, отчество)
_____	_____
(подпись)	(фамилия, имя, отчество)

Приложение №3

к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям к защите
персональных данных

ЖУРНАЛ

учета мероприятий по контролю над соблюдением режима защиты персональных данных в
государственном бюджетном учреждении Калининградской области «Региональный перинатальный центр»

№ п/п	Мероприятие	Дата	Исполнитель	Результат