

УТВЕРЖДЕНЫ
приказом ГБУСО «ЦМиРАД»
от «15» января 2024 г. № 02-3-04/1/22
с изменением утвержденным
приказом от «08» августа 2025 г.
№ 02-3-04/22/1

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

Екатеринбург
2025

Оглавление

1. Общие положения	3
2. Основания проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных	4
3. Порядок осуществления внутреннего контроля	4
4. Права комиссии по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.....	9
5. Ответственность	10
Приложение №1	11

1. Общие положения

1.1. Государственное бюджетное учреждение Свердловской области «Центр микрографии и реставрации архивных документов Свердловской области» (далее – Организация) руководствуется настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила), определяющими основания и порядок осуществления внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» принятыми в соответствии с ним: нормативно-правовым актом, требованиям к защите персональных данных, к Политике Организации в отношении обработки персональных данных, к локальным актам Организации.

1.2. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.3. Перечень нормативных правовых актов, на основании которых разработаны Правила:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

- постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – постановление Правительства РФ № 687);

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационной системе персональных данных» (далее – постановление Правительства РФ № 1119);

- приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных с использованием средств криптографической защиты информации, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных» (далее – приказ ФСТЭК России № 21).

- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»»;

- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;

- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 №180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»;

1.4. Работники, допущенные к обработке персональных данных в Организации в связи с необходимостью выполнения ими трудовых обязанностей, должны быть ознакомлены с настоящими Правилами под роспись до начала обработки персональных данных. Обязанность по организации ознакомления указанных работников с настоящими Правилами возлагается на ответственного за организацию обработки персональных данных.

2. Основания проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. Основаниями для проведения внутреннего контроля являются требования пункта 4 части 1 статьи 18.1., пункта 1 части 4, статьи 22.1. Федерального закона № 152-ФЗ, пункта 17 требований к защите персональных данных при их обработке в информационной системе персональных данных (далее - требования), утвержденных постановлением Правительства РФ № 1119, ежегодный план внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных, утверждаемый руководителем Организации.

2.2. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) осуществляется в Организации путем проведения проверок соблюдения требований законодательства в сфере персональных данных и внутренних документов Организации по обработке и защите персональных данных.

2.3. Разработка проекта ежегодного плана внутренних проверок обеспечивается работником, ответственным за организацию обработки персональных данных.

3. Порядок осуществления внутреннего контроля

3.1. Внутренний контроль проводится самостоятельно Организацией и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.2. Для проведения внутреннего контроля в Организации создается комиссия по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Комиссия).

3.3. Состав Комиссии, состоящий из не менее трех работников Организации, утверждается приказом Организации.

3.4. Председателем Комиссии, как правило, назначается ответственный за организацию обработки персональных данных в Организации.

3.5. В состав Комиссии также входят администратор информационной безопасности информационной системы (систем) персональных данных и работник кадрового аппарата Организации.

3.6. Все члены комиссии при принятии решения обладают равными правами.

3.7. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения внутреннего контроля, обеспечивают конфиденциальность персональных данных субъектов персональных данных.

3.8. Комиссия при проведении проверки обязана:

3.8.1. Провести анализ реализации мер, направленных на обеспечение выполнения Организацией обязанностей, предусмотренных статьями 18.1, 19 Федерального закона № 152-ФЗ и принятыми в соответствии с ним локальными актами в отношении обработки персональных данных, и проверить:

- наличие актуального приказа о назначении лица, ответственного за организацию обработки персональных данных в Организации, утвержденной инструкции ответственного за организацию обработки персональных данных в Организации, а также внесение соответствующих дополнений в должностную инструкцию работника, назначенного ответственным за организацию обработки персональных данных в Организации;

- актуальность уведомления о намерении осуществлять обработку персональных данных, направленного в уполномоченный орган по защите прав субъектов персональных данных;

- актуальность политики в отношении обработки персональных данных в Организации (далее - Политика) и обеспечение неограниченного доступа к Политике и сведениям о реализуемых требованиях к защите персональных данных, в том числе размещение их на официальном сайте Организации в информационно-телекоммуникационной сети;

- наличие и актуальность Перечня персональных данных по каждой категории персональных данных, обрабатываемых в Организации, и Перечня информационных систем персональных данных в Организации;

- наличие правовых оснований для обработки персональных данных по каждой категории субъектов персональных данных, независимо от способа обработки персональных данных;

- соответствие целей обработки персональных данных содержанию и объему обрабатываемых персональных данных, независимо от способа их обработки;

- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения Организацией обязанностей, предусмотренных Федеральным законом № 152-ФЗ. В

случае необходимости по результатам проверки оценки вреда оформляется соответствующий акт, форма которого утверждается приказом Организации;

- ознакомление работников (документально подтвержденное), непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальными актами по вопросам обработки и обеспечения безопасности персональных данных;

- соответствие установленных прав доступа к персональным данным в информационной системе (системах) персональных данных трудовым обязанностям работников Организации;

- наличие и полноту заполнения работниками Организации обязательств о соблюдении конфиденциальности персональных данных, документа об информировании о факте обработки персональных данных без использования средств автоматизации, разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

- наличие согласий субъектов персональных данных на обработку персональных данных и разъяснений субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в случаях, когда этого требует законодательство Российской Федерации;

- наличие и ведение Журнала обращений субъектов персональных данных и представителей субъектов персональных данных, соблюдения процедур и сроков подготовки ответов на обращения субъектов персональных данных, а также учета предоставления персональных данных субъектам персональных данных по письменным запросам третьих лиц в порядке, установленном действующим законодательством Российской Федерации;

- наличие (в случае заключения соответствующего договора) в поручении на обработку персональных данных: перечня действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанности соблюдения конфиденциальности персональных данных, обеспечения безопасности персональных данных при их обработке, а также требований к защите обрабатываемых персональных данных со статьей 19 Федерального закона № 152-ФЗ;

- актуальность Перечня мест хранения материальных носителей персональных данных и обеспечение контроля хранения материальных носителей персональных данных в условиях, исключающих несанкционированный доступ к ним, а также обеспечение раздельного хранения персональных данных в случаях их обработки без использования средств автоматизации при несовместимости целей обработки персональных данных;

- соблюдение сроков хранения и порядка уничтожения материальных носителей персональных данных, а также персональных данных на носителях информации;

- актуальность организационно-распорядительных документов по вопросам обработки персональных данных.

3.8.2. Проанализировать выполнение в Организации требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства РФ № 1119, и проверить:

- соответствие указанных в утвержденном Перечне обрабатываемых персональных данных в информационной системе персональных данных категорий персональных данных, категорий субъектов персональных данных и количества субъектов персональных данных, фактически обрабатываемых в информационной системе персональных данных;

- соответствие фактического типа актуальных угроз безопасности персональных данных в информационной системе персональных данных с учетом оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, типу актуальных угроз безопасности персональных данных, указанному в утвержденном руководителем Организации Акте классификации информационной системы персональных данных (в случае, если проводились работы по аттестации информационной системы персональных данных) либо в акте определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных (в случае, если работы по аттестации информационной системы персональных данных не проводились);

- назначение работника, ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;

- соответствие Перечня помещений, в которых размещена информационная система персональных данных, утвержденного в Организации, фактическому размещению оборудования информационной системы персональных данных, включая средства защиты информации;

- соответствие перечня лиц, имеющих доступ к персональным данным в связи с исполнением своих должностных обязанностей, перечню лиц, имеющих доступ в помещения, в которых размещена информационная система персональных данных, утвержденному в Организации, фактически находящимся в указанных помещениях на момент проверки;

- фактическое выполнение организационных и технических мер по обеспечению безопасности помещений, в которых размещена информационная система персональных данных, препятствующих возможности неконтролируемого проникновения или пребывания в указанных помещениях лиц, не имеющих права доступа в них (при наличии - фактическое опечатывание входных дверей указанных помещений, применение систем контроля и управления доступом, средств охранной сигнализации, систем видеонаблюдения, оборудование оконных проемов первых и

последних этажей здания, где размещено оборудование информационной системы персональных данных, запирающимися ставнями и т.д.);

- наличие сертификатов соответствия требованиям безопасности информации на все используемые средства защиты информации, фактически используемые в Организации;

- обеспечение сохранности машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные в информационной системе персональных данных путем проведения сверки соответствия количества учтенных носителей фактическому, а также сверки заводских и учетных номеров, фактической проверки условий хранения и использования машинных носителей персональных данных.

3.8.3. Проанализировать состояние работы в Организации по реализации Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных, утвержденных приказом ФСТЭК России № 21 и проверить:

- фактическую реализацию установленного в Организации порядка идентификации и аутентификации пользователей информационной системы персональных данных;

- реализацию процесса управления доступом к ресурсам информационной системы персональных данных;

- регистрацию событий информационной безопасности в информационной системе персональных данных в соответствии с Инструкцией по управлению событиями информационной безопасности;

- реализацию выявления инцидентов информационной безопасности и реагирования на них при наличии запланированных работ по аттестации информационной системы персональных данных;

- организацию антивирусной защиты в информационной системе персональных данных и регулярность обновления базы данных признаков вредоносных программ (вирусов);

- реализацию выявления, анализа и устранения уязвимостей в информационной системе персональных данных при наличии запланированных работ по проведению аттестации информационной системы персональных данных;

- установку обновлений программного обеспечения, в том числе обновление программного обеспечения средств защиты информации;

- наличие проверок настройки правильности функционирования программного обеспечения и средств защиты информации в информационной системе персональных данных;

- организацию физического доступа к техническим средствам, средствам защиты информации информационной системы персональных данных, (в том числе опечатывание корпуса средств вычислительной техники);

- организацию размещения технических средств отображения информации информационных систем персональных данных, исключая ее несанкционированный просмотр;

- состав технических средств, программного обеспечения и средств защиты информации, входящих в состав информационной системы, на соответствие Техническому паспорту информационной системы в случае, если запланировано проведение работ по аттестации информационной системы персональных данных;

- реализацию процесса управления конфигурацией информационной системы персональных данных и системы защиты персональных данных в случае, если запланировано проведение работ по аттестации информационной системы персональных данных.

4. Права комиссии по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

4.1. Комиссия при проведении проверки вправе:

- запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;

- получать в соответствии с Инструкцией пользователей информационной системы персональных данных временный доступ к ресурсам информационной системы персональных данных, в части касающейся ее полномочий;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;

- вносить руководителю Организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите персональных данных, установленных нормативными правовыми актами Российской Федерации.

4.2. При проведении проверки члены Комиссии не вправе:

- требовать представления документов и сведений, не относящихся к предмету проверки;

- распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

4.3. По результатам проверки составляется Акт проверки, который подписывается всем составом комиссии и представляется руководителю Организации для принятия соответствующего решения. В Организации разработана и используется специальная форма соответствующего Акта (Приложение №1).

4.4. В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации в области защиты персональных данных, об их характере и о лицах, допустивших указанные нарушения.

4.5. Акт должен содержать заключение о соответствии или несоответствии обработки персональных данных требованиям к защите персональных данных и Политике Организации в отношении обработки персональных данных, установленным Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Заключение о соответствии должно быть сформулировано для информационной системы персональных данных.

5. Ответственность

5.1. Работники Организации несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами в соответствии с законодательством Российской Федерации.

Приложение №1
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных
в ГБУСО «ЦМиРАД»

Акт № _____
проведения внутренней проверки условий
обработки персональных данных в ГБУСО «ЦМиРАД»

Дата составления: «___» _____ 20___ г.

Место проведение проверки: _____

Комиссия, назначенная приказом руководителя от «___» _____ 20___ № _____ в составе:
Председатель:

_____ (Ф.И.О.)

Члены комиссии:

_____ (Ф.И.О.)

_____ (Ф.И.О.)

руководствуясь «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, Политикой Государственное бюджетное учреждение Свердловской области «Центр микрографии и реставрации архивных документов Свердловской области» (далее – ГБУСО «ЦМиРАД») в отношении обработки персональных данных», провела проверку условий обработки персональных данных в ГБУСО «ЦМиРАД».

В ходе проверки:

- проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных статьями 18.1, 19 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и, принятыми в соответствии с ним, локальными актами ГБУСО «ЦМиРАД», определяющими его Политику в отношении обработки персональных данных;
- проведен анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационной системе персональных данных»;
- проведен анализ реализации в ГБУСО «ЦМиРАД» организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных»;
- проведен анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы.

Выявленные нарушения: _____

ЗАКЛЮЧЕНИЕ комиссии:

Обработка персональных данных соответствует (не соответствует) *(нужное подчеркнуть)* требованиям к защите персональных данных и политике организации в отношении обработки персональных данных, установленным Федеральным законом Российской Федерации от 27 июля 2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Председатель комиссии _____ (подпись)

Члены комиссии: _____ (подпись)

_____ (подпись)

УПРАВЛЕНИЕ АРХИВАМИ СВЕРДЛОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ СВЕРДЛОВСКОЙ ОБЛАСТИ
«ЦЕНТР МИКРОГРАФИИ И РЕСТАВРАЦИИ АРХИВНЫХ ДОКУМЕНТОВ
СВЕРДЛОВСКОЙ ОБЛАСТИ»

ПРИКАЗ

11.08.2025

№ 02-3-04/22/2

г. Екатеринбург

**О создании комиссии по осуществлению внутреннего контроля соответствия
обработки персональных данных требованиям к защите персональных
данных**

В целях принятия мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», в том числе выполнения требований к защите персональных данных, установленных Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119,

ПРИКАЗЫВАЮ:

1. Создать комиссию для проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в составе:

Председатель комиссии:

– Полушкина С. Е. – главный бухгалтер-начальник отдела ФЭРБУКиДО.

Члены комиссии:

– Абрамова А. В. – документовед отдела ФЭРБУКиДО;

– Крутиков И. А. – ведущий специалист по защите информации;

2. Комиссии в своей работе руководствоваться требованиями к защите персональных данных при их обработке в информационных системах персональных данных.

3. Комиссии по результатам работ в срок до 28.08.2025 года предоставить на утверждение директору акты установления уровня защищенности персональных данных в информационных системах.

4. Контроль за исполнением приказа оставляю за собой.

Директор

Ю. В. Демина

Акт № 1
проведения внутренней проверки условий
обработки персональных данных в ГБУСО «ЦМиРАД»

Дата составления: «27» августа 2025 г.

Место проведения проверки: г. Екатеринбург, ул. Артинская, д. 4, ГБУСО «ЦМиРАД»

Комиссия, назначенная приказом руководителя от «11» августа 2025 № 02-3-04/22/2
в составе:

Председатель:

Полушкина Светлана Евгеньевна – главный бухгалтер-начальник отдела финансово-экономической работы, бухгалтерского учета, кадрового и документационного обеспечения

Члены комиссии:

Абрамова Анастасия Владимировна – документовед

Крутиков Игорь Андреевич – ведущий специалист по защите информации

руководствуясь «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, Политикой Государственное бюджетное учреждение Свердловской области «Центр микрографии и реставрации архивных документов Свердловской области» (далее – ГБУСО «ЦМиРАД») в отношении обработки персональных данных», провела проверку условий обработки персональных данных в ГБУСО «ЦМиРАД».

В ходе проверки:

- проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных статьями 18.1, 19 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и, принятыми в соответствии с ним, локальными актами ГБУСО «ЦМиРАД», определяющими его Политику в отношении обработки персональных данных;
- проведен анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационной системе персональных данных»;
- проведен анализ реализации в ГБУСО «ЦМиРАД» организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных»;

- проведен анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы.

Выявленные нарушения: нарушений, установленных законодательством и локальными нормативными актами не выявлено.

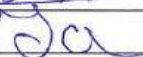
ЗАКЛЮЧЕНИЕ комиссии:

Обработка персональных данных соответствует требованиям к защите персональных данных и политике организации в отношении обработки персональных данных, установленным Федеральным законом Российской Федерации от 27 июля 2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Председатель комиссии

 (подпись)

Члены комиссии:

 (подпись)
 (подпись)