Республика Карелия
Муниципальное учреждение Петрозаводского городского округа
«Централизованная бухгалтерия №1 г. Петрозаводска»

П Р И К А З

«23» 01 2026 г. № 36

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 муниципальном бюджетном учреждении Петрозаводского городского округа "Централизованная бухгалтерия № 1" (приложение 1);

2) Функциональные обязанности администратора информационной безопасности муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1" (приложение 2);

3) Функциональные обязанности администратора информационных систем муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1" (приложение 3);

2. Назначить ответственным за организацию обработки персональных данных из числа сотрудников муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1" руководителя Бойцову Л.Б.

3. Ответственному за организацию обработки персональных данных:

1) организовать сбор и хранение в личных делах сотрудников обязательств сотрудников муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1" (далее – Организация), 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 Организации 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 Организацией 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 Организации, 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 Организации, 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 Организации в отношении обработки персональных данных, локальных актов. Решение о необходимости внепланового инструктажа принимает ответственный за организацию обработки персональных данных Организации 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 муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1" системного администратора БалатаеваР.В.

5. Назначить ответственным за техническое обслуживание информационных систем из числа сотрудников муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1" системного администратора Балатаева Р.В.

6. Администратору информационной безопасности:

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

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 Организации в вопросах информационной безопасности;

5) организовать доступ Пользователей ИС к ресурсам информационных систем, в соответствии с утвержденным руководителем 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 руководителю на утверждение по результатам работ

акты об установлении уровня защищённости персональных данных в информационных системах персональных данных Организации.

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 руководителю на утверждение по результатам работ акты о классификации государственных и (или) муниципальных информационных систем Организации.

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» Организации;

2) при необходимости привлекать к работе с комиссией сотрудников Организации, а также определять необходимость и выступать с инициативой о привлечении третьих лиц, не являющихся сотрудниками Организации, 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. Контроль за выполнением настоящего приказа оставляю за собой.

15. Приказ вступает в силу со дня его подписания.

Руководитель Л.Б. Бойцова

Составитель проекта:

Системный администратор (подпись) Р.В. Балатаев

Приложение 1

УТВЕРЖДЕНА
приказом МУ "ЦБ № 1"
от 23.01.2026 № 36

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в муниципальном бюджетном учреждении Петрозаводского городского округа "Централизованная бухгалтерия № 1"

1. Общие положения

Ответственный за организацию обработки персональных данных (далее – Ответственный) является сотрудником муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1" (далее – Организация).

Ответственный назначается приказом руководителя.

Ответственный в вопросах организации обработки персональных данных (далее – ПДн) подчиняется непосредственно руководителю и проводит мероприятия по защите ПДн в интересах Организации.

Ответственный в своей деятельности руководствуется:

1) Конституцией Российской Федерации;

2) федеральными законами Российской Федерации и нормативными правовыми актами органов государственной власти по вопросам защиты ПДн;

3) государственными стандартами Российской Федерации в области защиты информации;

4) руководящими и нормативными правовыми документами Федеральной Службы по техническому и экспортному контролю России;

5) локальными нормативными актами Организации по защите ПДн;

6) правилами внутреннего трудового распорядка.

Деятельность Ответственного осуществляется согласно утвержденного руководителем «Плана мероприятий по защите ПДн Организации» на год. «План мероприятий по защите ПДн Организации» разрабатывается на каждый календарный год.

2. Задачи

На Ответственного возложены следующие задачи:

1) организация внутреннего контроля за соблюдением сотрудниками Организации соответствия обработки ПДн требованиям к защите ПДн, установленные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), принятыми в соответствии с ним нормативными правовыми актами и локальными актами Организации;

2) разработка, внедрение и актуализация локальных актов по вопросам обработки ПДн;

3) доведение до сведения сотрудников Организации, непосредственно осуществляющих обработку ПДн, положений законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн, и проведение обучения указанных сотрудников;

4) осуществление контроля приёма и обработки обращений или запросов субъектов ПДн или их представителей по вопросам обработки ПДн и внесение предложений по организации приёма и обработки таких обращений или запросов;

5) осуществление рассмотрения обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и организация предоставления субъектам ПДн или их представителям информации, предусмотренной Федеральным законом № 152-ФЗ;

6) организация комплексной защиты объектов информатизации Организации, а именно:

а) информационных ресурсов, представленных в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащих ПДн субъектов Организации;

б) средств и систем информатизации (средств вычислительной техники, информационно-вычислительных комплексов, локальных вычислительных сетей и корпоративных информационных систем), программных средств (операционных систем, систем управления базами данных, другого общесистемного и прикладного программного обеспечения), автоматизированных систем управления информационными, управленческими и технологическими процессами, систем связи и передачи данных, технических средств приёма, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорных устройств и других технических средств обработки графической, смысловой и буквенно-цифровой

информации), используемых для реализации процессов ведения деятельности, обработки информации, содержащей ПДн субъектов Организации.

7) организация защиты ПДн субъектов Организации;

8) разработка и проведение организационных мероприятий, обеспечивающих безопасность объектов защиты Организации, своевременное выявление и устранение возможных каналов утечки информации;

9) организация проведения работ по технической защите информации на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций Организации;

10) реализация технических мер, обеспечивающих своевременное выявление возможных технических каналов утечки информации в структурных подразделениях (отделах) Организации;

11) методическое руководство системой обеспечения информационной безопасности Организации;

12) организация контроля состояния и проведение оценки эффективности системы обеспечения информационной безопасности ПДн, а также реализация мер по её совершенствованию;

13) внедрение в информационную инфраструктуру Организации современных методов и средств обеспечения информационной безопасности .

3. Функции

Для решения поставленных задач Ответственный осуществляет следующие функции:

1) участие в разработке и внедрении правовых, организационных и технических мер по комплексному обеспечению безопасности ПДн;

2) контроль обеспечения соблюдения режима конфиденциальности при обработке ПДн и внесение предложений по соблюдению такого режима;

3) разработка планов по защите ПДн на объектах Организации;

4) контроль выполнения мер по защите ПДн, анализ материалов контроля, выявление недостатков и нарушений. Разработка и реализация мер по их устранению;

5) обеспечение взаимодействия с контрагентами по вопросам организации и проведения проектно-изыскательских, научно-исследовательских, опытно-конструкторских и других работ по защите информации. Участие в разработке технических заданий на выполняемые исследования и работы;

6) контроль выполнения плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите ПДн, выполняемых контрагентами;

7) разработка и внесение предложений по обеспечению финансирования работ по защите ПДн, в том числе выполняемых по договорам (контрактам);

8) участие в проведении работ по технической защите информации на объектах информатизации Организации. Оценка эффективности принятых мер по технической защите информации;

9) внесение предложений по обеспечению выбора, установке, настройке и эксплуатации средств защиты информации в соответствии с организационно-распорядительной и эксплуатационной документацией;

10) контроль организации режима обеспечения безопасности помещений, в которых происходит обработка ПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в такие помещения, а также внесение предложений по обеспечению безопасности таких помещений;

11) участие в организации доступа сотрудников Организации к ПДн в соответствии с возложенными на них должностными обязанностями и подготовка предложений по организации такого доступа;

12) разработка и внедрение локальных актов, определяющих перечень сотрудников Организации, имеющих доступ к ПДн;

13) контроль размещения устройств ввода (отображения) информации, исключающего её несанкционированный просмотр;

14) проведение оценки вреда, который может быть причинён субъекту(-ам) ПДн в случае нарушения законодательства по защите ПДн;

15) участие в разработке и реализации политики по работе с инцидентами информационной безопасности в части обработки ПДн;

16) внесение предложений по актуализации внутренней организационно-распорядительной документации по защите ПДн при изменении существующих и выходе новых нормативных правовых документов по вопросам обработки ПДн и подготовка соответствующих необходимых проектов документов.

4. Права

Ответственный имеет право:

1) осуществлять контроль за деятельностью структурных подразделений (отделов) Организации по выполнению ими требований по защите ПДн;

2) составлять акты, докладные записки, отчёты для рассмотрения руководителем, при выявлении нарушений порядка обработки ПДн;

3) принимать необходимые меры при обнаружении несанкционированного доступа к ПДн, как сотрудниками Организации, так и третьими лицами, и докладывать о принятых мерах руководителю с предоставлением информации о субъектах, нарушивших режим доступа;

4) вносить на рассмотрение руководителю предложения, акты, заключения о приостановлении работ, в случае обнаружения каналов утечки (или предпосылок к утечке) информации ограниченного доступа;

5) давать структурным подразделениям (отделам) Организации, а также отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного;

6) запрашивать и получать от всех структурных подразделений (отделов) Организации сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного;

7) составлять акты и другую техническую документацию о степени защищённости объекта(-ов) информатизации;

8) готовить и вносить предложения: на проведение работ по защите ПДн; о привлечении к проведению работ по оценке эффективности защиты ПДн на объекте(-ах) Организации (на договорной основе) учреждений и организаций, имеющих лицензию на соответствующий вид деятельности; о закупке необходимых технических средств защиты и другой спецтехники, имеющих в обязательном порядке сертификат соответствия;

9) осуществлять визирование договоров (контрактов) с контрагентами с целью правового обеспечения передачи им ПДн субъектов Организации в ходе выполнения работ по этим договорам (контрактам);

10) представлять интересы Организации при осуществлении государственного контроля и надзора за обработкой ПДн Уполномоченным органом по защите прав субъектов ПДн.

5. Взаимоотношения (служебные связи)

Ответственный выполняет свои задачи осуществляя взаимодействие со всеми структурными подразделениями (отделами) Организации.

Для выполнения своих функций и реализации предоставленных прав, Ответственный взаимодействует с территориальными и региональными подразделениями Федеральной службы по техническому и экспортному контролю России, Федеральной службы безопасности России, Федеральной

службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерства внутренних дел Российской Федерации и другими представителями исполнительной власти Российской Федерации и организациями, предоставляющие услуги и работы в области защиты ПДн на законном основании.

6. Ответственность

Ответственный несёт ответственность за надлежащее и своевременное выполнение возложенных задач и функций по организации обработки ПДн в Организации, в соответствии с положениями законодательства Российской Федерации в области ПДн.

С должностной инструкцией ответственного за организацию обработки персональных данных ознакомлен(-а):

Бойцова Л.Б. (ФИО)	Бойцова (подпись)	«23» 01. 2026 г.
_____ (ФИО)	_____ (подпись)	«___» _____ 20___ г.
_____ (ФИО)	_____ (подпись)	«___» _____ 20___ г.

Приложение 2

УТВЕРЖДЕНЫ
приказом МУ "ЦБ № 1"
от 23.01.2026 № 36

ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ
администратора информационной безопасности муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1"

1. Общие положения

Настоящие функциональные обязанности разработаны на основе постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности (далее – Администратор ИБ).

Администратор ИБ является сотрудником муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1" (далее – Организация).

Администратор ИБ подчиняется непосредственно руководителю и отвечает за обеспечение конфиденциальности, целостности и доступности, обрабатываемой в информационных системах (далее – ИС) Организации конфиденциальной информации, в том числе и персональные данные (далее – ПДн), обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в ИС Организации.

Администратор ИБ является ответственным должностным лицом, уполномоченным за проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИС и её ресурсов на всех этапах жизненного цикла ИС.

Администратор ИБ осуществляет контроль выполнения требований по защите ИС в соответствии с требованиями действующих федеральных законов, общегосударственных, ведомственных, а также внутренних нормативных документов по вопросам защиты информации и обеспечивает их выполнение пользователями ИС.

Администратор ИБ осуществляет решение вопросов информационной безопасности дополнительно к своим непосредственным обязанностям.

В своей деятельности Администратор ИБ руководствуется настоящим документом, «Правилами обработки ПДн субъектов ПДн в Организации», «Политикой обработки ПДн Организации» и действующим законодательством в сфере защиты информации.

Администратор ИБ имеет право требовать от пользователей ИС выполнения указаний и инструкций, связанных с защитой информации в ИС.

Функциональные обязанности Администратора ИБ не регламентирует вопросы защиты и охраны зданий и помещений, в которых расположены ИС, вопросы обеспечения физической целостности компонентов ИС, защиты от стихийных бедствий (пожаров, наводнений и др.), сбоев в системе энергоснабжения, а также меры обеспечения безопасности сотрудников и меры, принимаемые при возникновении в ИС нештатных ситуаций.

2. Квалификационные требования

Администратор ИБ в своей работе руководствуется следующими нормативными документами Российской Федерации и организационно - распорядительной документацией Организации:

1) Федеральным законом № 149-ФЗ от 27 июля 2006 г. «Об информации, информатизации и защите информации»;

2) Федеральным законом № 152-ФЗ от 27 июля 2006 г. «О персональных данных»;

3) «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утверждённые постановлением Правительства РФ № 1119 от 1 ноября 2012 г.;

4) «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённые приказом ФСТЭК России № 21 от 18 февраля 2013 г.;

5) «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10 июля 2014 г.

3. Функциональные обязанности

В обязанности Администратора ИБ входит:

1) изучение особенностей бизнес-процессов и технологических процессов обработки информации в Организации с целью принятия решения о необходимости защиты информации в ИС;

2) классификация и (или) установление уровня защищённости информации, содержащейся в ИС, либо поиск специализированных организаций, производящих на договорной основе данные работы. В случае привлечения сторонних организаций, Администратор ИБ обязан сопровождать процесс сбора информации обо всех ИС работниками сторонней организации;

3) определение актуальных угроз безопасности информации и разработка документа «Модель угроз безопасности информации в ИС», а также, в случае необходимости, её согласование с регуляторами в области ИБ (в пределах их компетенций). В случае применения средств криптографической защиты информации (далее – СКЗИ) в ИС, необходима разработка совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учётом типа актуальных угроз требуемого класса СКЗИ («Модель нарушителя»), либо привлечение на договорной основе сторонних организаций, имеющих компетенции в данных вопросах;

4) пересмотр актуальных угроз безопасности информации необходимо проводить периодически в следующих случаях:

• ежегодный плановый пересмотр актуальных угроз безопасности информации;

• появление в общедоступных источниках информации о новых угрозах и уязвимостях, имеющих предпосылки в ИС, а также в банке данных угроз безопасности информации, расположенная на сайте ФСТЭК России (http://bdu.fstec.ru/);

• существенное изменение условий функционирования ИС, изменение технологического процесса обработки информации;

• изменение нормативной документации, касающейся моделирования угроз безопасности информации и нарушителя;

• в результате инцидента безопасности.

5) разработка проектной документации на систему защиты информации ИС, либо привлечение на договорной основе сторонних организаций (лицензиатов ФСТЭК России, ФСБ России) для данных работ;

6) участие в подготовке технических заданий для конкурсов и аукционов, связанных по вопросам информационной безопасности;

7) участие в разработке технологии обеспечения информационной безопасности Организации, предусматривающей порядок взаимодействия структурных подразделений (отделов) Организации по вопросам обеспечения безопасности при эксплуатации ИС и модернизации её программных и аппаратных средств. Рассматривать целесообразность применения новых технологий для повышения эффективности функционирования ИС;

8) сопровождение работ, связанных с реализацией проекта по защите информации ИС (тестирование системы защиты информации, внедрение системы защиты информации, аттестация ИС по требованиям к защите информации, ввод в действие аттестованной ИС);

9) установка и настройка средств защиты информации (далее – СЗИ), а также выполнение других возложенных на него работ в соответствии с распорядительными, инструктивными и методическими материалами, в части его касающейся;

10) осуществление контроля изменений (в том числе и несанкционированных) аппаратного обеспечения автоматизированных рабочих мест и серверов;

11) предотвращение несанкционированных модификаций программного обеспечения, добавления новых функций, несанкционированного доступа к защищаемой информации и другим общим ресурсам Организации;

12) информирование руководителя об уязвимых местах ИС, возможных путях несанкционированного доступа и воздействии на ИС Организации;

13) подготовка предложений руководителю по совершенствованию системы защиты информации в ИС Организации;

14) ведение учёта применяемых в ИС СЗИ, эксплуатационной и технической документации к ним;

15) знание состава, структуры, назначение выполняемых задач ИС, а также состава информационных технологий и технических средств, позволяющих осуществлять обработку конфиденциальной информации, в том числе и ПДн;

16) разработка и принятие мер по выполнению плана мероприятий по обеспечению безопасности защищаемой информации в ИС и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятий по мере необходимости;

17) хранение технического паспорта и аттестационной документации ИС, контроль конфигурации ИС и ведение учёта изменений аппаратно-программной конфигурации (архив документов, на основании которых были произведены данные изменения). При изменении условий обработки защищаемой информации, а также расположения и состава технических средств, состава программного обеспечения, физического и логического строения сети на аттестованной ИС, Администратор ИБ должен уведомить орган по аттестации (проводивший аттестационные испытания) о планируемых изменениях и получить согласование таких работ;

18) осуществление контроля физической сохранности и целостности технических средств ИС, а также контроль сохранности и целостности опечатывающих пломб на технических средствах ИС (в том числе и программно-аппаратных средствах защиты информации). Контроль неизменности состава технических средств в ИС;

19) организация учёта машинных носителей информации. Настройка соответствующих программных механизмов посредством средств защиты информации для запрета использования неучтённых машинных носителей, в том числе съёмных носителей. Ведение журнала учёта носителей;

20) проведение инструктажей сотрудников, работающих с защищаемой информацией в ИС (далее – Пользователи ИС), по темам: правила работы в ИС, защита информации и применяемые средства защиты в ИС, положения законодательства в сфере защиты информации, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников Организации в вопросах информационной безопасности;

21) организация первоначального доступа Пользователей ИС к ресурсам информационных систем, в соответствии с утвержденным руководителем перечнем лиц, допущенных к работе с ИС. Блокировка учётных записей, изменение полномочий и добавление новых Пользователей ИС;

22) осуществление резервирования ключевых узлов ИС (межсетевых экранов, серверов баз данных, сервера AD, криптошлюзов, коммутаторов, маршрутизаторов и других важных элементов);

23) осуществление контроля целостности программного обеспечения (в том числе и СЗИ);

24) соблюдение условий эксплуатации СЗИ Пользователями ИС;

25) оказание помощи Пользователям ИС, в части применения средств защиты от несанкционированного доступа и других средств защиты, входящих в состав ИС;

26) участие в составе комиссии по реагированию на инциденты информационной безопасности, расследованиях причин инцидентов безопасности и внесение по результатам таких расследований предложений по совершенствованию систем безопасности. По мере возможности, Администратор ИБ должен восстанавливать ущерб, нанесённый информационной системе во время инцидента безопасности, а также восстанавливать ПДн и конфиденциальную информацию, модифицированную или уничтоженную в результате такого инцидента;

27) контроль выполнения Пользователями ИС установленных требований обеспечения безопасности защищаемой информации в ИС Организации. В случае получения от Пользователей ИС информации о фактах утраты или компрометации парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, Администратор ИБ незамедлительно принимает все необходимые меры для обеспечения безопасности конфиденциальной информации, в том числе ПДн, в пределах своих полномочий;

28) периодическое сканирование компонентов ИС на наличие уязвимостей. Принятие мер по устранению выявленных уязвимостей;

29) контроль целостности печатей (пломб) на автоматизированных рабочих местах Пользователей ИС и серверах ИС;

30) проведение периодического анализа журналов безопасности средств защиты информации, а также архивирование и хранение этих журналов;

31) контроль обновлений системного, прикладного программного обеспечения и СЗИ (в том числе обновлений антивирусных баз, сигнатур сценариев вторжений, информации об уязвимостях). В случае нарушения работоспособности технических средств и программного обеспечения ИС, в том числе СЗИ, Администратор ИБ принимает участие по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности;

32) оказание помощи ответственному за техническое обслуживание информационных систем (далее – Администратор ИС) в разработке и согласование перечня информационных ресурсов ИС, подлежащих резервному копированию, а также осуществлять контроль выполнения резервного копирования информационных ресурсов Администратором ИС;

33) своевременное информирование ответственного за организацию обработки защищаемой информации Организации о выявленных нарушениях требований по обеспечению безопасности конфиденциальной информации, в том числе ПДн и попытках несанкционированного доступа к ИС.

В случае увольнения, Администратор ИБ Организации обязан передать своему непосредственному начальнику структурного подразделения (отдела), в штате которого он состоит или при отсутствии такового, руководству Организации, или созданной комиссии при приёму дел, все носители защищаемой информации Организации, которые находились в его распоряжении в связи с выполнением им служебных (должностных) обязанностей во время работы в Организации.

4. Права

Администратор ИБ имеет право:

1) знакомиться с нормативными актами Организации, регламентирующими процессы обработки и защиты конфиденциальной информации, в том числе и ПДн;

2) вносить предложения руководителю по совершенствованию существующей системы защиты информации в ИС;

3) сообщать руководителю обо всех выявленных в процессе осуществления должностных обязанностей недостатках и сбоях информационной безопасности Организации и вносить предложения по их устранению, в пределах своей компетенции;

4) требовать от Пользователей ИС соблюдения требований нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности конфиденциальной информации, в том числе и ПДн;

5) инициировать проведение служебных расследований по выявленным фактам нарушения установленных требований обеспечения безопасности конфиденциальной информации, в том числе и ПДн;

6) отключать любые элементы СЗИ при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке;

7) изменять в установленном порядке конфигурацию элементов ИС и СЗИ;

8) требовать прекращения работы в ИС, как в целом, так и отдельных Пользователей ИС, в случае выявления нарушений требований по обеспечению безопасности защищаемой информации, осуществивших

несанкционированный доступ к защищаемым ресурсам ИС Организации или в связи с нарушением функционирования ИС;

9) контролировать выполнение Пользователями ИС установленных требований обеспечения безопасности защищаемой информации в ИС Организации;

10) контролировать соблюдение условий эксплуатации средств защиты информации Пользователями ИС;

11) запрещать устанавливать на серверах и рабочих станциях ИС нештатное программное и аппаратное обеспечение;

12) обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к ответственному за организацию обработки ПДн Организации, а также с требованием о прекращении обработки информации, в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации.

5. Ответственность

Администратор ИБ несёт персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИС, по обеспечению защиты информации, состоянием и поддержанием установленного уровня защиты ИС Организации.

Администратор ИБ несёт ответственность по действующему законодательству Российской Федерации за разглашение конфиденциальной и (или) коммерческой тайны Организации, ставшую ему известной в связи с исполнением обязанностей, а также:

1) несвоевременное или некачественное выполнение приказов руководства Организации;

2) непринятие мер по пресечению выявленных нарушений информационной безопасности в ИС и средствах защиты информации, создающих угрозу деятельности и репутации Организации.

С функциональными обязанностями администратора информационной безопасности ознакомлен(-а):

Балатаев Р.В. (ФИО)	(подпись)	«23» 01 2026 г.
(ФИО)	(подпись)	«___» _____ 20___ г.
(ФИО)	(подпись)	«___» _____ 20___ г.

Приложение 3

УТВЕРЖДЕНЫ
приказом МУ "ЦБ № 1"
от 23.01.2026 № 36

ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ
администратора информационных систем муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1"

1. Общие положения

Настоящие функциональные обязанности разработаны на основе постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Настоящий документ определяет основные обязанности, права и ответственность администратора информационных систем (далее – Администратор ИС).

Администратор ИС является сотрудником муниципального бюджетного учреждения Петрозаводского городского округа "Централизованная бухгалтерия № 1" (далее – Организация).

Администратор ИС подчиняется непосредственно своему руководителю структурного подразделения (отдела), а при отсутствии такового, непосредственно руководителю, а также ответственному за организацию обработки персональных данных, ответственному за обеспечение безопасности персональных данных в информационных системах и отвечает за обеспечение работоспособности и надлежащее функционирование всех элементов информационных систем (далее – ИС) Организации.

Администратор ИС руководствуется положениями федеральных законов и нормативных актов органов государственной власти, ведомственных организационно-распорядительных актов, нормативных актов Организации, а также другими распорядительными документами, в части его касающейся.

В своей деятельности Администратор ИС руководствуется настоящим документом, «Правилами обработки персональных данных субъектов

персональных в Организации», «Политикой обработки персональных данных Организации».

Администратор ИС имеет право требовать от пользователей ИС выполнения указаний и соблюдения правил работы в ИС, приведенных в «Инструкции пользователя, допущенного к обработке персональных данных в ИС».

Функциональные обязанности Администратора ИС не регламентирует вопросы защиты и охраны зданий и помещений, в которых расположены ИС, вопросы обеспечения физической целостности компонентов ИС, защиты от стихийных бедствий (пожаров, наводнений и др.), сбоев в системе энергоснабжения, а также меры обеспечения безопасности сотрудников и меры, принимаемые при возникновении в ИС нештатных ситуаций.

2. Функциональные обязанности

Администратор ИС обязан:

1) обеспечивать работоспособность средств вычислительной техники ИС, проводить организационно-технические мероприятия по их обслуживанию;

2) осуществлять настройку компонентов ИС, включая прикладное программное обеспечение и специальное программное обеспечение;

3) рассматривать целесообразность применения новых технологий для повышения эффективности функционирования ИС Организации;

4) подготавливать обоснования и спецификации для закупки, заказывать новые элементы ИС и расходные материалы;

5) поддерживать резерв расходных материалов;

6) изучать рынок программных средств и предоставлять рекомендации по приобретению и внедрению системного и прикладного программного обеспечения;

7) выполнять своевременное обновление программного обеспечения элементов ИС и системы защиты информации (в пределах своей компетенции) по мере появления новых версий;

8) выполнять учёт информационных ресурсов ИС (перечень информационных ресурсов разрабатывается и согласовывается совместно с руководителями структурных подразделений (отделов) и администратором информационной безопасности);

9) выполнять резервное копирование данных ресурсов и, в случае необходимости – восстановление данных. Все факты осуществления

резервного копирования данных должны фиксироваться в «Журнале учёта проведения полного резервного копирования». Все факты восстановления данных должны фиксироваться в «Журнале восстановления конфиденциальной информации». График проведения резервного копирования должен быть утверждён руководителем;

10) проводить инструктаж пользователей ИС по внедряемым и используемым технологиям или прикладному программному обеспечению, если это требует от пользователей дополнительных навыков и знаний. Возможен инструктаж не только в устной форме, но и в письменной, либо в электронном виде, путём создания инструкций, файлов, справок, описаний, руководств пользователя и прочее, с последующим обязательным доведением до каждого пользователя;

11) совместно с администратором информационной безопасности (далее – Администратор ИБ) обеспечивать контроль выполнения пользователями положений «Инструкции пользователя, допущенного к обработке персональных данных в ИС»;

12) вести учёт всех технических средств, на которых осуществляется обработка конфиденциальной информации, в том числе персональных данных;

13) предоставлять доступ к информационным ресурсам ИС пользователям по заявке от руководителей структурных подразделений (отделов), которым необходим доступ к ИС по согласованию с Администратором ИБ;

14) оказывать помощь Администратору ИБ при анализе работы элементов ИС и средств защиты информации с целью выявления и устранения неисправностей, а также оптимизации их функционирования;

15) оказывать помощь Администратору ИБ в осуществлении контроля действий пользователей ИС Организации по работе с паролями;

16) предоставлять Администратору ИБ любую затребованную им информацию о настройках, конфигурации, составу и структуре ИС и механизмов защиты информации ИС;

17) выполнять действия по изменению элементов ИС, необходимость в которых определяется согласованным решением, определенным совместно с Администратором ИБ;

18) участвовать совместно с Администратором ИБ в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;

19) сопровождать работников внешних организаций, которые выполняют работы по обслуживанию ИС Организации;

20) в случае обнаружения попытки несанкционированного доступа, в отношении защищаемых ресурсов со стороны пользователей или внешних нарушителей, оповещать Администратора ИБ Организации;

21) осуществлять контроль технологических процессов обработки защищаемой информации;

22) осуществлять при необходимости совместно с ответственным за организацию обработки персональных данных и Администратором ИБ периодические проверки состояния защиты конфиденциальной информации (в соответствии с утверждённым «Планом внутренних проверок состояния защиты» и «Регламентом проведения внутренних проверок состояния защиты»).

23) участвовать при необходимости в качестве члена комиссии по:

• проведению классификации информационных систем;

• установлению уровней защищённости персональных данных в информационных системах персональных данных;

• реагированию на инциденты информационной безопасности, расследованию причин инцидентов безопасности;

• уничтожению конфиденциальной информации;

• контролю защищённости информации.

24) разрабатывать предложения ответственному за организацию обработки персональных данных и Администратору ИБ по изменению нормативных документов, регламентирующих процессы обработки и обеспечения безопасности информации Организации;

25) планировать дальнейшее развитие структуры и функциональности ИС, а также вносить предложения о совершенствовании работы и повышении эффективности функционирования средств вычислительной техники, серверов ИС и системы защиты информации.

В случае увольнения, Администратор ИС Организации обязан передать своему непосредственному начальнику структурного подразделения (отдела), в штате которого он состоит или при отсутствии такового, Администратору ИБ или ответственному за организацию обработки персональных данных, все носители защищаемой информации Организации, которые находились в его распоряжении в связи с выполнением им служебных (должностных) обязанностей во время работы в Организации.

3. Права

Администратор ИС имеет право:

1) знакомиться с нормативными актами Организации, регламентирующими процессы обработки и защиты конфиденциальной информации, в том числе и персональных данных;

2) вносить предложения по совершенствованию функционирования ИС Организации;

3) анализировать работу любых элементов ИС для выявления и устранения неисправностей, а также для оптимизации её функционирования;

4) требовать от пользователей ИС соблюдения правил работы в ИС, приведенных в «Инструкции пользователя, допущенного к обработке персональных данных в ИС»;

5) отключать любые элементы ИС при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей после согласования и заблаговременного предупреждения пользователей ИС;

6) отключать элементы системы защиты информации при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке после согласования с Администратором ИБ;

7) в установленном порядке изменять конфигурацию элементов ИС.

4. Ответственность

Администратор ИС несёт персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИС и по обеспечению работоспособности ИС Организации.

Администратор ИС несёт ответственность по действующему законодательству Российской Федерации за разглашение конфиденциальной и (или) коммерческой тайны Организации, ставшую ему известной в связи с исполнением обязанностей, а также:

1) за ненадлежащее исполнение или неисполнение своих должностных (функциональных) обязанностей;

2) непринятие мер по пресечению выявленных нарушений в работе ИС, создающих угрозу деятельности и репутации Организации.

С функциональными обязанностями администратора информационных систем ознакомлен(-а):

Балатаев Р.В (ФИО)	(подпись)	«23» 01 20 26 г.
(ФИО)	(подпись)	«___» _____ 20___ г.
(ФИО)	(подпись)	«___» _____ 20___ г.

Приложение 4

УТВЕРЖДЕН
приказом МУ "ЦБ № 1"
от 23.01.2026 № 36

СОСТАВ
комиссии по установлению уровня защищённости персональных данных в информационных системах персональных данных

Бойцова Людмила Борисовна	-	руководитель, председатель комиссии.
		Члены комиссии:
Патроева Светлана Анатольевна	-	главный бухгалтер;
Балатаев Руслан Вадимович	-	системный администратор;
Балатаев Никита Вадимович	-	инженер по автоматизации и механизации производственных процессов.

Руководитель Л.Б. Бойцова

Приложение 5

УТВЕРЖДЕН
приказом МУ "ЦБ № 1"
от 23.01.2026 № 36

СОСТАВ
комиссии по классификации государственной и (или) муниципальной информационной системы по требованиям защиты информации, не составляющей государственную тайну

Бойцова Людмила Борисовна	-	руководитель, председатель комиссии.
		Члены комиссии:
Патроева Светлана Анатольевна	-	главный бухгалтер;
Балатаев Руслан Вадимович	-	системный администратор;
Балатаев Никита Вадимович	-	инженер по автоматизации и механизации производственных процессов.

Руководитель Л.Б. Бойцова

Приложение 6

УТВЕРЖДЕН
приказом МУ "ЦБ № 1"
от 23.01.2026 № 36

СОСТАВ
постоянно действующей комиссии по работе с инцидентами информационной безопасности

Бойцова Людмила Борисовна	-	руководитель, председатель комиссии.
		Члены комиссии:
Балатаев Руслан Вадимович	-	системный администратор;
Балатаев Никита Вадимович	-	инженер по автоматизации и механизации производственных процессов.

Руководитель Л.Б. Бойцова

Приложение 7

УТВЕРЖДЕН
приказом МУ "ЦБ № 1"
от 23.01.2026 № 36

СОСТАВ
комиссии по уничтожению персональных данных субъектов персональных данных

Бойцова Людмила Борисовна	-	руководитель, председатель комиссии.
		Члены комиссии:
Патроева Светлана Анатольевна	-	главный бухгалтер;
Балатаев Руслан Вадимович	-	системный администратор;
Балатаев Никита Вадимович	-	инженер по автоматизации и механизации производственных процессов.

Руководитель Л.Б. Бойцова