Областное государственное унитарное предприятие
«Информационный центр «Регион-Курск»

ПРИКАЗ

г. Курск № 12 п/д « 21 » мая 2012

Об утверждении Положения о персональных данных обрабатываемых в информационных системах ОГУП «Информационный центр «Регион-Курск»

В целях исполнения Федерального закона №152-ФЗ от 27 июля 2006 года «О персональных данных», требований иных руководящих документов по обеспечению безопасности персональных данных при их обработке ПРИКАЗЫВАЮ:

1. На основании действующего законодательства Российской Федерации, нормативных и методических документов вышестоящих организаций по вопросам обработки персональных данных и особенностей обработки персональных данных в ОГУП «Информационный центр «Регион-Курск» утвердить Положение о персональных данных обрабатываемых в информационных системах ОГУП «Информационный центр «Регион-Курск» (Приложение №1).
2. Приказ вступает в силу со дня подписания.

Директор
«Информационный центр «Регион-Курск» Брагин И. В.

Приложение №1
к приказу № 12 п/д
от 21.05.2012

Директор
Областного государственного унитарного
предприятия «Информационный центр
«Регион-Курск»

_____ И. В. Брагин

«22» мая 2012 г.

**Положение о персональных данных
обрабатываемых в информационных системах
ОГУП «Информационный центр «Регион-Курск»**

1. Общие положения

1.1. Настоящее Положение о персональных данных, обрабатываемых в информационных системах (далее - Положение) разработано с целью определения порядка обработки в информационных системах ОГУП «Информационный центр «Регион-Курск» персональных данных субъектов, обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установления ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Положение определяет порядок сбора, хранения, передачи и любого другого использования в ОГУП «Информационный центр «Регион-Курск» персональных данных субъектов, данные которых подлежат обработке в информационных системах ОГУП «Информационный центр «Регион-Курск» в соответствии с законодательством Российской Федерации в целях выполнения задач и функций предприятия.

1.3. Положение разработано на основе Федерального закона №149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федерального закона №152-ФЗ «О персональных данных», Постановления правительства РФ №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК, ФСБ, Мининформсвязи России № 55/86/20 «Порядка проведения классификации информационных систем персональных данных», Приказа ФСТЭК России №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» и других действующих нормативных актов Российской Федерации.

1.4. Настоящее Положение утверждается директором ОГУП «Информационный центр «Регион-Курск».

1.5. Изменения в Положение вносятся приказом и утверждаются директором ОГУП «Информационный центр «Регион-Курск».

1.6. Положение является внутренним документом предприятия. Все сотрудники предприятия должны быть ознакомлены с данным Положением и изменениями к нему, что должно быть подтверждено соответствующей распиской.

1.7. Порядок обработки персональных данных сотрудников предприятия без использования средств автоматизации осуществляется в соответствии с Положением о порядке обработки персональных данных работников ОГУП «Информационный центр «Регион-Курск».

1.8. Настоящее Положение распространяется на следующие информационные системы персональных данных с информацией ограниченного доступа (далее ИСПДн):
- ИСПДн «Администрирование и безопасность»;
- ИСПДн «Бухгалтерия и кадры»;

2. Понятия и определения

В Положении используются следующие основные понятия:

Персональные данные (ПДн) субъекта - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных

данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

Информация - сведения (сообщения, данные) независимо от формы их представления;

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных (БД), а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

3. Принципы обработки ПДн

3.1. Цели обработки ПДн. Обработка персональных данных субъектов может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов Российской Федерации, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, бухгалтерского учета, расчета заработной платы сотрудников предприятия, ведения учета получателей универсальных электронных карт (далее УЭК), клиентов, абонентов, а также в целях надлежащего выполнения иных функций предприятия.

Персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

3.2. Принципы обработки ПДн. При обработке персональных данных в ОГУП «ОГУП «Информационный центр «Регион-Курск»» необходимо соблюдать следующие принципы:

- законность целей и способов обработки ПДн, добросовестность;
- соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям оператора;
- соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверность ПДн, их достаточность для целей обработки, недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимость объединения созданных для несовместимых между собой целей баз данных ИСПДн;
- осуществление хранения ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки;
- уничтожение ПДн по достижении целей обработки или в случае отзыва субъектом согласия на их обработку.

3.3. Круг субъектов, персональные данные которых подлежат обработке. Обработке в ОГУП «Информационный центр «Регион-Курск» подлежат персональные данные граждан РФ, проживающих на территории Курской области, являющихся получателями универсальных электронных карт, а также работников предприятия.

3.4. Способы (содержание) обработки персональных данных. Обработка ПДн в ОГУП «Информационный центр «Регион-Курск» осуществляется следующими способами: сбор,

ввод в электронную БД, систематизация, накопление, хранение, уточнение, использование, печать, передача, обезличивание, блокирование, уничтожение.

3.5. Юридические (либо затрагивающие права и свободы) последствия, порождаемые в результате действий (операций) с персональными данными. В результате обработки полученных персональных данных граждан, проживающих на территории Курской области, в ОГУП «Информационный центр «Регион-Курск» формируются документы, на основании которых гражданам (субъектам ПДн) предоставляется УЭК и весь спектр услуг связанных с ее использованием.

В результате обработки персональных данных работников предприятия осуществляется обеспечение соблюдения трудового законодательства, обучение и продвижение работников по службе, обеспечение их личной безопасности, контроль количества и качества выполняемой работы, установление заработной платы, предоставление предусмотренных действующим законодательством гарантий и компенсаций.

3.6. Обозначение принадлежности персональных данных субъекту. Способом обозначения принадлежности персональных данных, содержащихся в информационной системе персональных данных ИСПДн «Администрирование и безопасность», конкретному субъекту персональных данных является присвоение уникального идентификационного номера получателя УЭК.

3.7. Правовые основы обработки персональных данных.

3.7.1. В процессе обработке персональных данных Оператор руководствуется следующими законодательными актами:

- Федеральный закон №152-ФЗ от 27.07.2006 «О персональных данных»;
- Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента РФ 6.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации №1233 от 03.11.94 г. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;
- Приказ ФСТЭК РФ от 05.02.2010 №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 №282 (Инв. № 2153), и иных действующих нормативных актов Российской Федерации.

3.7.2. При обработке персональных данных без использования средств автоматизации Оператор, в дополнение к вышеуказанным актам, руководствуется следующими нормативными документами РФ:

- Постановление Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3.7.3. При обработке персональных данных средствами автоматизации Оператор, в дополнение к вышеуказанным актам, руководствуется следующими нормативными документами РФ:

- Приказ ФСТЭК, ФСБ, Мининформсвязи 13.02.08 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

- Постановление Правительства Российской Федерации от 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

3.8. Места обработки ПДн. Обработка ПДн в ОГУП «Информационный центр «Регион-Курск» осуществляется по месту расположения предприятия по адресу: 305002, г.Курск, ул. М. Горького, 65 а-3, офис 7.

3.9. Состав персональных данных обрабатываемых в ИСПДн «Администрация и безопасность»: подлежат следующие персональные данные субъектов:

- фамилия,
- имя,
- отчество,
- пол,
- гражданство,
- адрес прописки,
- адрес фактического проживания,
- день рождения,
- месяц рождения,
- год рождения,
- паспортные данные (серия паспорта, номер паспорта, дата выдачи паспорта, кем выдан паспорт),
- номер контактного телефона,
- СНИЛС,

Состав персональных данных обрабатываемых в ИСПДн «Бухгалтерия»

- фамилия,
- имя,
- отчество сотрудника,
- образование,
- сведения о трудовом и общем стаже,
- паспортные данные,
- сведения о воинском учете и о военнообязанных лицах,
- сведения о заработной плате сотрудника,
- данные о расчетных счетах сотрудников учреждения,
- декларации, подаваемые в налоговую инспекцию,
- отчеты, направляемые в органы статистики,
- специальность,
- занимаемая должность,
- адрес места жительства,
- домашний телефон,
- содержание трудового договора,
- сведения об отпусках работниках,
- сведения о командировках

3.10. Источники и способы получения ПДн. Персональные данные отдельных категорий граждан обрабатываемых в ИСПДн «Администрирование и безопасность» поступают в предприятие от пунктов приема-выдачи заявлений. Персональные данные сотрудников учреждения предоставляются ими лично.

3.11. Действия при получении ПДн от третьих лиц. При получении персональных данных от третьих лиц оператор ПДн до начала обработки обязан получить у субъекта этих ПДн письменное разрешение на их обработку, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если они являются общедоступными и в иных случаях предусмотренных статьей 6 Федерального закона №152-ФЗ «О персональных данных». Оператор обязан обеспечивать режим конфиденциальности персональных данных в процессе передачи документов (или иных материальных носителей), содержащих ПДн субъекта.

3.12. Передача ПДн третьим лицам. Согласно Федеральному закону №152-ФЗ "О персональных данных", передача ПДн является частным случаем обработки ПДн. В случаях, когда цель передачи ПДн субъекта соответствует целям обработки ПДн в учреждении, в целях исполнения Трудового кодекса РФ и законодательства РФ, а также в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, дополнительное согласие на такую передачу не запрашивается. Оператор обязан обеспечивать режим конфиденциальности персональных данных в процессе передачи документов (или иных материальных носителей), содержащих ПДн субъекта. Третьими лицами, получающими в результате передачи доступ к персональным данным, в дальнейшем должна обеспечиваться конфиденциальность ПДн, за исключением общедоступных или обезличенных данных.

3.13. Передача ПДн. В процессе осуществления обработки ПДн в ОГУП «Информационный центр «Регион-Курск» осуществляются следующие виды передачи персональных данных:

- периодическая передача сведений в отношении работников предприятия в Пенсионный фонд РФ, в Фонд социального страхования, Фонд медицинского страхования, налоговые органы.

3.14. Передача ПДн субъектам ПДн, их представителям и наследникам.

3.14.1. Правовое обоснование. Согласно Федерального закона №152-ФЗ, ст.14, субъекту ПДн предоставляется право на доступ к своим персональным данным, а также на получение сведений об операторе. Передача ПДн субъекта может осуществляться непосредственно субъекту ПДн либо его законному представителю (в случае недееспособности субъекта ПДн), либо наследнику субъекта ПДн (в случае смерти субъекта ПДн).

3.14.2. Объем предоставляемой информации. Субъект ПДн имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту ПДн, а также на ознакомление с такими персональными данными. При обращении субъекта ПДн или при получении соответствующего запроса оператором может быть предоставлена следующая информация:

- подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
- способы обработки персональных данных, применяемые оператором;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

3.14.3. Сроки реагирования на обращения субъектов персональных данных. Передача персональных данных осуществляется оператором при обращении субъекта ПДн или его законного представителя либо в течение 10 рабочих дней с даты получения оформленного в соответствии с законодательством запроса.

3.14.4. Форма запроса. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

3.14.5. Порядок реагирования на обращения субъектов персональных данных. При обращении субъекта ПДн или его законного представителя, сотрудником, осуществляющим обработку ПДн данного субъекта, делается отметка в «Журнале учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных». В указанный в п.3.14.3. срок сотрудником должен быть сформирован ответ на соответствующее обращение или официальный запрос. Перед передачей персональных данных сотрудник должен удостовериться в подлинности предоставленных документов, удостоверяющих личность субъекта ПДн или его законного представителя при личном обращении, либо правильность данных и подлинность удостоверяющей подписи при получении запроса. Сформированный ответ на запрос субъекта ПДн о предоставлении персональных данных и сведений об операторе оформляется сотрудником в регламентированной ниже форме, с соответствующими реквизитами исходящего документа. При передаче ответа субъекту ПДн или законному представителю сотрудником делается отметка в «Журнале регистрации внутренних и исходящих документов, содержащих персональные данные».

3.14.6. Способы и форма предоставления персональных данных и сведений об операторе, а также объем предоставляемой информации. Предоставление персональных и сведений об операторе субъекту ПДн или его законному представителю осуществляется в материальной документированной форме любым доступным способом, исключающим при передаче несанкционированный доступ к данным. Форма предоставления персональных данных должна содержать реквизиты получателя персональных данных и сведений об операторе, а также основание для предоставления таких данных. Содержание предоставляемого перечня персональных данных должно полностью соответствовать запросу субъекта ПДн или его законного представителя. Сведения о наличии персональных данных предоставляются в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам ПДн.

3.14.7. Запрет на передачу ПДн. Запрет на передачу ПДн может быть получен в случае, когда предоставление персональных данных нарушает конституционные права и свободы других лиц или законодательство РФ.

3.14.8. Отказ в предоставлении ПДн. В случае отказа в предоставлении субъекту ПДн или его законному представителю при обращении либо при получении соответствующего запроса информации о персональных данных и сведений об операторе, предоставляется в письменной форме мотивированный ответ, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, в сроки в соответствии со статьей 20 Федерального закона №152-ФЗ.

3.15. Обезличенные данные.

3.15.1. Согласно Федерального закона №152-ФЗ, статье 3, пункт 8, обезличиванием персональных данных признаются действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3.15.2. Применяемые способы обезличивания данных определяются оператором ПД. Среди них выделяют: уменьшение перечня обрабатываемых сведений; замена части сведений идентификаторами; замена численных значений минимальным, средним, или максимальным значением; понижение точности сведений; деление сведений на части и обработка в разных информационных системах и т.д.

3.15.3. В случае обезличивания персональных данных обеспечение оператором конфиденциальности таких данных не требуется.

3.16. Общедоступные данные.

3.16.1. Согласно Федерального закона №152-ФЗ, статье 3, пункт 12, общедоступными персональными данными признаются персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

3.16.2. Согласно Федерального закона №152-ФЗ, статье 3, пункт 1, в общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

3.16.3. Порядок отнесения ПДн к общедоступным ПДн. Основанием для отнесения персональных данных к общедоступным ПДн является письменное согласие субъекта персональных данных, с наличием полного перечня таких данных, даты составления и личной подписи субъекта.

3.16.4. Порядок прекращения режима общедоступности. Согласно Федерального закона №152-ФЗ, статье 8, пункт 2, сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов. При прекращении режима общедоступности оператору необходимо обеспечить защиту персональных данных в соответствии с законодательством РФ.

3.17. Согласие на обработку ПДн.

3.17.1. Согласно Федерального закона №152-ФЗ, субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе.

3.17.2. Обработка ПДн, не относящихся к категории специальных, без согласия субъекта ПДн может производиться в следующих случаях:

- обработка ПДн необходима в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;
- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Перечень случаев обработки ПДн без согласия субъекта ПДн определяется в соответствии со статьей 6 Федерального закона №152-ФЗ.

3.17.3. Письменное согласие на обработку ПДн в общем случае предоставляет субъект ПДн при его обращении в УОС. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта ПДн. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие, а также порядок его отзыва.

В случае изменения действующего законодательства форма письменного согласия определяется в соответствии со статьей 9 Федерального закона №152-ФЗ.

3.17.4. Срок действия согласия определяется в тексте заявления о согласии.

3.17.5. Если обязанность предоставления персональных данных установлена федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные. Оператор вправе не предоставлять услуги субъекту в случае отказа от предоставления персональных данных, если иное не предусмотрено нормативными актами РФ.

3.17.6. Порядок отзыва согласия. Субъект ПДн имеет право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен в адрес оператора по почте заказным письмом с уведомлением о вручении, либо вручен лично под расписку представителю Оператора.

3.17.7. Действия при отзыве согласия. В случае отзыва субъектом ПДн согласия на обработку своих персональных данных оператор, обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 3 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом ПДн. Об уничтожении персональных данных оператор обязан уведомить субъекта ПДн, форма уведомления субъектов представлена в Приложении №1.

3.18. Права и обязанности субъекта ПДн. Права и обязанности субъекта персональных данных определяются Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», иными законодательными актами Российской Федерации, а также заключенными соглашениями между субъектом и оператором (при их наличии).

3.18.1. В числе прав субъекта ПДн можно выделить следующие группы:

- права на доступ к своим персональным данным: ознакомление, уточнение, блокирование и уничтожение;
- права на информацию об условиях обработки ПДн оператором и лицах, допущенных им для ознакомления с ПДн;
- права, возникающие при обработке персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации;
- права, возникающие при принятии юридически значимых решений на основании исключительно автоматизированной обработки персональных данных субъектов;
- права на обжалование действий или бездействия оператора.

3.18.2. В числе обязанностей субъекта ПДн можно выделить следующие группы:

- обязанности субъекта о передаче оператору комплекта всех необходимых для достижения целей обработки достоверных, документированных персональных данных;
- обязанности субъекта о своевременном информировании оператора об изменениях своих персональных данных.

3.19. Права и обязанности оператора. Права и обязанности оператора персональных данных определяются Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», иными законодательными актами Российской Федерации, а также заключенными соглашениями между субъектом и оператором (при их наличии).

3.19.1. В числе прав оператора ПДн можно выделить следующие группы:

- права оператора самостоятельно определять места, способы и формы обработки полученных ПДн;

- права оператора на передачу ПДн при соблюдении требуемых законодательством РФ условий.

3.19.2. В числе обязанностей оператора ПДн можно выделить следующие группы:

- обязанности оператора при сборе персональных данных;

- обязанности оператора о принятии мер по обеспечению безопасности персональных данных при их обработке;

- обязанности оператора при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных;

- обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных;

- обязанность оператора об уведомлении субъекта и уполномоченных органов об обработке персональных данных.

3.20. Действия в случае выявления фактов нарушения законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных.

3.20.1. Оператор обязан внести в персональные данные субъекта необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом ПДн или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы, форма уведомления субъектов представлена в Приложении №2.

3.20.2. В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий 3 рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий 3 рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.21. Право на обжалование действий или бездействия оператора. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке. Субъект персональных данных имеет право на защиту своих прав и

законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3.22. Сроки обработки (хранения) персональных данных и порядок действий при их истечении.

3.22.1. Сроки обработки (хранения) персональных данных определяются целью обработки данных и установленными для документации архивными сроками хранения (номенклатурой дел ОГУП «Информационный центр «Регион-Курск»).

3.22.2. Сроки архивного хранения управленческих документов, содержащих ПДн, устанавливаются номенклатурой дел ОГУП «Информационный центр «Регион-Курск» в соответствии с «Перечнем типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения», утвержденным Росархивом.

3.22.3. В случае достижения цели обработки персональных данных или истечения сроков архивного хранения документов, содержащих ПДн, оператор незамедлительно прекращает обработку ПДн и уничтожает соответствующие персональные данные в срок, не превышающий 3 рабочих дней, если иное не предусмотрено федеральными законами.

3.22.4. В целях уничтожения части персональных данных производится уничтожение или блокирование материального носителя с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.22.5. При уничтожении ПДн оператором производится уведомление о факте уничтожения субъектов ПДн или их законных представителей, форма уведомлений субъектов содержится в Приложении №1.

3.22.6. При уничтожении ПДн оператором составляется «Акт уничтожения персональных данных субъектов персональных данных», форма которого указана в Приложении №3.

3.23. К информации, конфиденциальность которой оператор не обязан соблюдать, относятся следующие типы информации:

- персональные данные, признанные общедоступными;
- обезличенные персональные данные;
- информация, доступ к которой открыт в силу требований действующих нормативно-правовых актов Российской Федерации.

3.24. Порядок учета и маркирования материальных носителей информации, образующихся в процессе обработки персональных данных. В организации должен осуществляться постоянный учет всех материальных носителей информации, образующихся в процессе обработки персональных данных, с помощью их маркировки и с занесением учетных данных в «Журнал учета машинных носителей, содержащих сведения ограниченного доступа». Учету подлежат такие носители конфиденциальной информации, как жесткие магнитные диски - ЖМД, магнитные дискеты - МД, лазерные диски – ЛД, flash-накопители – ФН и др. В Журнале первыми следует зарегистрировать ЖМД АРМов, на которых производится обработка персональных данных, а в дальнейшем – МД, ЛД и ФН по мере необходимости.

Маркировка материальных носителей информации производится с помощью наклеек (этикеток), либо надписей несмываемым маркером (фломастером) с указанием учетного номера носителя согласно Журналу, даты постановки носителя на учет, подписи сотрудника, осуществившего постановку носителя на учет, пометки о конфиденциальности содержащейся на носителе информации.

При утрате съемных носителей персональных данных, содержащих персональные данные, немедленно ставится в известность начальник соответствующего структурного подразделения и ответственный за обеспечение режима ограничения доступа к информации (персональным данным) в организации/обособленном подразделении. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета материальных носителей персональных данных.

Материальные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению с составлением акта.

Временно не используемые носители информации должны храниться пользователем в местах, недоступных для посторонних лиц.

3.25. Режим конфиденциальности. Режим конфиденциальности сохраняется на всем протяжении срока обработки и хранения документов, содержащих персональные данные субъектов.

3.26. Порядок снятия режима конфиденциальности. Снятие режима конфиденциальности осуществляется следующими способами: удаление персональных данных, обезличивание персональных данных. Применяемый способ снятия режима конфиденциальности выбирается оператором, исходя из целесообразности в текущей ситуации.

3.27. Состав мероприятий по обеспечению безопасности. Мероприятия по обеспечению безопасности персональных данных в информационных системах включают в себя:

- определение угроз безопасности персональных данных, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- разработку нормативной, регламентирующей, эксплуатационной и технической документации в организации;
- назначение ответственных лиц по вопросам защиты персональных данных в организации, разграничение их обязанностей;
- составление и утверждение списков лиц, допущенных к работе с персональными данными в организации, ознакомление сотрудников с разработанной документацией;
- установку, настройку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с персональными данными в информационной системе;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

3.28. Требования по уровню обеспечения безопасности. Уровень обеспечения безопасности персональных данных в организации определяется, исходя из класса обрабатываемых данных в соответствии с требованиями законодательства Российской Федерации. Информационная система персональных данных «Администрирование и безопасность», в соответствии с «Актом классификации» признана специальной, с уровнем обеспечения безопасности персональных данных по отношению к типовым ИСПДн не ниже класса К1. Информационная система персональных данных «Бухгалтерия» в соответствии с «Актом классификации» признана специальной, с уровнем обеспечения безопасности персональных данных по отношению к типовым ИСПДн не ниже класса К3. В информационной системе вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий.

3.29. Требования по обеспечению безопасности персональных данных при обработке. При обработке персональных данных в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

- своевременное обнаружение фактов несанкционированного доступа к персональным данным;

- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- постоянный контроль за обеспечением уровня защищенности персональных данных.

3.30. Порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в организации.

3.30.1. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

3.30.2. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе

шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3.30.3. Контроль за обеспечением безопасности ПДн. Контроль за обеспечением безопасности ПДн заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Он может проводиться оператором или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

3.31. Требования к входным дверям помещений. Помещения, в которых осуществляется обработка персональных данных, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

3.32. Требования к окнам помещений. Окна помещений, в которых осуществляется обработка персональных данных, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения. Для предотвращения просмотра извне помещений, в которых осуществляется обработка персональных данных, окна должны быть защищены изнутри непрозрачными шторами, жалюзи или иными средствами.

3.33. Требования к охране помещений. Специальное оборудование и охрана помещений, в которых ведется обработка и хранение персональных данных, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

3.34. Требования к наличию металлических хранилищ в помещениях. Для хранения ключевых документов и носителей, эксплуатационной и технической документации, инсталлирующих криптосредств и программных СЗИ носителей и иных представляющих особую важность объектов должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин.

3.35. Требования к организационным мероприятиям по контролю доступа в помещения. Организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц. Двери помещений, в которых осуществляется обработка персональных данных, должны быть постоянно закрыты на замок, и могут открываться только для санкционированного прохода сотрудников и посетителей. Доступ сотрудников в помещение регулируется в соответствии с «Приказом об определении должностных лиц, допущенных к обработке информации ограниченного доступа» и регулируется ответственным за обеспечение режима конфиденциальности в помещении (подразделении) при их неавтоматизированной обработке, ответственным за обеспечение режима ограничения доступа к информации (персональным данным) в организации/обособленном подразделении. Открытие и закрытие помещений осуществляется исключительно сотрудниками, включенными в «Список лиц,

имеющих право вскрытия и закрытия помещений, в которых обрабатываются персональные данные».

3.36. Требования к персоналу, задействованному в работе с персональными данными. Допуск сотрудников к ПДн осуществляется по приказу руководителя организации, и только после ознакомлениями с регламентирующими документами по работе с ПДн, обязанностями сотрудника и мерами его ответственности. В соответствующих списках должны быть утверждены сотрудники, имеющие доступ к обработке информации в автоматизированном и неавтоматизированном виде. Обязанности персонала определяются в соответствии с утвержденными в организации инструкциями сотрудникам по правилам обработки персональных данных при автоматизированной и неавтоматизированной их обработке.

3.37. Требования к порядку передачи (пересылки) отчуждаемых носителей информации. При передаче (пересылке) носителей информации, содержащих персональные данные, должны быть приняты все необходимые меры для предупреждения несанкционированного доступа к передаваемой информации. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

Все передаваемые носители информации должны проходить строгий учет. В случае, когда информация передается на машинном носителе, последний маркируется и вносится в «Журнал учета машинных носителей, содержащих сведения ограниченного доступа (персональных данных)». В случае, когда информация передается на бумажном носителе, передаваемые документы нумеруются и вносятся в «Журнал регистрации внутренних исходящих документов».

Передача (пересылка) отчуждаемых носителей информации должна осуществляться сотрудником, имеющим доступ к информации ограниченного доступа.

Факт осуществления передачи носителя ПДн должен подтверждаться письменно обеими сторонами. Одним из способов подтверждения факта передачи является ведение соответствующего журнала с проставлением отметок о факте передачи, даты передачи, идентификаторов передаваемых носителей ПДн и личных подписей сторон.

В случае, когда предотвратить несанкционированный доступ к физическому носителю информации невозможно или представляется нецелесообразным, персональные данные должны быть представлены в зашифрованном виде (ключ для дешифрования информации в таком случае передается отдельно от носителя информации по защищенному каналу передачи данных или с курьером).

Запрещается передача персональных данных без использования специальных средств защиты по общедоступным каналам, в том числе Интернет, телефон, факс, электронная почта, за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан.

3.38. Требования по оформлению организационно-распорядительной и эксплуатационной документации. Все организационно-распорядительные и эксплуатационные документы в организации должны иметь все требуемые, правильно составленные и оформленные реквизиты, должны быть утверждены руководителем организации или иным лицом, имеющим соответствующие права. Ввод в эксплуатацию производится с даты утверждения документа. Все сотрудники, действия которых регламентируются организационно-распорядительным или эксплуатационным документом, должны быть ознакомлены с его текстом под роспись. Все изменения, вносимые в организационно-распорядительную и эксплуатационную документацию, требуют проведения повторного утверждения и ознакомления сотрудников.

3.39. Рекомендации по хранению документации на объектах. Для хранения организационно-распорядительной и эксплуатационной документации, а также документов, содержащих персональные данные, отводится специальное помещение, в которое ограничивается доступ персонала организации и посторонних лиц. Защищаемая документация запирается в шкафах, сейфах или иных хранилищах. Контроль за правильностью хранения защищаемой документации осуществляет ответственный за обеспечение режима ограничения доступа к информации (персональным данным) в организации/обособленном подразделении.

3.40. Способы обеспечения безопасности ПДн. В соответствии с п.3 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержденное Постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781) методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий» (приказ ФСТЭК РФ от 05.02.2010 N 58).

3.41. Требования к техническим средствам защиты информации. Требования к техническим средствам защиты информации устанавливаются официальными регуляторами в пределах их компетенции. Все средства защиты информации, применяемые в информационных системах обработки персональных данных, в установленном порядке проходят обязательную процедуру оценки соответствия. В соответствии с «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» № 149/54-144 от 21 февраля 2008 года: «Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации) криптосредства».

3.42. Требования к техническим средствам, системному программному обеспечению, телекоммуникационному оборудованию. Требования к техническим средствам, системному программному обеспечению, телекоммуникационному оборудованию определяются содержанием нормативных актов Российской Федерации и внутренними регламентирующими документами организации. Все аппаратные и программные средства обработки персональных данных должны проходить обязательный учет, с занесением в технический паспорт объекта информатизации. Размещение устройств вывода информации, средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях должны осуществляться таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

3.43. Требования к каналам связи. В соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных» (утвержден Приказом ФСТЭК РФ от 05.02.2010 № 58), обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) применения технических средств. Для передачи информации по каналам связи, выходящим за пределы Контролируемой Зоны необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи, а при использовании открытых каналов связи применять криптографические средства защиты информации.

3.44. Требования к настройкам системного программного обеспечения и средств защиты информации. Требования к настройкам системного программного обеспечения и средств защиты информации определяются требованиями нормативных актов Российской Федерации с учетом класса ИСПДн, технологических особенностей защищаемой системы и процесса обработки персональных данных в системе. Настройка системного программного обеспечения и средств защиты информации осуществляется на основании технического паспорта объекта информатизации, технического задания на построение системы защиты персональных данных, инструкций и руководств на применяемые средства защиты информации.

3.45. Регламент оценки соответствия требованиям по безопасности информации. В соответствии с законодательством РФ, оценка соответствия ИСПДн по требованиям безопасности ПДн проводится в зависимости от класса информации в форме декларирования соответствия или обязательной сертификации (аттестация) по требованиям безопасности информации по решению оператора.

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации в пределах их полномочий или иными организациями, наделенными соответствующими полномочиями.

3.46. Проведение контроля выполнения требований по безопасности персональных данных. Контроль выполнения требований по безопасности персональных данных подразделяется на внутренний и внешний. Внутренний контроль осуществляется назначенными сотрудниками организации в соответствии с установленным планом. Внешний контроль и надзор за соблюдением требований по обращению и обеспечению безопасности данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

3.47. Порядок внутреннего контроля за соблюдением требований по обращению и обеспечению безопасности данных. В целях соблюдения безопасности персональных данных в организации обеспечивается постоянный внутренний контроль. Назначенными в качестве исполнителей сотрудниками организации должны регулярно осуществляться внутренние проверки в соответствии с «Планом внутренних проверок режима защиты персональных данных». После проведения проверки составляется внутренний отчет, содержащий предмет проверки, результаты проведенной проверки, дату завершения проверки и личную подпись лица, осуществляющего проверку.

3.48. Основные параметры контроля. При внутренних проверках контролю подвергается соблюдение сотрудниками регламентирующих документов, выявление изменений в режиме обработки и защиты ПДн, настройках операционных систем, средств защиты информации и средств контроля доступа, правильность и своевременность проведения мероприятий по обеспечению защиты персональных данных, учет носителей персональных данных, эксплуатационной и технической документации к ним, соблюдение условий использования СЗИ. В ходе проведения внешней контролирующей проверки территориальный орган контроля осуществляет рассмотрение документов оператора, а также исследование

(обследование) информационной системы персональных данных, в части, касающейся персональных данных субъектов персональных данных, обрабатываемых в ней.

3.49. Мероприятия при нарушении безопасности персональных данных. В случае выявления нарушений безопасности персональных данных сотрудник, обнаруживший нарушение, сообщает о факте нарушения лицу, ответственному за обеспечение режима ограничения доступа к информации (персональным данным) в организации/обособленном подразделении, и администратору безопасности информации в АС объекта информатизации. В срок, не превышающий 3 рабочих дней с даты выявления нарушения, оператор должен устранить допущенные нарушения. При невозможности оперативно устранить нарушения безопасности руководитель организации должен принять соответствующие меры, предусмотренные законодательством РФ.

3.50. Ответственность за нарушение норм, регулирующих обработку персональных данных. При нарушении норм, регулирующих обработку персональных данных, виновный в нарушении может быть привлечен к дисциплинарной, административной, гражданско-правовой или уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

3.51. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор). В случае возникновения угрозы жизни и здоровью или возникновении предпосылок к таким угрозам сотрудники ОГУП «Информационный центр «Регион-Курск» обязаны немедленно эвакуироваться без эвакуации носителей конфиденциальной информации и материальных ценностей. При возникновении обстоятельств непреодолимой силы, не угрожающих здоровью сотрудников, однако способных негативно повлиять на конфиденциальность персональных данных, сотрудникам следует:

- немедленно прекратить работу и обесточить оборудование;
- лицам, ответственным за конфиденциальное делопроизводство, изъять носители конфиденциальной информации и поместить их во внутренний отсек сейфа, закрыть и опечатать сейф;
- проверить отключение всего оборудования, закрытие вентиляционных отверстий;
- забрать личные вещи и покинуть помещение;
- закрыть и опечатать помещение;
- сообщить директору ОГУП «Информационный центр «Регион-Курск» о выполненных действиях;
- следовать распоряжениям руководства ОГУП «Информационный центр «Регион-Курск» или службы МЧС.

3.52. Мероприятия по обработке ПДн при прекращении деятельности. При прекращении деятельности учреждения следует осуществить процедуру уничтожения персональных данных с уведомлением об этом субъектов ПДн или их законных представителей, а также государственных органов РФ, регулирующих обработку и защиту персональных данных. Формы уведомления субъектов представлены в Приложениях №1 и №2.

4. Список должностей работников ОГУП «Информационный центр «Регион-Курск» уполномоченных на обработку персональных данных

4.1. Бухгалтерия (в отношении ПДн обрабатываемых в ИСПДн «Бухгалтерия и кадры»):
- главный бухгалтер;
- бухгалтера;

- начальник юридического отдела;
- юрист.

4.2. Отдел администрирования и безопасности информации (в отношении ПДн обрабатываемых в ИСПДн «Администрирование и безопасность»):
- начальник отдела;
- администратор;
- специалист по защите информации;

4.3. Директор предприятия, заместитель директора.

Директор
«Информационный центр «Регион-Курск» Брагин И. В.

Приложение №1

Кому:

_____,
Ф.И.О.

проживающему по адресу:

_____ _____
индекс адрес проживания

_____

УВЕДОМЛЕНИЕ
о прекращении обработки персональных данных

Наименование (фамилия, имя, отчество) оператора: Областное государственное унитарное предприятие «Информационный центр «Регион-Курск»

Адрес оператора: 305002, г.Курск, ул. М. Горького д. 65 а-3, оф. 7

Регион: Курская область

Цель обработки персональных данных: учет получателей карт УЭК и предоставление им государственных услуг

Категория субъектов, персональные данные которых обрабатываются: получатели карт УЭК

Дата начала обработки персональных данных: _____

Настоящим уведомлением доводим до Вашего сведения факт прекращения обработки вышеназванным оператором Ваших персональных данных.

Причина прекращения обработки персональных данных (*нужное подчеркнуть*)**:**

реорганизация/ликвидация ОГУП «Информационный центр «Регион-Курск»; достижение целей обработки персональных данных, истечение срока обработки персональных данных, отзыв согласия субъекта персональных данных на обработку его персональных данных;

_____
указать иные обстоятельства в соответствии с действующим законодательством

_____

"___" _____ 20___ г.

Составитель уведомления: _____ _____
И.О.Фамилия подпись

Приложение №2

Кому:

_____,
Ф.И.О.

проживающему по адресу:

_____ _____
индекс адрес проживания

_____

УВЕДОМЛЕНИЕ

о _____

Наименование (фамилия, имя, отчество) оператора: Областное государственное унитарное предприятие «Информационный центр «Регион-Курск»

Адрес оператора: 305002, г.Курск, ул. М. Горького д. 65 а-3, оф. 7

Регион: Курская область

Цель обработки персональных данных: учет получателей карт УЭК и предоставление им государственных услуг

Категория субъектов, персональные данные которых обрабатываются: получатели карт УЭК

Дата начала обработки персональных данных: _____

Настоящим уведомлением доводим до Вашего сведения следующий факт:

_____
_____
_____
_____
_____
_____

"___" _____ 20___ г.

Составитель уведомления: _____ _____
И.О.Фамилия подпись

Приложение №3

АКТ
уничтожения персональных данных субъектов персональных данных
в ОГУП «Информационный центр «Регион-Курск»

С целью выполнения требований руководящих документов по обеспечению безопасности персональных данных при их обработке по причине

_____
указать причину

было осуществлено уничтожение следующих персональных данных:

Состав ПДн	Субъект ПДн	Носитель ПДн	Способ уничтожения ПДн

Уничтожение персональных данных осуществил:

_____
должность

_____ _____
Ф.И.О. подпись