РД-01	Положение об обработке персональных данных	

УТВЕРЖДАЮ

Директор департамента образования

и науки Костромской области

_____ Т.Е. Быстрякова

«_1_» сентября 2015 г.

ПОЛОЖЕНИЕ
об обработке персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение принято в целях обеспечения защиты персональных данных работников департамента образования и науки Костромской области (оператора ПДн), членов их семей, а также иных физических лиц, состоящих в договорных отношениях с департаментом.

1.2. Положение определяет политику оператора в отношении обработки персональных данных, права и обязанности оператора и субъектов персональных данных, порядок использования персональных данных в целях реализации требований действующего законодательства и исполнения служебных обязанностей, а также порядок взаимодействия по вопросам сбора, документирования, хранения и уничтожения персональных данных.

1.3. Настоящее Положение разработано на основании и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», положений главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников», постановления Правительства РФ от 21 марта 2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иных нормативно-правовых актов.

1.4. Персональные данные обрабатываются с согласия субъекта персональных данных, если иное не определено федеральным законом. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме.

1.5. Специальные категории персональных данных, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья обрабатываются в случаях, предусмотренных ст. 10 Федерального закона от 26.07.2006 г.№ 152-ФЗ «О персональных данных», только при наличии письменного согласия субъекта персональных данных.

1.6. Обработка персональных данных в целях оказания услуг с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

1.7. Обработка персональных данных в департаменте ограничивается достижением конкретных, заранее определенных и законных целей. Содержание и объём обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки.

Обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается.

2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Для целей настоящего Положения используются следующие основные понятия:

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

оператор – орган исполнительной власти, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение

(обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. МЕРЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В департаменте образования и науки Костромской области разработаны и внедрены следующие меры для обеспечения выполнения предусмотренных действующим законодательством обязанностей по предотвращению несанкционированного доступа или неправомерного использования, утраты информации, содержащей персональные данные работников:

- назначен ответственный за организацию обработки персональных данных;
- определены Перечни категорий персональных данных, обрабатываемых в департаменте (Приложение 1);
- определен Перечень должностей, имеющих доступ к различным группам (базам) персональных данных (Приложение 2);
- определен тип угроз безопасности персональных данных, актуальных для информационной системы, установлен уровень защищенности персональных данных в ИСПДн в соответствии с требованиями постановления правительства Российской Федерации от 01.11.2012 г. № 1119;
- назначены ответственные за обеспечение безопасности персональных данных при работе в информационных системах;

- определены места хранения материальных носителей персональных данных в подразделениях департамента;
- организован ограниченный доступ в помещения, где обрабатываются персональные данные;
- определен порядок передачи помещений, в которых обрабатываются персональные данные, под охрану в нерабочее время;
- ведётся учёт электронных носителей информации (flash-карты, внешние НЖМД);
- реализованы требования по парольной и иной защите доступа к информационным ресурсам (длина не менее шести знаков, регулярная смена паролей);
- определен порядок размещения мониторов на рабочих местах пользователей, исключающий просмотр визуальной информации посторонними лицами;
- обеспечивается защита от воздействия вредоносных программ и программно-математических воздействий (антивирусная защита, администрирование);
- реализована передача обрабатываемых персональных данных по общедоступной телекоммуникационной сети (Интернет) с использованием сертифицированных программных средств защиты информации;
- организован контроль выполнения условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

4. ОБРАБОТКА ПДн СОТРУДНИКОВ ДЕПАРТАМЕНТА И ЧЛЕНОВ ИХ СЕМЕЙ

4.1. Обработка персональных данных сотрудников осуществляется в соответствии с требованиями трудового, налогового, пенсионного и иного законодательства.

4.2. В соответствии с требованиями Федерального закона Российской Федерации от 24.07.2004 № 79-ФЗ «О государственной гражданской службе в РФ» при заключении трудового договора лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета – для военнообязанных и лиц, подлежащих призыву на военную службу;

- документы об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
- справку о наличии (отсутствии) судимости – при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию.

В отдельных случаях может предусматриваться необходимость предъявления дополнительных документов.

Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом и иными федеральными законами, регламентирующими деятельность государственного гражданского служащего, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

4.3. Персональные данные работника предоставляются самим работником. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.4. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

4.5. Работник обязан предоставлять работодателю достоверную персональную информацию. При изменении персональных данных работник должен письменно уведомить об этом работодателя в срок, не превышающий 14 дней. Работодатель имеет право запрашивать у работника дополнительные сведения и документы, подтверждающие их достоверность.

4.6. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия (Приложение 3).

4.7. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных» или иными федеральными законами.

4.8. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных (Приложение 4). В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта

персональных данных при наличии оснований, указанных в федеральном законодательстве.

4.9. Для изучения и оценки возможности приема на работу в департамент, кандидаты на вакантные должности проходят собеседование и иные, предусмотренные законодательством процедуры. В случае принятия положительного решения, кандидат заполняет анкету установленной формы и оформляется на работу.

Персональные данные кандидатов обрабатываются без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации.

Порядок обработки персональных данных без использования средств автоматизации определен Правилами обработки персональных данных, осуществляемой без использования средств автоматизации.

4.10. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5. ОБРАБОТКА ПДн ФИЗИЧЕСКИХ ЛИЦ И КОНТРАГЕНТОВ

5.1. Оператор ПДн в случаях предусмотренных законодательством имеет право обрабатывать персональные данных физических лиц и контрагентов.

5.2. При заключении договора с физическим лицом (субъект ПДн) или контрагентом (должностное лицо) согласие на обработку своих персональных данных, предоставленных в разделах договора не требуется.

5.3. Персональные данные, полученные оператором в связи с заключением договора, стороной которого является субъект персональных данных (физическое либо должностное лицо), не распространяются и не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного.

6.ПОРЯДОК ХРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ ПДн

6.1. Хранение персональных данных работников осуществляется на бумажных носителях, а при необходимости ведения централизованных учетов, устанавливаемых федеральным законодательством, и на электронных носителях.

6.2. Доступ к персональным данным, хранящимся на электронных носителях, а также к программному обеспечению регламентирован и осуществляется при введении пароля, использования электронной подписи иных средств защиты от несанкционированного доступа.

6.3. Документы (на бумажных носителях), содержащие ПДн, хранятся в шкафах работников, ответственных за ведение и хранение таких документов.

6.4. Помещения, в которых хранятся персональные данные работников, оборудуются средствами физической защиты (двери, замки, сигнализация).

6.5. Обработка персональных данных в департаменте осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, исполнения работодателем договорных обязательств.

6.6. Допуск к персональным данным разрешен должностным лицам, включенным в Перечень должностей, которым персональные данные необходимы для выполнения конкретных трудовых функций.

6.7. К персональным данным, обрабатываемым в департаменте, могут допускаться работники контрольно-ревизионных органов при наличии документов, являющихся основанием к работе с персональными данными.

6.8. Работники, обрабатывающие персональные данные с использованием и без использования средств автоматизации, обязаны обеспечивать их безопасность от несанкционированного доступа к ним и копирования.

6.9. Работники, допущенные к обработке персональных данных, обязаны:

- осуществлять передачу персональных данных работников в пределах организации в соответствии с Перечнем должностей;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- передавать персональные данные работника представителям работников в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

6.10. Работникам, допущенным к обработке персональных данных, запрещается:

- сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных законодательством Российской Федерации;

- сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

6.11. Защита персональных данных работников от их неправомерного использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном законодательством Российской Федерации.

7. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном законодательством Российской Федерации.

7.2. Персональные данные работников подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении таких целей.

7.3. Уничтожение документов, содержащих персональные данные, производится комиссионно. Комиссия назначается приказом директора департамента. По результатам работы комиссии оформляются акты об уничтожении (Приложение 5).

8. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъекты персональных данных имеют право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законодательством;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства Российской Федерации;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Форма запроса на получение сведений от оператора персональных данных приведена в Приложении 6.

9. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ ПРИ ОБРАБОТКЕ ПДн

9.1. Работники департамента образования и науки при приеме на работу проходят инструктаж относительно принятых в департаменте мер по защите персональных данных и порядке их обработки, после чего дают Согласие на обработку своих ПДн и Обязательство о неразглашении персональных данных и иной конфиденциальной информации (Приложение 7).

9.2. Разглашение персональных данных, то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей, содержащих персональные данные работника; иные нарушения обязанностей по их защите, обработке и хранению влекут наложение дисциплинарного взыскания – выговора, увольнения.

В случае причинения организации ущерба, связанного с нарушением правил обработки и защиты персональных данных работник несёт материальную ответственность в соответствии с п. 7 ч. 1 ст. 243 Трудового кодекса РФ.

В случае незаконного собирания или распространения работником сведений о частной жизни лица, составляющих его личную или семейную тайну, без согласия субъекта ПДн либо распространения этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации он несет уголовную ответственность.

9.3. Представление работником недостоверных сведений является основанием для вынесения дисциплинарных взысканий вплоть до увольнения, если данное действие не содержит состава преступления.

Положение обязательно для всех работников департамента.

В соответствии с требованиями п. 8 ст. 86 Трудового кодекса Российской Федерации, работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

Приложение: 1. Перечень категорий ПДн, обрабатываемых в департаменте;
2. Перечень должностей департамента, имеющих доступ к ПДн;
3. Согласие на обработку ПДн;
4. Заявление на отзыв своих ПДн;
5. Акт о выделении документов на уничтожение;
6. Запрос субъекта ПДн на получение информации;
7. Обязательство о неразглашении.

Приложение 1	**Положение «Обработка и защита персональных данных работников в департаменте образования и науки Костромской области»**	

УТВЕРЖДАЮ

Директор департамента образования и
науки Костромской области
_____ Т.Е. Быстрякова

«___» сентября 2015 г.

ПЕРЕЧЕНЬ
категорий персональных данных, обрабатываемых
в департаменте образования и науки

- фамилия, имя, отчество, дата и место рождения, гражданство;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- адрес регистрации и фактического проживания;
- дата регистрации по месту жительства;
- паспорт (серия, номер, кем и когда выдан);
- паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);
- образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);
- послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и т.п.);
- классный чин федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации, воинское и (или) специальное звание;
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
- места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
- владение иностранными языками и языками народов Российской Федерации;
- пребывание за границей (когда, где, с какой целью);
- номер мобильного телефона или домашнего телефона;
- отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- идентификационный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- наличие (отсутствие) судимости;
- допуск к государственной тайне, оформленный за период работы, службы, учёбы (форма, номер и дата);
- наличие (отсутствие) заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению, подтвержденного заключением медицинского учреждения;
- результаты обязательных медицинских осмотров (обследований) (без использования средств автоматизации);
- сведения о доходах, имуществе и обязательствах имущественного характера;
- сведения о последнем месте государственной или муниципальной службы.
- сведения об изображении лица (без использования средств автоматизации).

Приложение 2	**Положение «Обработка и защита персональных данных работников в департаменте образования и науки Костромской области»**	

УТВЕРЖДАЮ

Директор департамента образования и

науки Костромской области

_____ Т.Е. Быстрякова

«___» сентября 2015 г.

ПЕРЕЧЕНЬ
должностей департамента, имеющих по своим должностным обязанностям доступ к ПДн.

№ п.п.	Должность	Состав персональных данных (ПДн)	Прим.
1	Директор департамента	Персональные данные сотрудников департамента[1], должностных лиц образовательных учреждений и контрагентов, обратившихся граждан РФ и иных субъектов ПДн	
2	Заместители директора – начальники отдела	Персональные данные сотрудников департамента, должностных лиц образовательных учреждений и контрагентов, обратившихся граждан РФ	
3	Начальник отдела - главный бухгалтер	Отдельные категории персональных данных сотрудников департамента, должностных лиц образовательных учреждений и контрагентов, обратившихся граждан РФ	
4	Начальник отдела	Персональные данные должностных лиц образовательных учреждений и контрагентов, обратившихся граждан РФ	
5	Зам. начальника отдела	Персональные данные должностных лиц образовательных учреждений и контрагентов, обратившихся граждан РФ	
6	Главный специалист – эксперт кадрового подразделения	Персональные данные сотрудников департамента, должностных лиц образовательных учреждений и обратившихся граждан РФ	
7	Главный специалист – эксперт	Отдельные категории персональных данных должностных лиц образовательных учреждений и контрагентов, обратившихся граждан РФ	
8	Ведущий специалист-эксперт	Отдельные категории персональных данных должностных лиц образовательных учреждений и контрагентов, обратившихся граждан РФ	
9			
10			

[1] Работа с персональными данными сотрудников осуществляется в служебном помещении кадрового работника и его присутствии

Приложение 3	**Положение «Обработка и защита персональных данных работников в департаменте образования и науки Костромской области»**	

СОГЛАСИЕ

на обработку персональных данных.

Я, _____, паспорт ____ № _____, выдан ___.___.____года _____ проживающий(ая) по адресу: _____ даю своё согласие департаменту образования и науки Костромской области, расположенному по адресу г. Кострома, ул. Ленина, д. 20, (далее Оператор) на обработку (автоматизированную и без использования средств автоматизации) моих персональных данных в целях соблюдения моих конституционных прав (ст. 24 Конституции РФ), исполнения требований федеральных законов, регулирующих работу с персональными данными (Трудовой и Налоговый Кодексы РФ, федеральный закон № 152-ФЗ «О защите персональных данных», иные нормативные акты), в целях содействия мне в обеспечении трудовой деятельности и установленных законодательством условий работы (гарантий и компенсаций), обеспечения моей личной безопасности, обучении и должностном росте, осуществления контроля количества и качества выполняемой работы, а также в целях систематизации производственной деятельности, организации функционального взаимодействия между подразделениями и обеспечения сохранности имущества Оператора, а именно:

- использовать нижеперечисленные данные для формирования кадровых документов и для выполнения Оператором всех требований трудового, налогового, страхового, пенсионного и иного федерального законодательства;
- использовать персональные данные в информационной системе персональных данных Оператора для ведения кадрового и бухгалтерского учёта, осуществления расчетов Оператора со мной как работником;
- использовать мои фамилию, имя, отчество, дату рождения, номера служебного и мобильного телефона, e-mail, адрес проживания в создаваемых справочных и иных информационных документах.

Мои персональные данные, в отношении которых дается согласие, включают в себя:

- Фамилию, имя, отчество;
- Место и дату рождения;
- Паспортные данные (серия, номер паспорта, кем и когда выдан, место регистрации);
- Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, дата начала и завершения обучения, квалификация и специальность, данные о повышении квалификации или переподготовки);
- Сведения о трудовой деятельности (номер, серия, дата выдачи трудовой книжки и вкладышей к ней, данные о записях в трудовой книжке, должностной инструкции, приказах по л/составу, материалах аттестации и оценке трудовой деятельности, об имеющихся государственных и ведомственных наградах и т.п.);
- Сведения о семейном положении;
- Сведения о заработной плате;
- Сведения о воинском учёте военнообязанных лиц (номер военного билета, кем и когда выдан, иные данные);
- Сведения необходимые для определения социального статуса и предоставления социальных льгот (серия, номер, дата выдачи и наименование органа, выдавшего документы, являющиеся основанием для предоставления льгот);
- Сведения о страховом свидетельстве пенсионного страхования (номер СНИЛС);
- Сведения о регистрации в налоговом органе (ИНН);
- Контактные данные (телефонный номер – домашний, мобильный, E-mail);
- Место и адрес проживания;
- Сведения об изображении лица.

Данное согласие вступает в силу со дня его подписания и действует в течение периода моей работы. После моего увольнения Оператор обязан уничтожить мои персональные данные установленным порядком за исключением тех, хранение которых предусмотрено действующим законодательством.

Данное согласие может быть отозвано мною в любое время на основании моего письменного заявления.

_____ дата

_____ подпись

Наименование (Ф.И.О.) оператора

Адрес оператора

Ф.И.О. субъекта персональных данных

Адрес, где зарегистрирован субъект персональных данных

Номер основного документа, удостоверяющего личность

Дата выдачи указанного документа

Наименование органа, выдавшего документ

ЗАЯВЛЕНИЕ

На основании п. 2 ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», отзываю ранее данное мной согласие на обработку персональных данных.

В случае, если согласие на обработку персональных данных давалось мной неоднократно, настоящим я отзываю все ранее данные мной согласия на обработку персональных данных.

В соответствии с п. 5 ст. 21 Федерального закона «О персональных данных», в случае отзыва субъектом персональных данных согласия на их обработку, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва.

Я уведомлен, что в случае отзыва согласия на обработку персональных данных, департамент образования и науки Костромской области вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2÷11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

Уведомление о прекращении обработки и уничтожении моих персональных данных прошу предоставить в письменной форме.

"__" _____ 20__ г.

(подпись) (расшифровка подписи)

УТВЕРЖДАЮ

Директор департамента образования

и науки Костромской области

_____ Т.Е. Быстрякова

«___» сентября 2015 г.

АКТ
о выделении документов на уничтожение

«__» _____ 201__ г. г. Кострома

Комиссия в составе:

председатель комиссии:_____

члены комиссии: _____,

_____,

составила настоящий акт о том, что в результате проведенной экспертной оценки подлежат уничтожению следующие документы, срок хранения которых истек (опись прилагается):

1. Анкеты кандидатов на работу департамента образования и науки за 2012 год (8 анкет).
2. Авансовые отчеты за 2010 год (1 папка).
3. Кассовая книга за 2010 год.

…

Всего: 10 (десять) наименований.

Председатель комиссии: ___ _____ (_____);

Члены комиссии: _____ (_____);

_____ ___ (_____).

УТВЕРЖДАЮ

Директор департамента образования и

науки Костромской области

_____ Т.Е. Быстрякова

«___» сентября 2015 г.

АКТ
об уничтожении документов, срок хранения которых истек

«__» _____ 201__ г. г. Кострома

Комиссия в составе:

председатель комиссии:_____

члены комиссии: _____,

_____,

составила настоящий акт в том, что согласно описи, утвержденной актом от «__» _____ 201__ года, были уничтожены путём сожжения документы, срок хранения которых истек:

1. Анкеты кандидатов на работу департамента образования и науки за 2012 год (8 анкет).
2. Авансовые отчеты за 2010 год (1 папка).
3. Кассовая книга за 2010 год.

Всего: 10 (десять) наименований.

Председатель комиссии: _____ (_____);

Члены комиссии: _____ (_____);

_____ (_____).

Приложение 6	**Положение «Обработка и защита персональных данных работников в департаменте образования и науки Костромской области»**	

_____
Наименование (Ф.И.О.) оператора

_____
Адрес оператора

_____
Ф.И.О. субъекта персональных данных

_____
Адрес, где зарегистрирован субъект персональных данных

_____
Номер основного документа, удостоверяющего личность

_____
Дата выдачи указанного документа

_____
Наименование органа, выдавшего документ

ЗАПРОС

на получение информации о персональных данных

«___» _____ 201_ г. я был принят на работу в департамент образования и науки Костромской области, со мной был заключен служебный контракт № _____, тогда же мной было дано согласие на обработку моих персональных данных.

В соответствии со ст. 14 Федерального закона «О персональных данных» прошу предоставить мне следующие сведения:

1) Перечень конкретных персональных данных, относящихся ко мне, и источники получения этих персональных данных.

2) Какие лица (за исключением сотрудников компании) имеют или могут иметь доступ к моим персональным данным.

Указанную информацию прошу предоставить мне в письменной форме.

В соответствии с п. 1 ст. 20 Федерального закона «О персональных данных», указанная информация должна быть предоставлена в течение тридцати рабочих дней со дня получения настоящего запроса.

«__» _____ 201__ г.

_____ _____
(подпись) (расшифровка подписи)

ОБЯЗАТЕЛЬСТВО

о неразглашении персональных данных и иной конфиденциальной информации

Я, _____ ,
(Фамилия, имя, отчество)

уведомлен(а), что в процессе работы в департаменте образования и науки Костромской области получу доступ к конфиденциальной информации, в том числе, к отдельным категориям персональных данных сотрудников департамента, должностных лиц подведомственных образовательных организаций и контрагентов, граждан РФ, обратившихся в департамент.

Я подтверждаю, что ознакомлен(а) с Положением об обработке персональных данных и иными нормативными документами, определяющими порядок обработки (сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение) и защиты сведений, относимых к конфиденциальной информации.

Я подтверждаю, что не имею никаких обязательств перед каким-либо третьим лицом (физическим или юридическим), которые входят в противоречие с настоящим Обязательством, и обязуюсь в период трудовых отношений с департаментом образования и науки Костромской области и после их окончания:

- не разглашать и не передавать третьим лицам информацию, содержащую персональные данные, а также иные конфиденциальные сведения, которые мне будут доверены или станут известны по государственной гражданской службе при выполнении моих трудовых обязанностей;
- выполнять требования локальных нормативных актов и руководящих документов по обеспечению защиты информации в части меня касающейся;
- сообщать непосредственному руководителю о случаях попытки посторонних лиц получить от меня защищаемые сведения;
- сохранять ставшую мне известной в связи с осуществлением государственной гражданской службы конфиденциальную информацию;
- сообщать непосредственному руководителю о фактах утраты или обнаружении недостачи материальных носителей конфиденциальной информации, а также утраты иных атрибутов (ключей от хранилищ, сейфов, режимных помещений и т.п.), которые могут привести к разглашению или утечке защищаемой информации;
- в случае моего увольнения передать непосредственному руководителю все имеющиеся материальные носители конфиденциальной информации, находящиеся в моём распоряжении в связи с исполнением обязанностей государственной гражданской службы, на которых хранится или может храниться конфиденциальная информация.

Мне известно, что в случае невыполнения мной любого из вышеперечисленных пунктов настоящего Обязательства в отношении меня могут быть применены меры ответственности, предусмотренные трудовым, административным и уголовным законодательством Российской Федерации, включая обязанность по возмещению всех причиненных убытков.

Работник

_____
(подпись)

_____
(Фамилия, имя отчество)

«____»_____201__ г.

РД-03	Положение об экспертной комиссии департамента образования и науки Костромской области	

УТВЕРЖДАЮ

Директор департамента образования и науки Костромской области

_____ Т.Е. Быстрякова

«1» сентября 2015 г.

ПОЛОЖЕНИЕ
об экспертной комиссии департамента

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Экспертная комиссия (далее ЭК) образована в целях организации и проведения работы по экспертизе ценности документов, включая управленческую, кадровую и иную коммерческую документацию, в том числе содержащую персональные данные, подготовки её к уничтожению или передаче в архивы на хранение в соответствии с требованиями Федерального законодательства. Экспертная комиссия является совещательным органом.

1.2. В своей деятельности комиссия руководствуется настоящим Положением, требованиями Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 15.09.2008 № 687 «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», руководящими документами архивного фонда РФ[1], регулирующими деятельность организации в сфере документооборота.

1.3. Экспертная комиссия назначается приказом директора департамента образования и науки Костромской области и состоит из числа наиболее квалифицированных специалистов и сотрудников, имеющих отношение к работе с документами, содержащими персональные данные, к обработке конфиденциальной информации и обеспечению информационной безопасности департамента.

2. ФУНКЦИИ ЭКСПЕРТНОЙ КОМИССИИ

Экспертная комиссия организации осуществляет следующие функции:

[1] ФЗ РФ от 22.10.2004 № 125-ФЗ «Об архивном деле в РФ»

2.1. На регулярной основе проводит заседания комиссии и рассматривает вопросы о порядке обработки в департаменте персональных данных и иной конфиденциальной информации; вопросы, регламентирующие порядок учёта, хранения и уничтожения материальных и электронных носителей информации ограниченного распространения.

2.2. Ежегодно отбирает конфиденциальные документы организации (дела, журналы, книги) для проведения экспертизы ценности документов и принятия решения об их уничтожении либо дальнейшем хранении.

2.3. Выносит в установленном порядке предложения об одобрении и представлении на утверждение директора департамента сводных описей дел постоянного и описей дел долговременного (свыше 10 лет) хранения, в том числе по личному составу.

2.4. Готовит протоколы заседания комиссии и акты о выделении к уничтожению документов, сроки которых истекли *(Приложения 1, 2, 3)*.

2.5. Осуществляет на плановой основе внутренний контроль за вопросами организации работы с документами, содержащими персональные данные, и соблюдением установленного режима их обработки.

2.6. Принимает непосредственное участие в подготовке ежегодной номенклатуры дел конфиденциального делопроизводства департамента.

2.7. Выносит на рассмотрение руководства организации предложения об изменении сроков хранения отдельных видов документов, установленных действующими перечнями Росархива, и определении сроков хранения документов, не предусмотренных перечнями.

3. ПРАВА ЭКСПЕРТНОЙ КОМИССИИ

Экспертной комиссии в процессе своей деятельности предоставляется право:

3.1. Консультировать работников, имеющих отношение к обработке персональных данных, по вопросам ведения конфиденциального делопроизводства, учёта документов и подготовки их к передаче в архив предприятия или уничтожения.

3.2. Осуществлять контроль и требовать от сотрудников организации:

- выполнения установленного порядка работы с документами, содержащими персональные данные;
- розыска отсутствующих дел, подлежащих передаче на хранение в архив;
- представления письменных объяснений по фактам утраты дел и документов.

3.3. Приглашать в качестве консультантов и экспертов на свои заседания специалистов в области документационного обеспечения и архивоведения из администрации Костромской области и подведомственных ей учреждений.

3.4. Запрашивать от специалистов предприятия сведения и необходимые заключения для определения ценности документов и сроков их хранения.

3.5. Оказывать информационно-методическое содействие в вопросах обеспечения безопасности обрабатываемых в информационных системах сведений ограниченного распространения.

3.6. На регулярной основе информировать руководителя организации о состоянии работы комиссии по рассматриваемым вопросам, входящим в сферу компетенции комиссии.

4. ОРГАНИЗАЦИЯ РАБОТЫ ЭКСПЕРТНОЙ КОМИССИИ

4.1. Экспертная комиссия осуществляет свою деятельность в непосредственном контакте с руководителем ЗАО «Костромской автовокзал», получая от него необходимые организационно-методические указания.

4.2. Вопросы, относящиеся к деятельности и компетенции комиссии, рассматриваются на её заседаниях, которые проводятся по мере необходимости, но не реже 2-х раз в год.

4.3. Решения экспертной комиссии по рассматриваемым вопросам принимаются открытым голосованием большинством голосов.

4.4. Заседания комиссии протоколируются. Документирование работы комиссии и формирование дел с материалами её заседаний, возлагается на секретаря или одного из членов комиссии.

Приложение: 1. Форма Протокола заседания экспертной комиссии;
2. Форма Акта о выделении документов на уничтожение материальных носителей персональных данных и иной конфиденциальной информации;
3. Форма Акта об уничтожении электронных носителей конфиденциальной информации;

Приложение 1	**Положение об экспертной комиссии департамента образования и науки Костромской области»**	

УТВЕРЖДАЮ

Директор департамента образования и

науки Костромской области

_____ Т.Е. Быстрякова

«___» сентября 2015 г.

ПРОТОКОЛ № ___

заседания экспертной комиссии

«___»_____201_ года г. Кострома

Комиссия в составе:

- председателя комиссии – _____,
- членов комиссии – _____;
- секретаря комиссии – _____на очередном заседании рассмотрела следующие вопросы:

1. Об уничтожении материальных носителей конфиденциальной информации, в том числе персональных данных, цели обработки которой достигнуты;
2. Определение порядка работы с документами и материальными носителями персональных данных кандидатов, надобность в которых миновала.

По первому вопросу слушали _____, которая довела до членов комиссии о необходимости уничтожения материальных носителей персональных данных содержащихся в _____.

В ходе обсуждения данного вопроса были высказаны предложения о необходимости уничтожения материальных носителей конфиденциальной информации в соответствии с требованиями ФЗ «О персональных данных»

Внесенные предложения были приняты к исполнению.

Результаты голосования по первому вопросу:

ЗА: - ___; ПРОТИВ: - 0 ; ВОЗДЕРЖАЛИСЬ: - 0.

По второму вопросу слушали _____, которая(ый) предложил в качестве основных направлений деятельности комиссии включить рассмотрение вопросов совершенствования организации работы по защите персональных данных работников и принятия решений о дальнейшей судьбе документов и материалов, образующихся в процессе деятельности организации.

В ходе обсуждения данного вопроса поступили предложения одобрить предложенные направления.

Результаты голосования по первому вопросу:

ЗА: - ___; ПРОТИВ: - 0 ; ВОЗДЕРЖАЛИСЬ: - 0.

Секретарь комиссии: _____

"___"_____ 201__ г. Подписи: 1. _____

2. _____

3. _____

Приложение 2	**Положение об экспертной комиссии департамента образования и науки Костромской области»**	

УТВЕРЖДАЮ

Директор департамента образования и

науки Костромской области

_____ Т.Е. Быстрякова

«___» сентября 2015 г.

АКТ

о выделении документов на уничтожение

«__» _____ 201__ г. г. Кострома

Комиссия в составе:

председатель комиссии: _____,

члены комиссии: _____,

_____,

_____,

составила настоящий акт о том, что в результате проведенной экспертизы подлежат уничтожению документы, цели обработки которых дости*гнуты (срок хранения которых истек, не представляющие исторической ценности)*(опись прилагается):

1. *Анкеты кандидатов на работу за 2014 год (8 анкет).*
2. *Авансовые отчеты за 2010 год (1 папка).*
3. *Кассовая книга за 2010 год.*

…

Всего: _____*(тридцать)* наименований документов.

Председатель комиссии: _____,

Члены комиссии: _____,

_____,

_____.

Приложение 3	**Положение об экспертной комиссии департамента образования и науки Костромской области»**	

УТВЕРЖДАЮ

Директор департамента образования и

науки Костромской области

_____ Т.Е. Быстрякова

«___» сентября 2015 г.

АКТ

Об уничтожении документов, срок хранения которых истек

«__» _____ 201__ г. г. Кострома

Комиссия в составе:

председатель комиссии: _____,

члены комиссии: _____,

_____,

_____,

составила настоящий акт в том, что согласно описи, утвержденной Актом о выделении документов на уничтожение от «___» _____ 201__ года, были уничтожены путём сожжения документы, цели обработки которых достигнуты (либо срок хранения которых истек, либо не представляющих исторической ценности).

Председатель комиссии: _____,

Члены комиссии: _____,

_____,

_____.

РД-05	**Правила осуществления внутреннего контроля департамента образования и науки Костромской области**	

УТВЕРЖДАЮ

Директор департамента образования и

науки Костромской области

_____ Т.Е. Быстрякова

«__1__» сентября 2015 г.

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям нормативных документов

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны на основании требований пункта 4 части 1 ст. 18.1 и пункта 1 части 4 ст. 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и п. б ст.1 Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

1.2. В соответствии с законодательством Оператор ПДн обязан осуществлять внутренний контроль принятых мер, необходимых и достаточных для обеспечения безопасной обработки персональных данных и иной конфиденциальной информации, обрабатываемой в организации.

1.3. Оператор ПДн самостоятельно с учётом штатной структуры департамента, установленного порядка обработки персональных данных (их сбора, хранения, модификации, передачи, распространения и уничтожения), а также параметров автоматизированной информационной системы, в которой обрабатывается конфиденциальная информация, определяет состав и перечень режимных, правовых, криптографических и технических мер для обеспечения её защиты.

1.4. Мероприятия по осуществлению внутреннего контроля проводятся на плановой основе в соответствии с утверждаемыми директором департамента ежегодными планами.

2. ОСНОВНЫЕ НАПРАВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

В соответствии с требованиями федерального законодательства, регулирующего сферу обработки персональных данных и иной конфиденциальной информации регулярному контролю подвергаются:

2.1. Исполнение требований обработки персональных данных, установленных внутренними нормативными документами (Правилами, Положениями, Инструкциями, Порядками).

2.2. Контроль соответствия категорий персональных данных, обрабатываемых в подразделениях департамента, заявленным в Перечне персональных данных утвержденном актом руководителя.

2.3. Соответствие должностей служащих и сотрудников муниципального органа, замещение которых предусматривает обработку персональных данных, заявленному в утвержденном актом директора департамента Перечне должностей.

2.4. Выполнение порядка допуска работников департамента к обработке персональных данных и иной конфиденциальной информации с использованием средств автоматизации и без использования таковых.

2.5. Выполнение работниками департамента требований по обеспечению безопасного хранения материальных и электронных носителей персональных данных и доступа к ним посторонних лиц.

2.6. Реализация исполнения требований учётной политики при работе с материальными и электронными носителями.

2.7. Выполнение установленных режимных требований, правил доступа к местам хранения и обработки конфиденциальной информации, в том числе персональных данных.

2.8. Соответствие требований принятых для ИСПДн мер технической защиты требованиям, предусмотренным приказом ФСТЭК РФ от 18.02.2013 г. № 21, в соответствии с актуальными угрозами и определённым уровнем защищенности персональных данных.

2.9. Исполнение порядка ознакомления работников департамента с нормативными документами, регламентирующими безопасную обработку персональных данных;

2.10. Выполнение порядка и сроков обработки поступающих в департамент запросов от субъектов ПДн.

2.11. Проверка соответствия условий и режима обработки персональных данных, внесенных в реестр Операторов ПДн, действительному положению. Внесение, при необходимости, изменений в направленное ранее Уведомление об обработке ПДн.

3. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ

3.1. Осуществление мероприятий внутреннего контроля проводится строго в соответствии с установленными в Плане сроками и обязательной отметкой о выполненном мероприятии.

3.2. Контрольные проверки могут осуществляться лицом, ответственным за организацию обработки персональных данных самостоятельно либо с привлечением должностных лиц, имеющих допуск к обработке персональных данных в соответствии с профилем проводимого мероприятия.

3.3. При необходимости по распоряжению руководства организации могут проводиться внеплановые проверки по различным направлениям порядка обработки и защиты персональных данных.

3.4. За нарушение требований действующего законодательства, виновные несут ответственность в соответствии со ст. 24 Федерального закона от 27.07.2006 г. № 152 ФЗ «О персональных данных».

РД-04	**Правила рассмотрения запросов субъектов ПДн департамента образования и науки Костромской области**	

УТВЕРЖДАЮ

Директор департамента образования и науки Костромской области

_____ Т.Е. Быстрякова

«1» сентября 2015 г.

ПРАВИЛА
рассмотрения запросов субъектов ПДн

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны в соответствии с требованиями федеральных законов от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», от 27.07.2006 г. № 152-ФЗ «О персональных данных» и определяют порядок и сроки рассмотрения обращений субъектов персональных данных в департаменте образования и науки Костромской области.

1.2. В соответствии со ст. 14 Федерального закона «О персональных данных» любой гражданин либо субъект ПДн имеет право обратиться к Оператору персональных данных (Оператор ПДн) за получением информации, касающейся обработки его персональных данных в департаменте образования и науки Костромской области и получить исчерпывающий ответ о порядке её обработки.

1.3. Требуемые сведения могут предоставляются субъекту персональных данных устно - при личном обращении или письменно - по его письменному запросу. При обращении гражданина либо субъекта ПДн с письменным запросом пишется запрос, который должен содержать обязательные реквизиты документов, подтверждающих законность его обращения (номер основного документа, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором ПДн (например, № договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), а также подпись субъекта персональных данных или его законного представителя, дату обращения и адрес, по которому необходимо направить ответ.

1.4. Субъект ПДн находящийся на государственной гражданской службе в департаменте также вправе требовать от Оператора ПДн информации о порядке обработки своих персональных данных, а при необходимости, их уточнения, блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

В этом случае Оператор ПДн обязан в срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн сведений, подтверждающих, что эти сведения являются неполными, неточными или неактуальными, внести необходимые изменения (в том числе уничтожить) в существующие базы данных или на материальные носители. После чего Оператор ПДн обязан уведомить субъекта персональных данных о внесенных изменениях и предпринятых мерах, а также принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были ранее переданы.

1.5. При отзыве субъектом персональных данных согласия на обработку своих персональных данных (после увольнения либо перехода на другую работу) Оператор ПДн обязан прекратить их обработку и в случае, если сохранение персональных данных больше не требуется, уничтожить персональные данные в срок, не превышающий тридцати дней с момента регистрации указанного отзыва.

2. ПОРЯДОК РАССМОТРЕНИЯ ОБРАЩЕНИЯ СУБЪЕКТА ПДн

2.1. Поступившее обращение субъекта персональных данных (письменный запрос или устное обращение) по вопросу обработки его персональных данных подлежит обязательной регистрации в Журнале учёта обращений субъектов персональных данных *(Приложение 1)* и рассмотрению в течение трех дней с момента поступления.

2.2. Руководитель организации при поступлении запроса от субъекта персональных данных в своей резолюции назначает сотрудника, ответственного за рассмотрение запроса и подготовку ответа на поступившее обращение.

2.3. При этом руководитель или лицо, принимающее обращение от субъекта, обязано довести до заявителя информацию о порядке и сроках рассмотрения обращения, подтвердив либо опровергнув факт обработки его персональных данных Оператором ПДн.

2.4. При подготовке письменного ответа сотрудник Оператора ПДн обязан:

2.4.1. Предоставить при необходимости возможность личного ознакомления с имеющимися у Оператора ПДн персональными данными, в том числе:

- о составе обрабатываемых персональных данных, относящихся к соответствующему субъекту персональных данных, источнике их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- о правовых основаниях и целях обработки персональных данных;
- о применяемых оператором способах обработки персональных данных;
- о сроках и порядке обработки персональных данных, в том числе сроках их хранения и уничтожения;
- о наименовании и месте нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- о наименовании или фамилии, имени, отчестве и адресе лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- об иных сведениях, предусмотренных Федеральным законодательством или иными нормативными актами.

2.4.2. Подготовить в течение тридцати дней с даты регистрации запроса письменный ответ и направить его субъекту персональных данных (при определенных обстоятельствах заказным письмом).

2.5. В случае отказа в предоставлении информации субъекту персональных данных Оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение Федерального законодательства, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных.

2.6. В случае, если указанные сведения были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору не ранее чем через 30 (тридцать) дней после первоначального обращения.

3. ПОРЯДОК РАССМОТРЕНИЯ ИНЫХ ОБРАЩЕНИЙ ГРАЖДАН

3.1. Поступившее обращение гражданина по вопросам, не связанным с обработкой ПДн осуществляется в соответствии с требованиями федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и установленным в департаменте порядком.

3.2. Каждое поступившее в департамент письменное обращение гражданина регистрируется и передается на рассмотрение директору для определения исполнителя. Сотрудник, которому поступило на рассмотрение обращение гражданина, принимает необходимые меры для сбора информации по рассматриваемому вопросу и подготовки ответа заявителю. После подготовки письменного ответа заявителю ответственный сотрудник департамента обязан зарегистрировать его в Журнале подготовленных документов.

3.3. Срок рассмотрения и подготовки ответа составляет 30 суток. При необходимости получения дополнительных материалов изучения по рассматриваемому обращению и невозможности ответить гражданину в установленный срок, срок подготовки ответа может быть продлен директором департамента (не более 15 суток).

3.4. При невозможности подготовки квалифицированного и полного ответа в сроки, предусмотренные законодательством, ответственное лицо, исполняющее обращение, обязано сообщить заявителю информацию о причинах невозможности подготовки ответа и окончательных сроках рассмотрения обращения.

4. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОРЯДКА

4.1. Нарушение установленного законодательством Российской Федерации порядка рассмотрения обращений граждан влечет наложение административного штрафа в соответствии со статьями Кодекса Российской Федерации об административных правонарушениях.

Приложение: 1. Журнал учёта обращений субъектов персональных данных.

УТВЕРЖДАЮ

Директор департамента образования и

науки Костромской области

_____ Т.Е. Быстрякова

«___» сентября 2015 г.

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана в соответствии с требованиями п. 1) ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Положения об обработке персональных данных в департаменте образования и науки Костромской области.

1.2. Инструкция определяет права и обязанности ответственного за организацию обработки персональных данных в департаменте.

1.3. Ответственный за организацию обработки персональных данных в департаменте назначается приказом директора департамента из числа наиболее подготовленных сотрудников.

1.4. Ответственный за организацию обработки персональных данных в своей деятельности руководствуется положениями статьи 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также требованиями иных законодательных актов, регламентирующих обработку ПДн *(Приложение 1).*

2. ПРАВА ОТВЕТСТВЕННОГО ЛИЦА

Сотрудник, ответственный за организацию обработки персональных данных имеет право:

- осуществлять контроль исполнения требований внутренних нормативных документов, регламентирующих обработку персональных данных с использованием средств автоматизации и без их использования, всеми сотрудниками департамента;

- вносить директору департамента предложения по изменению и совершенствованию деятельности департамента в сфере обеспечения безопасной обработки персональных данных сотрудников, членов их семей работников, должностных лиц подведомственных организаций и контрагентов, субъектов ПДн и граждан РФ;

- подавать заявки руководству департамента об обучении по вопросам технической защиты информации и безопасной обработки персональных данных.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЛИЦА

Сотрудник, ответственный за организацию обработки персональных данных обязан:

- изучить и знать законодательство Российской Федерации в сфере обработки персональных данных[1];

- принимать активное участие в разработке внутренних нормативных документов, определяющих политику в отношении обработки персональных данных, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации и устранение последствий таких нарушений, а также поддерживать их в актуальном состоянии;

- уведомлять уполномоченный орган по защите прав субъектов персональных данных об изменениях сведений, касающихся обработки персональных данных, а также в случае прекращения обработки персональных данных в течение десяти рабочих дней с момента возникновения таких изменений или с момента прекращения обработки персональных данных;

- разрабатывать комплекс правовых, организационных и технических мер по обеспечению безопасности персональных данных, обрабатываемых на предприятии;

- составлять планы работы по организации безопасной обработки конфиденциальной информации, осуществлять плановый контроль исполнения

[1]Ст.23-24 Конституции РФ, Федеральные законы РФ от 27.07.2006 № 152-ФЗ «О персональных данных»; от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; от 09.02.2007 № 16-ФЗ «О транспортной безопасности»; Постановления правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»и от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»; Положения главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников»;Приказа Минтранса РФ от 19.07.2012 № 243 «Об обеспечении Порядка формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах, а также предоставления содержащихся в них данных» и иных нормативных документов.

установленных требований обработки персональных данных, их соответствие политике департамента в отношении обработки персональных данных;

- оценивать вред, который может быть причинен субъектам персональных данных в случае нарушения требований к обеспечению безопасности персональных данных;

- анализировать соответствие принимаемых мер защиты актуальности вероятных угроз, направленных на ослабление безопасности обрабатываемых ПДн;

- доводить до сведения сотрудников департамента требования законодательства Российской Федерации по вопросам обработки персональных данных, требований к их защите;

- организовать порядок обработки обращений и запросов субъектов персональных данных или их законных представителей и (или) осуществлять контроль за порядком приёма и обработки таких обращений и запросов;

- осуществлять внутренний контроль соблюдения работниками установленных требований законодательства Российской Федерации.

4. ОСУЩЕСТВЛЕНИЕ ВНУТРЕННЕГО КОНТРОЛЯ

Внутренний контроль соответствия порядка обработки персональных данных требованиям законодательства в департаменте осуществляется на основании ежегодно составляемого Плана проведения внутренних проверок состояния защиты персональных данных *(Приложение 2)*.

План утверждается руководителем организации и предусматривает работу по следующим основным направлениям:

- контроль выполнения требований по организации допуска сотрудников к работе с персональными данными субъектов ПДн;

- контроль выполнения требований по организации допуска сотрудников к работе с информационными ресурсами департамента и государственных информационных систем;

- контроль исполнения требований Положения об обработке персональных данных в части ознакомления вновь принимаемых работников с внутренними нормативными актами;

- проверка наличия и порядка использования работникам и учтённых электронных носителей информации;

- проверка исполнения работниками подразделений требований обработки персональных данных, осуществляемой без использования средств автоматизации;

- контроль исполнения порядка рассмотрения обращений поступивших в организацию от субъектов ПДн, в том числе сотрудников правоохранительных органов;
- порядок отбора и уничтожения материальных носителей информации, содержащих персональные данные, по достижении цели обработки.

При необходимости (изменение порядка и условий обработки, штатные перемещения и т.п.) контроль может проводиться внепланово (внезапно).

Плановые и внезапные проверки проводятся сотрудником, ответственным за организацию обработки персональных данных, совместно с членами экспертной комиссии департамента.

О проведении мероприятий внутреннего контроля делается отметка в соответствующей графе Плана. При выявлении недостатков или нарушений разрабатываются меры по их устранению и локализации с назначением лиц, ответственных за выполнение конкретных мероприятий (в данном случае на имя директора департамента готовится служебная записка).

Если выявленные недостатки содержат признаки правонарушения, виновные привлекаются к дисциплинарной ответственности.

Приложение: 1. Перечень нормативных документов, являющихся правовой базой в сфере безопасной обработки ПДн;
2. форма Плана проведения проверок внутреннего контроля.

Приложение 1

ПЕРЕЧЕНЬ ДОКУМЕНТОВ,
являющихся нормативно-правовой базой в сфере безопасной обработки конфиденциальной информации.

№ п/п	Наименование документа
1	Конституция Российской Федерации (ст. 23, 24)
2	Стратегия развития информационного общества в Российской Федерации (Распоряжение президента от 7.02.2008 № Пр-212)
3	Федеральный закон РФ от 12.08.1995 № **144-ФЗ** «Об оперативно-розыскной деятельности», ст.6, ст.15.
4	**Федеральный закон РФ** от 30.12.2001 № **197-ФЗ** (глава 14 ТК О защите ПДн)
5	Федеральный закон РФ от 27.12.2002 № **184-ФЗ** «О техническом регулировании».
6	Федеральный закон РФ от 18.12.2003 № 230-ФЗ Гражданский Кодекс (ч.IV - защита прав)
7	**Федеральный закон РФ** от 29.07.2004 № **98-ФЗ** «О коммерческой тайне»
8	**Федеральный закон РФ** от 27.07.2006 № **149-ФЗ** «Об информации, информационных технологиях и о защите информации»
9	**Федеральный закон РФ** от 27.07.2006 № **152-ФЗ** «О персональных данных»
10	**Федеральный закон РФ** от 09.02.2007 **№ 16-ФЗ** «О транспортной безопасности»
11	**Федеральный закон РФ** от 06.04.2011 **№ 63** «Об электронной подписи»
12	Федеральный закон РФ от 28.12.2010 № 390-ФЗ «О безопасности»
13	Федеральный закон РФ от 25.07.1998 № 128-ФЗ "О государственной дактилоскопической регистрации в Российской Федерации"
14	Указ Президента РФ от 06.03.1997 года № **188** «Об утверждении Перечня сведений конфиденциального характера»
15	**Постановление Правительства РФ** от 15.09.2008 **№ 687** «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
16	**Постановление Правительства** РФ от 16.03.2009 **№ 228** «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»
17	**Постановление Правительства РФ** от 21.03.2012 **№ 211** «Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом **«О персональных данных»** и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

18	**Постановление Правительства РФ** от 01.11.2012 **№ 1119** «Требования к защите ПДн при обработке в ИС»
19	**Приказ ФСБ РФ** от 09.02.2005 **№ 66** «Положение о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (Положение **ПКЗ-2005)**
20	**Приказ ФСБ РФ** от 21.02.2008 № 149/54-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в ИСПДн с использованием средств автоматизации»
21	**Приказ ФСБ РФ** от 10.07.2014 **№ 378** « Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации»
22	**Приказ ФСТЭК** от 18.02.2013 № **21** «« Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
23	**Приказ Минтранса** от 19.07.2012 № 243 «О порядке формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах, а также предоставления содержащихся в них данных»
24	**ГОСТ Р ИСО/МЭК 15408-2002**. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
25	**ГОСТ Р 51275-2006** Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения (дата введения с 01.02.2008 г).
26	ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
27	**ГОСТ Р 50922** Защита информации. Основные термины и определения
28	**ГОСТ Р 51583**-2000 Порядок создания АС в защищенном исполнении
29	ГОСТ Р 52069.0 - Защита информации. Система стандартов. Основные положения.
30	ГОСТ Р 53114-2008 - Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
31	ГОСТ Р 51897 - Менеджмент риска. Термины и определения.
32	ГОСТ Р 51898 - Аспекты безопасности. Правила включения в стандарты.
33	ГОСТ Р ИСО/МЭК 13335-1 - Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
34	ГОСТ Р ИСО/МЭК 13335-3 - Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных

УТВЕРЖДАЮ

Директор департамента образования
и науки Костромской области

_____ Т.Е. Быстрякова

1 сентября 2015

ПРАВИЛА
работы с информационными системами департамента образования и науки Костромской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила определяют основные принципы безопасной работы автоматизированных информационных систем департамента и обработки конфиденциальной информации сотрудниками департамента.

1.2. Целью данного документа является формализация требований, предъявляемых к сотрудникам, по обеспечению режима безопасности конфиденциальной информации, циркулирующей в информационных системах, в том числе при обработке персональных данных.

1.3. Правила разработаны в соответствии с требованиями Федеральных законов РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и иных нормативных актов.

2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированное рабочее место пользователя (далее АРМ) – персональный компьютер с предустановленным системным, прикладным и антивирусным программным обеспечением (далее ПО), в том числе предназначенным для защиты информации ограниченного распространения.

Информационная система персональных данных (далее ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Информационные ресурсы – программное обеспечение, документы и массивы документов расположенные, хранящиеся и обрабатываемые в информационных системах;

Интернет – всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных (телекоммуникационная сеть общего пользования);

Пользователь – сотрудник, допущенный к работе на автоматизированном рабочем месте и использующий для исполнения своих должностных обязанностей средства вычислительной техники;

Персональный компьютер (далее ПК) - компьютер, с предустановленным системным, прикладным и антивирусным ПО и предназначенный для эксплуатации одним пользователем, то есть для личного использования;

Электронная почта – технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети;

Flash-карта – разновидность твердотельной полупроводниковой энергонезависимой перезаписываемой памяти (один из видов электронных носителей информации).

3. ОБЩИЕ ПРАВИЛА РАБОТЫ НА АРМ

3.1. В целях исполнения своих служебных обязанностей, сотруднику департамента (пользователю) на период работы предоставляется автоматизированное рабочее место с предустановленным лицензионным системным, прикладным и антивирусным программным обеспечением, имеющим сертификаты соответствия по безопасности.

Для организации доступа пользователя к информационным ресурсам АИС его АРМ подключается к локальной вычислительной сети (далее ЛВС). Установку и настройку АРМ, а также подключение ПК к ЛВС выполняет Администратор безопасности.

3.2. Допуск пользователя к АРМ осуществляется по устной заявке директора департамента (либо его заместителя) на основании утвержденного Перечня должностей, имеющих право доступа к обработке конфиденциальной информации, в том числе персональных данных.

Доступ пользователя к работе на АРМ осуществляется на основании индивидуальной учетной записи (Логин + Пароль). Пользователь обязан использовать пароль в соответствии со следующими требованиями:

- длина пароля должна быть не менее 8 символов;
- пароль должен состоять из строчных и прописных букв, а также небуквенных символов (т.е. цифр, знаков пунктуации, специальных символов);
- пароль не должен быть легко угадываемым (не должен включать повторяющуюся последовательность каких-либо символов (например, "11111111", "абвгдеё" и т.п.), пароль не должен включать в себя легко подбираемые сочетания символов (имена, фамилии, даты рождения знакомых, наименования городов и улиц, клички домашних животных и т.п.), а также общепринятые сокращения (ЭВМ, ЛВС и т.п.).

3.3. Пользователь обеспечивает безопасное хранение пароля, исключающее возможность его утери или разглашения. Срок использования пароля составляет не более 90 дней. При смене пароля новое значение должно отличаться от предыдущего не менее чем в трёх-четырёх позициях.

3.4. При необходимости оставить рабочее место, даже на короткое время, пользователь должен заблокировать доступ к АРМ, нажав одновременно Ctrl + Alt + Delete, и принять иные меры по ограничению доступа к отображаемой на экране монитора информации.

3.5. При использовании телекоммуникационных возможностей сети общего пользования Интернет пользователи обязаны выполнять следующие требования:

- использовать ресурсы Интернет только для выполнения своих служебных обязанностей;
- не посещать ресурсы Интернет, содержащие материалы противозаконного, экстремистского или неэтичного характера, а также использовать доступ к социальным сетям Интернет и развлекательным сайтам;
- не размещать в сети Интернет информацию служебного характера, о её сотрудниках и решаемых задачах, если это не связано с выполнением служебных обязанностей;
- не использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) видео-, аудио- и информационных материалов, защищенных авторским правом;

3.6. При работе с электронной почтой пользователи должны соблюдать следующие требования:

- запрещается использовать возможности электронной почты для отправки сообщений противозаконного (террористического, экстремистского или

враждебного характера), а также содержащего в себе информацию неэтичного содержания;

- при получении электронных сообщений из незнакомого источника и/или сомнительного содержания не следует открывать файлы, вложенные в сообщение, так как они с большой долей вероятности могут содержать вирусы. Такие сообщения необходимо удалять;

- не отвечать на подозрительные письма и, тем более, сообщать любые данные о себе и сотрудниках.

3.7. По окончании рабочего времени при отсутствии служебной необходимости пользователь обесточивает АРМ и другую оргтехнику во избежание выхода её из строя и в целях обеспечения противопожарной безопасности.

3.8. В случае подозрения на компрометацию пароля доступа необходимо немедленно изменить пароль и проинформировать об этом своего непосредственного руководителя.

В процессе эксплуатации АРМ пользователям **ЗАПРЕЩАЕТСЯ**:

3.9. Открывать корпус системного блока и вносить изменения в конфигурацию ПК;

3.10. Без получения санкции руководителя и администратора безопасности изменять настройки программного обеспечения и параметры доступа к информационным ресурсам;

3.11. Отключать и изменять параметры настройки в установленное антивирусное программное обеспечение и иные средства защиты информации;

3.12. Подключать к АРМ неучтенные внешние запоминающие устройства (активное сетевое оборудование, незарегистрированные Flash-карты. НЖМД, смартфоны, фотоаппараты и т.д.), если это не связано с исполнением должностных обязанностей сотрудника;

3.13. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты для организации несанкционированного доступа к обрабатываемым информационным ресурсам. При обнаружении такого рода ошибок необходимо информировать своего непосредственного руководителя и администратора безопасности;

3.14. Осуществлять действия направленные на преодоление систем безопасности, получение несанкционированного доступа к ресурсам информационной сети и перехват информации, циркулирующей в ИС;

3.15. Оставлять оборудование АРМ, переносные компьютеры и средства хранения информации без личного присмотра, в случаях, если это может привести к их краже;

При наличии риска хищения ПК и (или) средств хранения информации, необходимо принять меры по их минимизации (например, убирать переносной компьютер на обеденный перерыв и после завершения рабочего дня в закрывающийся на ключ шкаф, не оставлять незакрытым помещение, в котором находится оборудование информационной системы, использовать замки для переносных компьютеров);

3.16. Осуществлять обработку конфиденциальной информации на ПК, не оснащенном принятыми в департаменте средствами защиты информации, а также в присутствии лиц, не имеющих права доступа к данной информации, если при этом указанные лица могут ознакомиться с обрабатываемой информацией;

3.17. Записывать и хранить конфиденциальную информацию на неучтённых носителях информации (Flash-карта, CD-диск, носимый HDD и т.п), а также оставлять без личного присмотра на рабочем месте или где бы то ни было носители информации и распечатки, содержащие подобную информацию;

3.18. Допускать к работе на ПК лиц, не имеющих прав доступа к информационным ресурсам;

4. ПОРЯДОК РАБОТЫ С ИНФОРМАЦИОННОЙ СИСТЕМОЙ

4.1. При работе с программными и техническими средствами, входящими в состав АРМ и информационной системы, пользователь обязан выполнять установленные правила их эксплуатации. За неисполнение установленных правил он несёт персональную ответственность.

4.2. Информационные ресурсы департамента и иных органов исполнительной власти (администрация области, департаменты, муниципалитеты и др.) считаются собственностью ОИВ, если иное не оговорено соответствующими соглашениями.

4.3. Департамент образования и науки Костромской области оставляет за собой право протоколировать и контролировать действия сотрудников при обработке конфиденциальной информации обрабатываемой в информационной системе.

4.4. Пользователи не имеют права предпринимать попыток получения доступа к закрытым информационным ресурсам, не получив официального разрешения на доступ к ним.

4.5. Пользователи не должны разглашать сведения о содержании информации, ставшей известной им в ходе выполнения должностных

обязанностей, а также о процедурах и технической реализации защиты информации, принятых в департаменте.

4.6. В целях повышения эффективности служебной деятельности для обмена открытыми информационными ресурсами (обновления программных продуктов, инструкции, правила и т.п.) между пользователями могут использоваться съёмные материальные носители информации (Flash-карты, переносные жесткие диски, иные устройства записи и чтения), зарегистрированные и учтённые по Журналу учёта съемных носителей информации.

4.7. Выдача сотрудникам и учёт материальных носителей информации осуществляется сотрудником, ответственным за организацию работы по защите персональных данных, по Журналу учёта съёмных носителей информации.

5. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОРЯДКА

5.1. Ответственность за неисполнение требований настоящей Инструкции возлагается на всех сотрудников, являющихся пользователями информационной системы департамента.

5.2. Сотрудник, нарушивший требования данной Инструкции, может быть подвергнут дисциплинарному наказанию в соответствии с законодательством Российской Федерации (уголовный, налоговый, гражданский, трудовой Кодексы и иное законодательство).

УТВЕРЖДАЮ

Директор департамента образования и науки Костромской области

_____ Т.Е. Быстрякова

1 сентября 2015

ИНСТРУКЦИЯ
администратора безопасности АИС.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана на основании действующих нормативных документов и определяет общие функции, права и обязанности администратора безопасности по вопросам обеспечения информационной безопасности при обработке персональных данных и иной конфиденциальной информации с использованием средств автоматизации, входящих в состав автоматизированных информационных систем (далее – АИС).

1.2. Администратор безопасности (далее – Администратор) в своей работе руководствуется настоящей Инструкцией, внутренними нормативными документами и требованиями законодательства в сфере защиты информации ограниченного доступа.

1.3. Администратор безопасности назначается из числа сотрудников Оператора ПДн, имеющих соответствующую квалификацию и опыт работы с оборудованием и программным обеспечением информационных систем.

Администратор безопасности является ответственным должностным лицом организации и обеспечивает правильное использование и функционирование установленного системного и прикладного программного обеспечения, средств технической защиты информации (далее по тексту - СЗИ) от несанкционированного доступа (далее по тексту - НСД), а также поддержание достигнутого уровня защиты АИС и её ресурсов на этапах эксплуатации и модернизации.

1.4. Администратор безопасности имеет рабочее место, размещаемое в выделенном помещении, оборудованном средствами физической защиты в которое исключается несанкционированный доступ посторонних лиц. Рабочее место Администратора подключается к ЛВС, оборудуется средствами удаленного контроля используемых информационных ресурсов и местами хранения конфиденциальных документов.

1.5. Требования Администратора безопасности к сотрудникам, связанные с выполнением ими своих должностных обязанностей, обязательны для исполнения всеми пользователями АИС.

1.6. Администратор безопасности осуществляет плановый и периодический контроль[1] действий пользователей при работе в АИС, определяет текущее состояние и поддерживает установленный уровень защиты конфиденциальной информации.

---

[1] План проведения проверок внутреннего контроля на год, при возникновении инцидентов информационной безопасности..

2. АДМИНИСТРАТОР БЕЗОПАСНОСТИ В СВОЕЙ ДЕЯТЕЛЬНОСТИ ИМЕЕТ ПРАВО:

2.1. Знать и выполнять требования действующих в организации нормативных и руководящих документов по защите информации, а также внутренних Инструкций регламентирующих работу с конфиденциальной информацией.

2.2. Оказывать содействие в установке и настройке автоматизированных рабочих мест сотрудников департамента, а также осуществлять сопровождение работы установленного системного и прикладного программного обеспечения и средств защиты информации.

2.3. Организовывать доступ пользователей к ресурсам автоматизированной информационной системы в соответствии с Перечнем должностей, имеющих право доступа к обработке конфиденциальной информации, на основании письменных заявок, утверждаемых руководителем организации.

2.4. Уточнять в установленном порядке обязанности пользователей ИС при обработке на автоматизированном рабочем месте (АРМ) конфиденциальных сведений, в том числе персональных данных, являющихся объектами защиты.

2.5. Осуществлять резервное копирование критичных для работы департамента информационных ресурсов, обеспечивая их защиту и целостность.

2.6. Принимать участие в реализации плановых мероприятий по защите конфиденциальной информации, в том числе персональных данных, циркулирующих в АИС.

2.7. Оказывать помощь пользователям ИСПДн в части консультирования по вопросам введенного режима защиты персональных данных.

2.8. Анализировать состояние принятых в организации мер защиты конфиденциальной информации, в том числе выявлять попытки несанкционированного доступа к ресурсам ИС и совершенствовать методы защиты от угроз информационной безопасности.

2.9. Вести журнал учёта событий, регистрируемых средствами защиты, с целью выявления возможных нарушений или попыток несанкционированного доступа.

2.10. Своевременно вносить коррективы в список пользователей информационных ресурсов и матрицу доступов к ПДн при приеме на работу и увольнении сотрудников. Удалять учётные записи пользователей ИС на доступ к информационным ресурсам в течение суток после подписания Обходного листа либо получения информации от руководителей подразделений об увольнении сотрудника.

2.11. В соответствии с планом внутренних проверок состояния обработки и защиты конфиденциальной информации в том числе персональных данных, на регулярной основе осуществлять контроль:

- за соблюдением сотрудниками требований действующих нормативных и руководящих документов, регламентирующих обработку конфиденциальной информации;
- за осуществлением неизменности и целостности программной среды АИС (системное и прикладное ПО), средств антивирусной защиты и межсетевого экранирования, их параметров и режимов;
- за наличием и возможным использованием на автоматизированных рабочих местах вредоносных программ и иного нелицензионного ПО, не связанного с выполнением функциональных задач;
- за соблюдением пользователями принятого в организации режима парольной политики и порядка использования учётных записей на доступ к информационным ресурсам;
- за состоянием допуска пользователей к работе с ресурсами АИС и изменением прав доступа к защищаемой конфиденциальной информации, в том числе персональным данным;
- за выполнением правил учёта, использования и хранения электронных носителей конфиденциальной информации;
- за соблюдением сроков смены паролей доступа к ресурсам АИС и выполнением рекомендаций по выбору наиболее безопасных паролей;

- за поддержанием установленного порядка обновления антивирусных баз и антивирусной защиты информационных ресурсов;
- за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусах системных блоков АРМ, обрабатывающих информацию ограниченного доступа;
- за сроками действия сертификатов и лицензий эксплуатируемого оборудования и ПО;

2.12. В случаях отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты, принимать меры по своевременному восстановлению и выявлению причин, приведших к отказу работоспособности, а также недопущения доступа посторонних лиц к конфиденциальной информации.

2.13. Периодически (не реже одного раза в полугодие) представлять руководству организации отчёт о состоянии защиты конфиденциальной информации, о нештатных ситуациях на объектах АИС, о работе сотрудников в сетях общего пользования, в том числе в Интернет, и допущенных пользователями нарушениях требований по защите информации, предусмотренных руководящими документами.

3. АДМИНИСТРАТОР БЕЗОПАСНОСТИ ОБЯЗАН:

3.1. Принимать необходимые меры по обеспечению безаварийного функционирования и работоспособности автоматизированных средств обработки информации, системного и прикладного ПО, СЗИ от НСД в пределах, возложенных на него функций;

3.2. Проводить инструктаж пользователей правилам работы на АРМ, с установленными СКЗИ и СЗИ от НСД;

3.3. Докладывать директору департамента или лицу, исполняющему его обязанности, о фактах и попытках несанкционированного доступа к конфиденциальной информации, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований безопасности информации.

3.5. Вносить изменения в документацию ИС в соответствии с требованиями нормативных документов в части, касающейся СЗИ от НСД;

3.6. Проводить работу по выявлению возможных каналов утечки конфиденциальной информации, вести их учёт и принимать меры к их устранению;

3.7. Регистрировать факты нарушений требований режима безопасности и организовывать проведение расследований по возникшим инцидентам информационной безопасности.

3.8. Блокировать учётные записи пользователей на АРМ в случае окончания срока действия сертификата соответствия ФСТЭК России, ФСБ России на любое СЗИ, из используемых в ИСПДн, до момента его продления.

В случае непродления сертификата соответствия на СЗИ администратор обязан поставить в известность орган по аттестации, проводивший аттестацию ИСПДн, для принятия дальнейшего совместного решения.

3.9. Контролировать действия пользователей при уничтожении и затирании информации записанной на электронных носителях (накопителях) информации.

4. АДМИНИСТРАТОР БЕЗОПАСНОСТИ ИМЕЕТ ПРАВО:

4.1. Запрашивать и получать необходимую информацию от структурных подразделений департамента для планирования и организации работ по защите конфиденциальной информации.

4.2. Требовать от сотрудников департамента – пользователей ИСПДн соблюдения установленных технологий обработки информации и выполнения требований руководящих документов.

4.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, доступа к информационным ресурасам, утраты, порчи защищаемой информации и технических компонентов автоматизированной системы.

4.4. Требовать от руководителей структурных подразделений департамента прекращения работы сотрудников в автоматизированной информационной системе при несоблюдении ими установленной технологии обработки информации или невыполнения требований по безопасности.

4.5. Вносить на рассмотрение руководства предложения по совершенствованию технических мер защиты.

5. АДМИНИСТРАТОР БЕЗОПАСНОСТИ НЕСЁТ ОТВЕТСТВЕННОСТЬ:

5.1. За разглашение конфиденциальных сведений организации (в том числе - персональных данных работников и должностных лиц контрагентов, используемых способов и методов защиты информационных ресурсов), ставших ему известными по роду своей деятельности.

5.2. За умышленное причинение материального ущерба, повлекшее отказ в работе оборудования корпоративной информационной системы, – в пределах, определенных действующим трудовым, уголовным и гражданским законодательством РФ.

Приложение 2	**Правила работы с информационными системами департамента образования и науки Костромской области**	

УТВЕРЖДАЮ

Директор департамента образования
и науки Костромской области
_____ Т.Е. Быстрякова

1 сентября 2015

ИНСТРУКЦИЯ

по проведению антивирусного контроля на автоматизированном рабочем месте (АРМ)

1. Настоящая Инструкция предназначена для администратора безопасности и пользователей, обрабатывающих персональные данные с использованием средств автоматизации.
2. В целях обеспечения защиты автоматизированной информационной системы от программных закладок и программно-математического воздействия на обрабатываемые конфиденциальные данные на автоматизированных рабочих местах (АРМ) производится антивирусный контроль.
3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности.
4. К установке и использованию в автоматизированной информационной системе и на АРМ разрешаются только лицензионные антивирусные средства, имеющие сертификат ФСТЭК.
5. На АРМ пользователя запрещается установка прикладного программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на АРМ.
6. Пользователи АРМ при работе с информацией (ПО, БД, файлы) записанной на электронных носителях информации (Flash-карты, CD-диски, дискеты и т.п.) обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.
7. Ярлык для запуска антивирусной программы должен быть вынесен на "Рабочий стол" операционной системы.
8. Обновление вирусных баз осуществляется ежедневно путём скачивания и установки антивирусных баз с сервера производителя антивирусного ПО.

Посредством настроек антивирусного средства и организации доступа к серверам разработчика антивирусного средства обновление можно выполнять в автоматическом режиме[1] без участия пользователя АРМ.

---

[1] При невозможности настроить доступ АРМ к серверам обновлений разработчика антивирусного средства Администратор информационной безопасности один раз в неделю производит установку пакетов

9. При обнаружении компьютерного вируса в процессе эксплуатации АРМ либо сканирования съёмных электронных носителей информации пользователь обязан немедленно поставить об этом в известность администратора безопасности и прекратить какие-либо действия, связанные с обработкой конфиденциальной информации на АРМ.

10. По факту заражения АРМ компьютерным вирусом администратор безопасности производит «лечение» зараженных файлов путём выбора соответствующего пункта меню антивирусной программы, после чего вновь проводит антивирусный контроль файловой системы и обрабатываемых данных на АРМ. По результатам заражения АИС администратор безопасности проводит служебное расследование.

11. При обнаружении не поддающегося лечению вируса, администратор безопасности обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность АРМ.

В случае отказа работоспособности АРМ – произвести восстановление и настройки соответствующего операционного и прикладного программного обеспечения.

12. О всех фактах заражения АИС и АРМ вредоносным программным обеспечением администратор безопасности обязан проинформировать ответственного за организацию обработки ПДн либо ответственного сотрудника службы безопасности.

обновлений антивирусных баз, осуществляет контроль их подключения к антивирусному пакету и проверку жесткого диска АРМ и съемных носителей на наличие вирусов.

УТВЕРЖДАЮ

Директор департамента образования и науки Костромской области

_____ Т.Е. Быстрякова

1 сентября 2015

ИНСТРУКЦИЯ
по резервному копированию информации и восстановлению работоспособности ИС

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В целях предупреждения возможности неблагоприятных последствий и обеспечения защиты важной или критичной для обеспечения работоспособности автоматизированных информационных систем информации от её случайного либо умышленного уничтожения, модификации или хищения, а также обеспечения её сохранности сотрудники департамента обязаны создавать её резервные копии.

1.2. Настоящая Инструкция разработана в соответствии с требованиями Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 15.09.2008 № 687 «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативных документов[1] и определяет общие правила резервирования обрабатываемых данных, в том числе при обработке информации ограниченного распространения (обработка персональных данных и иной конфиденциальной информации).

1.3. При осуществлении резервирования (резервного копирования) данных пользователи в своей работе руководствуется настоящей Инструкцией, иными внутренними нормативными документами и требованиями законодательства в сфере защиты информации ограниченного доступа.

1.4. Резервирование данных проводится для обеспечения восстановления работоспособности автоматизированных информационных систем (АИС), вызванной сбоями в работе либо отказами аппаратного и программного обеспечения, чрезвычайными обстоятельствами, ошибками пользователей и (или) иными внешними воздействиями, ведущими к полной или частичной утрате информации.

1.5. Требования настоящей Инструкции, связанные с резервным копированием критичной информации обязательны для исполнения всеми сотрудниками (пользователями), обрабатывающими такую информацию.

---

[1] Приказ ФСТЭК России от 18.02.2013 № 21 и приказ ФСБ России от 10.07.2014 № 378.

1.6. Администратор безопасности департамента осуществляет плановый и периодический контроль[2] действий пользователей по обеспечению резервного копирования критически важных для обеспечения работоспособности АИС данных (информация о серийных номерах лицензионного ПО, настройках и т.п.).

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная информационная система (АИС) - взаимосвязанная совокупность данных, оборудования, программных средств, персонала, реализующая информационную технологию выполнения установленных функций, предназначенных для сбора, обработки, распределения, хранения, выдачи (предоставления) информации (по ГОСТ 34.003).

Критичная информация - любая важная информация, а также системное и прикладное программное обеспечение, утрата которых может привести к перебоям либо отказу в работе автоматизированной информационной системы и затруднению (либо невозможности) исполнения служебных обязанностей.

Резервное копирование - сохранение текущего состояния информации (системы) без обязательного сохранения предыдущего.

Съемный носитель информации - носитель информации, предназначенный для автономного хранения информации вне зависимости от места записи и использования (НЖМД, CD-DVD-диск, Flash-накопитель и т.п).

Гарантированное хранение - хранение, обеспечивающее целостность информации, определяемую требованиями федерального законодательства и внутренними организационно-распорядительными документами департамента.

3. ИНФОРМАЦИЯ, ПОДЛЕЖАЩАЯ РЕЗЕРВИРОВАНИЮ

В целях скорейшего восстановления работоспособности автоматизированной ИС и исключения неблагоприятных последствий вызванных отказами в её работе либо утратой критичной информации в департаменте определен перечень информационных ресурсов, системного и прикладного ПО, подлежащих резервному копированию (Приложение 1), в который включены:

3.1. Персональные данные работников организации, обрабатываемые с использованием средств автоматизации и прикладного программного обеспечения (1:С Предприятие, Камин, Парус Кадры) в отделе информационного, кадрового и правового обеспечения и отделе бухгалтерского учёта, отчетности и финансового контроля;

3.2. Рабочие документы сотрудников подразделений департамента (файлы, базы данных, отчеты, анализы и т.п.), включая результаты выполненных работ, сохраняемые на жестком диске и в системных папках;

3.3. Инсталляции системного и прикладного ПО, используемого для защиты и обработки критичной информации, персональных данных и иной конфиденциальной информации

4. ПОРЯДОК РЕЗЕРВИРОВАНИЯ ДАННЫХ

Организация обеспечения резервного копирования обрабатываемой критичной информации, в том числе персональных данных, возложена на руководителей подразделений департамента, в которых она обрабатывается (одного из его сотрудников).

4.1. Обязательному резервному копированию и гарантированному хранению подлежит информация, указанная в Приложении 1.

---

[2] План проведения проверок внутреннего контроля на год, при возникновении инцидентов информационной безопасности..

4.2. В качестве носителей, на которые осуществляется резервное копирование информации, в зависимости от сохраняемых информационных ресурсов, используются:

- папки на сетевом диске департамента образования и науки;
- накопители на жестких магнитных носителях АРМ пользователей, физически разнесенные с накопителями, где происходит обработка критичной информации;
- перезаписываемые или не перезаписываемые диски (CD, DVD, Blu-Ray).

4.3. К носителям, на которые производится резервное копирование предъявляются следующие требования:

4.4.1. Наличие достаточного объема свободного дискового пространства либо свободной памяти для обеспечения надежного хранения резервных копий;

4.4.2. Носитель должен периодически проходить полную проверку целостности (не реже одного раза в 6 месяцев);

4.4.3. Носитель должен быть учтён по Журналу учёта электронных носителей с указанием наименования, информационной емкости, ответственного за его эксплуатацию сотрудника;

4.4.4. К носителю должен быть ограничен физический доступ посторонних лиц, в том числе по сети. Его хранение осуществляется в местах с ограниченным доступом (запираемый шкаф, сейф и т.п.);

4.4.5. Ход выполнения установленных требований соблюдения установленных правил хранения и доступа, целостности ячеек памяти и работоспособности осуществляется на регулярной основе в соответствии с планом проведения внутренних проверок.

4.5. Период сохранения резервных копий определяется комиссионно, исходя из целесообразности обеспечения гарантированного сохранения тех или иных информационных ресурсов (частота внесения изменений в данные, критичность их утраты и т.п.) и производится по окончании рабочего времени ежеквартально, ежегодно с сохранением информации за указанный период + 1 день.

5. УЧЁТ МАТЕРИАЛЬНЫХ НОСИТЕЛЕЙ РЕЗЕРВНЫХ КОПИЙ

5.1 В целях обеспечения сохранности резервируемой в департаменте ведётся журнальный учёт электронных носителей, на которых сохраняются резервные копии критичной информации. Журнал учёта электронных носителей информации (Приложение 2) ведётся ответственным за организацию работы с персональными данными.

5.2 Сотрудник подразделения департамента, отвечающий за резервное копирование критичной информации, обязан зарегистрировать электронный носитель по Журналу учёта и в дальнейшем хранить его в недоступном для посторонних лиц месте (запираемом шкафу, сейфе или иных защищенных местах хранения).

5.3 Уничтожение электронных носителей с резервными копиями (при необходимости) производится членами экспертной комиссии департамента на основании принятого ими решения в соответствии с установленным порядком (РД-03 «Положение об экспертной комиссии»).

6. ПОРЯДОК ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ ИС

6.1 В случае потери (уничтожения, модификации) критичной информации пользователь информационных ресурсов ИСПДн либо ответственный работник обязан сообщить руководителю отдела о факте происшедшего сбоя в работе информационной системы, в результате которого произошла утрата данных. При этом сотрудник сообщает о возможных признаках сопутствующих отказу в работе АИС и принимает незамедлительные меры по восстановлению утраченной информации в кратчайший срок.

6.2 При потере критичной информации хранящейся на сетевом диске локальной информационной системы восстановление производится при участии администратора безопасности департамента.

6.3 По итогам происшедшего инцидента с утратой критичной информации в целях предотвращения подобных фактов в дальнейшем администратором безопасности проводится разбирательство с выявлением причин инцидента и лиц, допустивших нарушение.

7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ УСТАНОВЛЕННОГО ПОРЯДКА РЕЗЕРВИРОВАНИЯ ДАННЫХ

7.1 Персональная ответственность за обеспечение безопасного хранения критичной информации пользователя в соответствии с установленным порядком возлагается на ответственных работников, обрабатывающих эту информацию.

7.2 Ответственность за обеспечение резервного копирования критичной информации, обрабатываемой и сохраняемой в ИСПДн, возлагается на руководителя и ответственных работников подразделений.

7.3 Хранение резервных копий и инсталляций эксплуатируемого ПО, серийных номеров и регистрационных кодов возлагается на администратора безопасности.

7.4 Нарушение требований настоящей Инструкции влечёт за собой дисциплинарную ответственность в соответствии с трудовым законодательством РФ.

7.5 К лицам, нарушившим установленный порядок резервирования критичной информации, обеспечения сохранности и уничтожения электронных носителей информации ограниченного доступа, вследствие которых произошло нанесение материального ущерба организации, могут быть приняты меры по возмещению убытков и компенсации морального вреда[3].

Приложение: 1. Перечень критичных информационных ресурсов;
2. Журнал учёта электронных носителей информации.

[3] Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению установленного порядка резервирования или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

Приложение 1	**Инструкция по резервному копированию информации и восстановлению работоспособности ИС**

ПЕРЕЧЕНЬ

критичных информационных ресурсов,
подлежащих резервному копированию

№ п/п	Наименование информационного ресурса	Подразделение (сотрудник) ответственное за резервирование	Период резервирования	Носитель
1	Данные кадрового учёта	Еремина Г.И.	ежеквартально	Flash-накопитель
2	Данные бухгалтерского учёта	Гл. бухгалтер	ежеквартально	Жесткий диск гл. бухгалтера
3	Системное ПО	Администратор безопасности	При установке	DVD-диск
4	Прикладное ПО	Администратор безопасности	При установке	DVD-диск
5				
6				