Департамент образования Вологодской области
бюджетное профессиональное образовательное учреждение Вологодской области «Череповецкий многопрофильный колледж»

ПРИНЯТО
на Совете учреждения
от «10» сентября 2019 года
Протокол № 12

УТВЕРЖДАЮ
Директор БПОУ ВО
«Череповецкий многопрофильный колледж»
_____ С.А. Мартяшов

# ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ БЮДЖЕТНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВОЛОГОДСКОЙ ОБЛАСТИ «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ» И ШЕКСНИНСКОГО ФИЛИАЛА БЮДЖЕТНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВОЛОГОДСКОЙ ОБЛАСТИ «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ»

г. Череповец
2019 г

Приложение 10. Порядок доступа работников БПОУ ВО «Череповецкий многопрофильный колледж» в помещения, в которых ведется обработка персональных данных
Приложение 11. Регламент защищенности персональных данных
Приложение 12 . Регламент взаимодействия с уполномоченным органом по защите прав субъектов персональных данных
Приложение 13. Журнал проведения инструктажей пользователей

## 1. Общие положения

1.1. Настоящее Положение обработке персональных данных работников и обучающихся (далее — Положение) бюджетного профессионального образо-

вательного учреждения Вологодской области «Череповецкий многопрофильный колледж» (далее БПОУ ВО ЧМК) и Шекснинского филиала бюджетного профессионального образовательного учреждения Вологодской области «Череповецкий многопрофильный колледж» (далее - филиал) разработано в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Правилами внутреннего трудового распорядка БПОУ ВО ЧМК и филиала.

1.2. Цель разработки Положения — определение порядка обработки персональных данных работников, обучающихся БПОУ ВО ЧМК и филиала; обеспечение защиты прав и свобод работников, обучающихся БПОУ ВО ЧМК и филиала при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников, обучающихся БПОУ ВО ЧМК и филиала, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения директором БПОУ ВО ЧМК и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом.

1.4. Все работники БПОУ ВО ЧМК и филиала должны быть ознакомлены с настоящим Положением.

1.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии БПОУ ВО ЧМК, если иное не определено законом.

## II. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

– персональные данные работника, обучающегося — любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, обучающемуся, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация,

необходимая работодателю в связи с трудовыми отношениями и для осуществления уставной деятельности;

– обработка персональных данных— сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников, обучающихся БПОУ ВО ЧМК и филиала;

– конфиденциальность персональных данных— обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, обучающихся требование не допускать их распространения без согласия работника, обучающегося или иного законного основания;

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

– использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом БПОУ ВО ЧМК и филиала в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников, обучающихся либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

– блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, обучающихся, в том числе их передачи;

– уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников, обучающихся или в результате которых уничтожаются материальные носители персональных данных работников, обучающихся;

– обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику, обучающемуся;

– общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника, обучающегося или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

– информация — сведения (сообщения, данные) независимо от формы их представления.

– документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. В состав персональных данных работников, обучающихся БПОУ ВО ЧМК и филиала входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья, а также о предыдущих местах их работы, учебы.

2.3. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в БПОУ ВО ЧМК или филиала при его приеме, переводе и увольнении.

2.3.1. Информация, представляемая работником при поступлении на работу в БПОУ ВО ЧМК или филиала, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации 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, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
– страховое свидетельство государственного пенсионного страхования;
– документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;
– документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;
– свидетельство о присвоении ИНН (при его наличии у работника).

справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям, выданную в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, - при поступлении на

работу, связанную с деятельностью, к осуществлению которой в соответствии с настоящим Кодексом, иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию;

справку о том, является или не является лицо подвергнутым административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ, которая выдана в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, - при поступлении на работу, связанную с деятельностью, к осуществлению которой в соответствии с федеральными законами не допускаются лица, подвергнутые административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ, до окончания срока, в течение которого лицо считается подвергнутым административному наказанию.

При оформлении работника в БПОУ ВО ЧМК или филиала работником отдела кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:
– общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство знание иностранного языка, образование, профессия, стаж работы, состояние в браке, состав семьи, паспортные данные)
– сведения о воинском учете;
– данные о приеме на работу;
В дальнейшем в личную карточку вносятся:
– сведения о переводах на другую работу;
– сведения об аттестации;
– сведения о повышении квалификации;
– сведения о профессиональной переподготовке;
– сведения о наградах (поощрениях), почетных званиях;
– сведения об отпусках;
– сведения о социальных гарантиях;
– сведения о месте жительства и контактных телефонах.

2.3.2. Информация, представляемая обучающимся при поступлении на обучение в БПОУ ВО ЧМК и филиала, должна иметь документальную форму. При зачислении в колледж предъявляют:

– паспорт или иной документ, удостоверяющий личность;
– страховое свидетельство государственного пенсионного страхования;
– документ об образовании,
– свидетельство о присвоении ИНН (при его наличии у работника).

При зачислении в БПОУ ВО ЧМК и филиала учебной частью вносится запись в Поименную книгу, в которых отражаются следующие анкетные и биографические данные:
– общие сведения (Ф.И.О. дата рождения, место рождения, национальность, домашний адрес, гражданство, образование)

2.3.3. В отделе кадров колледжа создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.3.3.1. Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству БПОУ ВО ЧМК, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

2.3.3.2. Документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции работников, приказы, распоряжения, указания руководства БПОУ ВО ЧМК и филиала); документы по планированию, учету, анализу и отчетности в части работы с персоналом БПОУ ВО ЧМК и филиала.

2.3.4. В учебной части колледжа создаются и хранятся следующие группы документов, содержащие данные об обучающихся в единичном или сводном виде:

2.3.4.1. Документы, содержащие персональные данные обучающегося (комплексы документов, сопровождающие процесс обучения; комплекс материалов по анкетированию, тестированию; подлинники и копии приказов по движению контингента; личные дела; дела, содержащие основания к приказу по движению контингента; справочно-информационный банк данных по обучающимся (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству БПОУ ВО ЧМК, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

## III. Сбор, обработка и защита персональных данных

3.1. Порядок получения персональных данных.

3.1.1. Все персональные данные работника, обучающегося БПОУ ВО ЧМК и филиала следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то работник, обучающийся должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо работодателя должно сообщить работнику, обучающемуся  БПОУ ВО ЧМК или филиала о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника, обучающегося дать письменное согласие на их получение.

3.1.2. Работодатель не имеет права получать и обрабатывать персональные данные работника, обучающегося БПОУ ВО ЧМК и филиала о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной 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, обучающегося только с его письменного согласия.
Обработка указанных персональных данных работников, обучающихся работодателем возможна только с их согласия либо без их согласия в следующих случаях:
– персональные данные являются общедоступными;
– персональные данные относятся к состоянию здоровья и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия невозможно;
– по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

3.1.3. Работодатель вправе обрабатывать персональные данные работников, обучающихся только с их письменного согласия.

3.1.4. Письменное согласие работника, обучающегося на обработку своих персональных данных должно включать в себя:

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

– наименование и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

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

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

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

Форма заявления о согласии на обработку персональных данных см. в приложении 1 к настоящему Положению.

3.1.5. Согласие работника, обучающегося не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

2) обработка персональных данных осуществляется в целях исполнения трудового договора;

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

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

3.2. Порядок обработки, передачи и хранения персональных данных.

3.2.1. Работник БПОУ ВО ЧМК или филиала предоставляет работнику отдела кадров, обучающийся в учебную часть достоверные сведения о себе. Работник отдела кадров, учебной части БПОУ ВО ЧМК или филиала проверяет достоверность сведений, сверяя данные, предоставленные работником, обучающимся, с имеющимися у работника документами.

3.2.2. В соответствии со ст. 86, гл. 14 ТК РФ в целях обеспечения прав и свобод человека и гражданина директор БПОУ ВО ЧМК и его представители при обработке персональных данных должны соблюдать следующие общие требования:

3.2.2.1. Обработка персональных данных может осуществляться 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.

3.2.2.2. При определении объема и содержания, обрабатываемых персональных данных Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

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

3.2.2.4. Защита персональных данных работника, обучающегося от неправомерного их использования или утраты обеспечивается Работодателем за счет его средств в порядке, установленном федеральным законом.

3.2.2.5. Работники и их представители должны быть ознакомлены под расписку с документами Организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.2.2.6. Во всех случаях отказ работника, обучающегося от своих прав на сохранение и защиту тайны недействителен.

## IV. Передача и хранение персональных данных

4.1. При передаче персональных данных работника, обучающегося Работодатель должен соблюдать следующие требования:

4.1.1. Не сообщать персональные данные третьей стороне без письменного согласия работника, обучающегося, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом.

4.1.2. Не сообщать персональные данные работника, обучающегося в коммерческих целях без его письменного согласия. Обработка персональных данных работников, обучающихся в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

4.1.3. Предупредить лиц, получивших персональные данные работника, обучающегося 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. Лица, получившие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

4.1.4. Осуществлять передачу персональных данных работников, обучающихся в пределах БПОУ ВО ЧМК и филиала в соответствии с настоящим Положением.

4.1.5. Разрешать доступ к персональным данным работников, обучающихся только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

4.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

4.1.7. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.

4.2. Хранение и использование персональных данных работников:

4.2.1. Персональные данные работников обрабатываются и хранятся в отделе кадров, обучающихся в учебной части.

4.2.2. Персональные данные работников, обучающихся могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде — локальной компьютерной сети, компьютерных программах, ИСПНДн, ГИС и прочих информационных системах.

4.3. При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании федерального закона или если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

– наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

– цель обработки персональных данных и ее правовое основание;
– предполагаемые пользователи персональных данных;
– установленные настоящим Федеральным законом права субъекта персональных данных.

## V. Доступ к персональным данным работников

5.1. Право доступа к персональным данным работников, обучающихся имеют:
–директор БПОУ ВО ЧМК;
- заведующий ресурсным центром;
- заведующий филиалом;
– работники отдела кадров, учебной части, документовед;
– работники планово-экономического отдела;
- классные руководители в своих группах
-педагог-психолог;
- социальный педагог (сироты), заведующий учебно-воспитательной и социальной работы (обучающиеся)

5.2. Работник, обучающийся БПОУ ВО ЧМК и филиала имеет право:

5.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные работника.

5.2.2. Требовать от Работодателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для Работодателя персональных данных.

5.2.3. Получать от Работодателя

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

5.2.3. Требовать извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Работодателя при обработке и защите его персональных данных.

5.3. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях .

5.4. Передача информации третьей стороне возможна только при письменном согласии работников, обучающихся.

## VI. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

6.1. Работники БПОУ ВО ЧМК и филиала, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, обучающегося, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

6.2. Директор БПОУ ВО ЧМК за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, обучающегося несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные работника.

**Приложение 1**

**ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ**
**к ТРУДОВОМУ ДОГОВОРУ № _____ от «____» _____ 20___ года**

**СОГЛАСИЕ РАБОТНИКА**
**на передачу его персональных данных третьим лицам**

**Я,** работающий(ая) в БПОУ ВО «Череповецкий многопрофильный колледж»

(далее по тексту - **Работник**),

Ф.И.О. полностью

имеющий(ая) паспорт гражданина(ки) Российской Федерации:
_____

серия, № паспорта

_____
_____ ,

когда, кем выдан паспорт

зарегистрированный(ая) по адресу:
_____

_____
_____ ,

в соответствии с нормами главы 14 Трудового кодекса РФ и Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» **ДАЮ СВОЕЙ ВОЛЕЙ ПИСЬМЕННОЕ СОГЛАСИЕ** на передачу Работодателем моих персональных данных третьим лицам (далее - иным операторам).

Передача моих персональных иным операторам должна осуществляться Работодателем только с целью исполнения обязательств, возложенных на него законодательными, нормативными актами либо установленных договорами и иными законными сделками, а также для соблюдения моих прав и интересов.

Работодатель с моего настоящего согласия имеет право передавать мои персональные данные, указанные ниже, следующим иным операторам:

1. Банку – для оформления безналичного счета, на который Работодателем будет перечисляться заработная плата и иные доходы Работника, при условии, что Работодатель заранее сообщит Работнику наименование и адрес данного банка:

Фамилия, имя, отчество
Дата, месяц, год рождения
Паспортные данные
ИНН
Размер заработной платы и иных доходов, выплачиваемых Работодателем
Адрес регистрации
Адрес фактического проживания

2. Кредитным организациям, в которые Работник обращался для оформления кредитов, ссуд либо получения иных услуг, при условии, что Работник заранее сообщит Работодателю наименования указанных кредитных организаций:

Фамилия, имя, отчество
Дата, месяц, год рождения
Паспортные данные
ИНН
Размер заработной платы, выплачиваемой Работодателем

3. Страховой компании – для оформления полиса добровольного медицинского страхования, при условии, что Работодатель заранее сообщит Работнику наименование и адрес данной страховой компании:

Фамилия, имя, отчество
Дата, месяц, год рождения
Паспортные данные
Адрес регистрации
Адрес фактического проживания
Семейное положение

4. Полиграфической организации или типографии - для изготовления визитных карточек Работника, при условии, что Работодатель заранее сообщит Работнику наименование и адрес данного полиграфического предприятия:

Фамилия, имя, отчество
Должность
Служебный номер телефона
Адрес электронной почты

5. Организации, осуществляющей охрану помещений, в которых расположен офис Работодателя, при условии, что Работодатель заранее сообщит Работнику наименование и адрес данной охранной организации:

Фамилия, имя, отчество
Должность
Служебный номер телефона

6. Налоговым органам (ИФНС России № 12 по г. Череповец), подразделениям Пенсионного фонда Российской Федерации (ГУ ПФР по г.Череповец и Вологодской области области), подразделениям Федеральной миграционной службы России (УФМС России по г. Череповцу), центрам занятости населения (ЦЗН г. Череповца) - для исполнения обязательств, возложенных на Работодателя законодательными и нормативными актами, а также исполнения законных официальных запросов, касающихся Работника:

Фамилия, имя, отчество
Дата, месяц, год рождения
Должность
Паспортные данные
ИНН
Размер заработной платы и иных доходов, выплачиваемых Работодателем
Адрес регистрации
Адрес фактического проживания
Сведения о трудовом и общем стаже
Сведения о воинском учете
Домашний и служебный телефоны

Я согласен с тем, что мои указанные выше персональные данные будут обрабатываться перечисленными выше иными операторами в моем интересе методом смешанный (в том числе автоматизированной с помощью средств вычислительной техники и на бумажных носителях) обработки, систематизироваться, храниться, распространяться и передаваться с использованием сети общего пользования Интернет третьим лицам, в том числе с использованием трансграничной передачи данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных.

Настоящее согласие мною дается на срок действия Трудового договора с Работодателем.

Настоящее согласие считается отозванным в случае досрочного расторжения Трудового договора с Работодателем по любой причине.

Подтверждаю, что с нормами Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», в том числе с порядком отзыва согласия на обработку персональных данных, я ознакомлен(а).

_____ _____

(собственноручная подпись **Работника**) (Ф.И.О. **Работника**)

«___» _____ 20___ года

**СОГЛАСИЕ**
**на обработку персональных данных**

Я,
_____
Проживающий (ая) по адресу:
_____
_____
_
Паспорт _____ № _____ выдан _____
_____
_

в соответствии с требованиями статьи 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» даю согласие бюджетному профессиональному образовательному учреждению Вологодской области «Череповецкий многопрофильный колледж» на обработку, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу по запросу уполномоченных учреждений по защищенному каналу связи в сети общего пользования (распространение, предоставление, доступ), обезличивание, блокирование, удаление или уничтожение персональных данных:
- фамилия, имя, отчество, пол, дата и место рождения, гражданство;
- сведения об изменении фамилии, имени, отчества (когда, где и по какой причине);
- профессиональное образование (оконченные учебные заведения и год окончания, специальность (направление) и квалификация);
- данные паспорта гражданина РФ;
- номер полиса добровольного медицинского страхования;
- отношение к воинской обязанности и воинское звание;
- сведения о месте регистрации и месте фактического проживания, номер домашнего телефона, номер сотового телефона;
- номер страхового свидетельства обязательного пенсионного страхования (СНИЛС);
- реквизиты актов гражданского состояния (состояние в браке, наличие детей и др.);
- идентификационный номер налогоплательщика (ИНН);
- сведения о замещаемой должности, дата принятия на работу, характер работы;
- сведения о стаже (общий трудовой стаж, стаж работы по специальности);
- сведения о допуске к государственной тайне;
- сведения о награждении наградами, поощрениях;
- сведения о временной нетрудоспособности;
- сведения о доходах;
- сведения о лицевом счете и расчетных счетах в кредитных организациях для перечисления назначенных выплат.

Все операции могут проходить как в бумажном ручном режиме, так и с использованием средств автоматизации, в том числе в режиме онлайн.

Настоящее согласие на обработку и передачу персональных данных может быть отозвано в порядке, установленном Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»

Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», мне разъяснены мои права и обязанности, связанные с обработкой и передачей персональных данных, в том числе, моя обязанность проинформировать БПОУ ВО «Череповецкий многопрофильный колледж», в случае изменения моих персональных данных.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

«___» _____ 20___ г. _____ /_____/
(подпись) (ФИО)

## СОГЛАСИЕ
## на обработку и передачу персональных данных

Я, _____

Проживающий (ая) по адресу: _____

_____

Паспорт _____ № _____ выдан _____

_____

в соответствии с требованиями статьи 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», даю своё согласие бюджетному профессиональному образовательному учреждению Вологодской области «Череповецкий многопрофильный колледж», расположенному по адресу: г. Череповец ул. Гоголя, д. 21, для ведения бухгалтерского учета, составления бухгалтерской, налоговой отчетности и отчетности в государственные внебюджетные фонды на автоматизированную, а также без использования средств автоматизации (на бумажных носителях), обработку и передачу в следующие организации:

- Филиал №1 ГУ - Вологодское региональное отделение Фонда социального страхования Российской Федерации Вологодская область г. Череповец пр. Советский, 135
- ГУ - управление Пенсионного фонда Российской Федерации в г. Череповце и Череповецком районе Вологодская область г. Череповец ул. Труда, 49
- Межрайонная инспекция ФНС России № 12 по Вологодской области Вологодская область г. Череповец пр. Строителей, 4Б
- Отделение занятости населения по городу Череповцу и Череповецкому району

Вологодская область г. Череповец пр. Советский, 66

- Комитет социальной защиты населения по городу Череповец Вологодская область г. Череповец ул. Сталеваров, 54
- Управление социальной защиты населения по Череповецкому муниципальному району Вологодская область г. Череповец ул. Первомайская, 58
- Банк ВТБ 24, Сбербанк России

(в части перечисления заработной платы и иных выплат), своих персональных данных:

- фамилия, имя, отчество, пол, дата и место рождения, гражданство;
- сведения об изменении фамилии, имени, отчества (когда, где и по какой причине);
- профессиональное образование (оконченные учебные заведения и год окончания, специальность (направление) и квалификация, наличие ученых степеней);
- сведения о стаже (общий трудовой стаж, стаж работы по специальности);
- данные паспорта гражданина РФ;
- номер полиса добровольного медицинского страхования;
- сведения о допуске к государственной тайне;
- отношение к воинской обязанности и воинское звание;
- сведения о месте регистрации и месте фактического проживания, номер домашнего телефона, номер сотового телефона;
- номер страхового свидетельства обязательного пенсионного страхования (СНИЛС);

- реквизиты актов гражданского состояния (состояние в браке, наличие детей и др.);
- идентификационный номер налогоплательщика (ИНН);
- сведения о замещаемой должности, дата принятия на работу, характер работы;
- сведения об условиях оплаты труда по замещаемой должности;
- сведения о присвоении классных чинов государственной гражданской службы области (дата присвоения, наименование чина, надбавка, дата и номер акта о присвоении);
- сведения о награждении государственными и ведомственными наградами, иными наградами, поощрениях;
- сведения о временной нетрудоспособности;
- сведения с предыдущих мест работы о доходах;
- сведения о лицевом счете и расчетных счетах в кредитных организациях для перечисления заработной платы и иных выплат.

Предоставляю бюджетному профессиональному образовательному учреждению Вологодской области «Череповецкий многопрофильный колледж» право осуществлять все действия (операции) с моими персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Настоящее согласие на обработку и передачу персональных данных может быть отозвано в порядке, установленном Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» или в случае прекращения деятельности бюджетного профессионального образовательного учреждения Вологодской области «Череповецкий многопрофильный колледж».

Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», мне разъяснены мои права и обязанности, связанные с обработкой и передачей персональных данных, в том числе, моя обязанность проинформировать работодателя, в случае изменения моих персональных данных.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

«___» _____ 20___ г. _____ /_____/

(подпись) (ФИО)

**СОГЛАСИЕ**

**на обработку и передачу персональных данных**

Я, _____

Проживающий (ая) по адресу: _____

_____

Паспорт _____ № _____ выдан _____

_____

в соответствии с требованиями статьи 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», даю своё согласие казенному учреждению системы образования Вологодской области «Централизованная бухгалтерия», расположенному по адресу: г. Вологда ул. Горького, д. 101, для ведения бухгалтерского учета, составления бухгалтерской, налоговой отчетности и отчетности в государственные внебюджетные фонды на автоматизированную, а также без использования средств автоматизации (на бумажных носителях), обработку и передачу в следующие организации:

- Филиал №1 ГУ - Вологодское региональное отделение Фонда социального страхования Российской Федерации Вологодская область г. Череповец пр. Советский, 135
- ГУ - управление Пенсионного фонда Российской Федерации в г. Череповце и Череповецком районе Вологодская область г. Череповец ул. Труда, 49
- Межрайонная инспекция ФНС России № 12 по Вологодской области Вологодская область г. Череповец пр. Строителей, 4Б
- Отделение занятости населения по городу Череповцу и Череповецкому району

Вологодская область г. Череповец пр. Советский, 66

- Комитет социальной защиты населения по городу Череповец Вологодская область г. Череповец ул. Сталеваров, 54
-Управление социальной защиты населения по Череповецкому муниципальному району Вологодская область г. Череповец ул. Первомайская, 58
- Банк ВТБ 24, Сбербанк России

(в части перечисления заработной платы и иных выплат), своих персональных данных:

- фамилия, имя, отчество, пол, дата и место рождения, гражданство;
- сведения об изменении фамилии, имени, отчества (когда, где и по какой причине);
- профессиональное образование (оконченные учебные заведения и год окончания, специальность (направление) и квалификация, наличие ученых степеней);
- сведения о стаже (общий трудовой стаж, стаж работы по специальности);
- данные паспорта гражданина РФ;
- номер полиса добровольного медицинского страхования;
- сведения о допуске к государственной тайне;
- отношение к воинской обязанности и воинское звание;
- сведения о месте регистрации и месте фактического проживания, номер домашнего телефона, номер сотового телефона;
- номер страхового свидетельства обязательного пенсионного страхования (СНИЛС);

- реквизиты актов гражданского состояния (состояние в браке, наличие детей и др.);
- идентификационный номер налогоплательщика (ИНН);
- сведения о замещаемой должности, дата принятия на работу, характер работы;
- сведения об условиях оплаты труда по замещаемой должности;
- сведения о присвоении классных чинов государственной гражданской службы области (дата присвоения, наименование чина, надбавка, дата и номер акта о присвоении);
- сведения о награждении государственными и ведомственными наградами, иными наградами, поощрениях;
- сведения о временной нетрудоспособности;
- сведения с предыдущих мест работы о доходах;
- сведения о лицевом счете и расчетных счетах в кредитных организациях для перечисления заработной платы и иных выплат.

Предоставляю казенному учреждению системы образования Вологодской области «Централизованная бухгалтерия» право осуществлять все действия (операции) с моими персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Настоящее согласие на обработку и передачу персональных данных может быть отозвано в порядке, установленном Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» или в случае прекращения деятельности казенного учреждения системы образования Вологодской области «Централизованная бухгалтерия».

Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», мне разъяснены мои права и обязанности, связанные с обработкой и передачей персональных данных, в том числе, моя обязанность проинформировать работодателя, в случае изменения моих персональных данных.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

«___» _____ 20___ г. _____ /_____/

(подпись) (ФИО)

**Приложение 2**

**Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а так-**

**же определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований**

## 1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с: Статьей 24 Конституции Российской Федерации; Главой 14 Трудового Кодекса Российской Федерации; Федеральным законом Российской Федерации № 152-ФЗ «О персональных данных» от 27.07.2006; Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006; Постановлением Правительства РФ от 21.03.2012 № 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»; Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Приказом ФСТЭК России 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». Приказ ФСБ России от 10.07.2014 N 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, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности». Приказом Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных" (вместе с "Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ").

1.2. Цель разработки документа — определение порядка обработки ПДн субъектов ПДн; обеспечение защиты прав и свобод субъектов ПДн при обработке их ПДн, а также установление ответственности должностных лиц,

имеющих доступ к ПДн субъектов, за невыполнение требований норм, регулирующих обработку и защиту ПДн.

1.3. Порядок ввода в действие и изменения Правил.
1.3.1 Настоящие Правила вступают в силу с момента их утверждения директором БПОУ ВО ЧМК и действуют бессрочно, до замены их новыми Правилами.
1.3.2 Все изменения в Правила вносятся приказом.

2. Состав, категории и содержание ПДн
2.1 Персональные данные, обрабатываемые в БПОУ ВО ЧМК и филиала, относятся к сведениям конфиденциального характера (конфиденциальной информации).

2.2 В БПОУ ВО ЧМК и филиале обрабатываются ПДн следующих субъектов ПДн:
- работники, обучающиеся БПОУ ВО ЧМК и филиала
- субъекты ПДн, не являющиеся работниками, обучающимися БПОУ ВО ЧМК и филиала.

3. Основные условия проведения обработки ПДн
3.1. Обработка ПДн осуществляется после получения согласия субъекта ПДн, за исключением случаев, предусмотренных частью 3.2 настоящих Правил.
3.2. Согласие субъекта ПДн, предусмотренное п.3.1 настоящих Правил не требуется в следующих случаях:
1) обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на колледж функций, полномочий и обязанностей;
2) обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
3) обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
4) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
5) обработка ПДн необходима для осуществления прав и законных интересов колледжа или третьих лиц, либо для достижения общественно значимых це-

лей при условии, что при этом не нарушаются права и свободы субъекта ПДн.

3.2. Письменное согласие субъекта ПДн должно включать:
1) фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2) фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);
3) наименование или фамилию, имя, отчество и адрес Оператора;
4) цель обработки ПДн;
5) перечень ПДн, на обработку которых дается согласие субъекта ПДн;
6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка будет поручена такому лицу;
7) перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;
8) срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;
9) подпись субъекта ПДн.

3.3. Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных п. 3.4 настоящих Правил.

3.4. Обработка специальных категорий ПДн допускается в случаях, если:
1) субъект ПДн дал согласие в письменной форме на обработку своих ПДн;
2) ПДн сделаны общедоступными субъектом ПДн;
3) обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;
4) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;
5) обработка ПДн необходима для установления или осуществления прав субъекта ПДн или третьих лиц, а равно и в связи с осуществлением правосудия;

6) обработка ПДн осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
7) обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

3.5. Лица, допущенные к обработке ПДн, в обязательном порядке под роспись знакомятся с требованиями настоящих Правил.

3.6. Запрещается:
обрабатывать ПДн в присутствии лиц, не допущенных к их обработке;
осуществлять ввод ПДн под диктовку (голосовой ввод).

4. Обработка ПДн
Обработка ПДн подразделяется на:
обработка ПДн в ИСПДн;
обработка ПДн, осуществляемая без использования средств автоматизации.

4.1. Обработка ПДн в ИСПДн
4.1.1 Обработка ПДн в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти. Не допускается обработка ПДн в ИСПДн с использованием средств автоматизации, если применяемые меры и средства обеспечения безопасности не соответствуют требованиям, утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Обработка ПДн с использованием средств автоматизации осуществляется в рамках ИСПДн колледжа и внешних информационных систем, предоставляемых сторонними организациями. Состав ИСПДн колледжа определяется «Перечнем информационных систем персональных данных», утверждаемым директором.

4.2. Обработка ПДн, осуществляемая без использования средств автоматизации
4.2.1 Лица, осуществляющие обработку ПДн без использования средств автоматизации (в том числе работники колледжа или лица, осуществляющие такую обработку по договору с колледжем), должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется колледжем

без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами колледжа.
4.2.2 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны соблюдаться следующие условия:
- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации; имени (наименовании) и адресе колледжа; фамилию, имя, отчество и адрес субъекта ПДн; источник получения ПДн; сроки обработки ПДн; перечень действий с ПДн, которые будут совершаться в процессе их обработки; общее описание используемых колледжем способов обработки ПДн; типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации,
- при необходимости получения письменного согласия на обработку ПДн; типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

5. Основные этапы Обработки ПДн
5.1. Получение ПДн
5.1.1. Колледж получает ПДн непосредственно от субъекта ПДн или от законных представителей субъектов, наделенных соответствующими полномочиями.
5.1.2. Субъект ПДн обязан предоставлять колледжу достоверные сведения о себе. Колледж имеет право проверять достоверность сведений, предоставленных субъектом, сверяя данные, предоставленные субъектом, с имеющимися колледжа документами. Предоставление субъектом ПДн подложных документов или заведомо ложных сведений при заключении трудового договора является основанием для расторжения трудового договора в соответствии с пунктом 11 части первой статьи 81 Трудового кодекса Российской Федерации. При изменении ПДн субъект ПДн – работник колледжа письменно уведомляет о таких изменениях в разумный срок, не превышающий 14 дней с момента изменений. Данное обязательство не распространяется на изменение ПДн, предоставление которых требует соответствующее согласие работника.
5.1.3. Если обязанность предоставления ПДн установлена федеральным законом, работники кадровой службы обязаны разъяснить субъекту ПДн юридические последствия отказа предоставить свои ПДн.
5.1.4. Если ПДн получены не от субъекта ПДн, колледж, за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона Россий-

ской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:
1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
2) цель обработки ПДн и ее правовое основание;
3) предполагаемые пользователи ПДн;
4) установленные федеральным законом права субъекта ПДн;
5) источник получения ПДн.
5.1.5. Колледж освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные п. 5.1.4, в случаях, если:
1) субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;
2) ПДн получены колледжем на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
3) ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника.

5.2. Хранение ПДн
5.2.1. Персональные данные субъектов ПДн хранятся на материальных носителях (бумажные, электронные носители), в том числе и на внешних (съемных) электронных носителях в ИСПДн.
5.2.2. В целях обеспечения сохранности и конфиденциальности ПДн все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только работниками колледжа, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных регламентах.
5.2.3. Хранение ПДн должно происходить в порядке, исключающем их утрату или неправомерное использование.
5.2.4. При работе с документами, содержащими ПДн, запрещается оставлять их на рабочем месте или оставлять шкафы (сейфы) с данными документами открытыми (незапертыми) в случае выхода из рабочего помещения.
5.2.5. В конце рабочего дня все документы, содержащие ПДн, должны быть убраны в шкафы (сейфы).
5.2.6. Хранение документов, содержащих ПДн работников колледжа, должно осуществляться следующим образом:
Личные дела работников, картотеки, учетные журналы и книги учета хранятся в запирающихся шкафах;
Трудовые книжки хранятся в несгораемом сейфе;
Хранение ПДн субъектов ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки в соответствии со сроками хранения, определяемыми законодательством Российской Федерации и нормативными документами колледжа;

Доступ к ИСПДн, содержащим ПДн, должен обеспечиваться с использованием средств защиты от несанкционированного доступа и копирования;
Все электронные носители ПДн должны быть учтены. Учет внешних съемных электронных носителей информации, содержащих ПДн, осуществляется в подразделениях, осуществляющих обработку ПДн.
5.2.7.Работник, имеющий доступ к ПДн работников колледжа в связи с исполнением трудовых обязанностей:
- обеспечивает хранение информации, содержащей ПДн, исключающее доступ к ним третьих лиц;
-при уходе в отпуск, нахождении в служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте он обязан передать документы и иные носители, содержащие ПДн, лицу, на которое приказом или распоряжением колледжа будет возложено исполнение его трудовых обязанностей.
5.2.8. При увольнении работника, имеющего доступ к ПДн, документы и иные носители, содержащие ПДн, сдаются работником своему непосредственному руководителю.
5.2.9. Режим конфиденциальности ПДн снимается в случаях их обезличивания и по истечении срока их хранения, если иное не определено законом.
5.2.10. После увольнения работника папка «Личное дело» перемещается в архив уволенных работников и хранится в архиве 75 лет.

5.3. Порядок учета носителей ПДн
5.3.1. В колледже должны быть учтены все машинные и бумажные носители информации, содержащие ПДн.
5.3.2. Ежегодно необходимо проводить инвентаризацию всех носителей информации, на которых хранятся

5.4. Использование ПДн
5.4.1. Запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных п. 5.4.2 настоящих Правил.
5.4.2. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.
5.4.3. Колледж обязан разъяснить субъекту ПДн положение принятия решения на основании исключительно автоматизированной обработки его ПДн и

возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения.
5.4.4. С документами, содержащими ПДн работника, которые создаются в колледже в период трудовой деятельности работника (приказы, служебные записки и т.п.), работник должен быть ознакомлен под роспись.

5.5. Лицо, ответственное за организацию обработки ПДн в колледже
5.5.1. Приказом по колледжу, назначается лицо, ответственное за организацию обработки ПДн в колледже (далее - Ответственное лицо).
5.5.2. Ответственное лицо получает указания непосредственно от директора и подотчетно ему.
5.5.3. Ответственное лицо обязано:
1) осуществлять внутренний контроль за соблюдением колледжем и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
2) доводить до сведения работников колледжа положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;
3) организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.6. Доступ работников к ПДн субъектов ПДн, обрабатываемым в колледже
5.6.1. Работники колледжа получают доступ к ПДн субъектов ПДн исключительно в объеме, необходимом для выполнения своих должностных обязанностей.
5.6.2. Список работников колледжа, имеющих доступ к ПДн, определяется в «Перечне должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным».
5.6.3. Работнику, должность которого не включена в «Перечень должностей колледжа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным», но которому необходим разовый или временный доступ к ПДн субъектов ПДн в связи с исполнением должностных обязанностей, распоряжением или приказом директора колледжа может быть предоставлен такой доступ на основании письменного мотивированного запроса непосредственного руководителя работника.
5.6.5. Работник колледжа получает доступ к ПДн субъектов ПДн после ознакомления и изучения требований настоящих Правил и иных внутренних нормативных документов колледжа по защите персональных данных в части, его касающейся.

5.7. Доступ субъектов ПДн к ПДн, обрабатываемым в колледже

5.7.1. Субъект ПДн имеет право на свободный доступ к своим ПДн, включая право на получение копии любой записи (за исключением случаев, когда предоставление ПДн нарушает конституционные права и свободы других лиц), содержащей его ПДн. Субъект имеет право вносить предложения по внесению изменений в свои ПДн в случае обнаружения в них неточностей.
5.7.2. Субъект ПДн – работник колледжа или его законный представитель, получает доступ к своим ПДн или к иной информации, касающейся обработки его ПДн по запросу в отделе кадров – для выдачи документов, связанных с его трудовой деятельностью (копии приказов о приеме на работу, переводу на другую работу, увольнении с работы, выписок из трудовой книжки, справок о месте работы, периоде работы в колледже и др.).
5.7.3. Субъект ПДн – иное физическое лицо или его законный представитель, получает доступ к своим ПДн или к иной информации, касающейся обработки его ПДн по запросу Ответственному лицу.
5.7.4. Субъект ПДн имеет право на получение при обращении информации, касающейся обработки его ПДн, в том числе содержащей:
1) подтверждение факта обработки ПДн колледжем;
2) правовые основания и цели обработки ПДн;
3) цели и применяемые колледжем способы обработки ПДн;
4) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
5) сроки обработки ПДн, в том числе сроки их хранения;
6) порядок осуществления субъектом ПДн прав, предусмотренных федеральным законом;
7) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
8) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению колледжа;
9) иные сведения, предусмотренные федеральными законами.
5.7.6. Уполномоченные лица обязаны сообщить субъекту ПДн или его законному представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с ними при обращении субъекта ПДн или его законного представителя не позднее тридцати рабочих дней с даты получения запроса субъекта ПДн или его законного представителя.
5.7.7. Ответ в адрес субъекта ПДн может быть направлен через отделение почтовой связи заказным письмом с уведомлением о вручении или курьером (непосредственно в руки адресату под роспись).
5.7.8. В случае отказа в предоставлении субъекту ПДн или его законному представителю при обращении либо при получении запроса субъекта ПДн или его законного представителя информации о наличии ПДн о соответствующем субъекте ПДн, а также таких ПДн, уполномоченные лица обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положе-

ние части 8 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта ПДн или его законного представителя, либо с даты получения запроса субъекта ПДн или его законного представителя.
5.7.9. Мотивированный ответ в адрес субъекта ПДн может быть направлен через отделение почтовой связи заказным письмом с уведомлением о вручении или курьером (непосредственно в руки адресату под роспись).
5.7.10. В случае отзыва субъектом ПДн согласия на обработку его ПДн колледж обязан прекратить их обработку и, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва.
5.7.11. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн колледж обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн колледж обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн  с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.
5.7.12. В случае подтверждения факта неточности ПДн колледж на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязано уточнить ПДн в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.
5.7.13. В случае выявления неправомерной обработки ПДн, осуществляемой колледжем оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн. В случае, если обеспечить правомерность обработки ПДн невозможно, колледж в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязано уничтожить такие ПДн. Об устранении допущенных нарушений или об уничтожении ПДн колледж обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.
5.7.14. В случае достижения цели обработки ПДн колледж обязан прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которо-

му является субъект ПДн, иным соглашением между колледжем и субъектом ПДн.
5.7.15. Передача (обмен и т.д.) ПДн между подразделениями колледжа осуществляется только между работниками, имеющими доступ к ПДн субъектов.
5.7.16. При передаче ПДн субъекта работники, осуществляющие передачу, предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.
5.7.17. Допуск к ПДн работников, не имеющим надлежащим образом оформленного разрешения, запрещается.

5.8. Регламент обмена/выдачи информации (ПДн субъекта) третьим лицам (физическим и юридическим)
5.8.1. К числу внешних потребителей ПДн колледжа в соответствии с нормами действующего законодательства относятся государственные органы:
налоговые органы;
правоохранительные органы;
военкоматы;
органы социального страхования;
пенсионные фонды;
банк, в который колледж осуществляет перечисление заработной платы стипендии;
судебные органы по запросу субъекта ПДн.
5.8.2. При передаче ПДн субъекта уполномоченные лица должны придерживаться следующих требований:
- передача ПДн субъекта третьим лицам осуществляется только с письменного согласия субъекта, за исключением случаев, установленных федеральными законами;
- не допускается передача ПДн субъекта в коммерческих целях без его письменного согласия;
- передача ПДн по телефону запрещается;
- работникам колледжа, имеющим доступ к ПД, запрещена запись, хранение и вынос за пределы колледжа на внешних носителях информации (диски, дискеты, USB флэш-карты и т.п.), передача по внешним адресам электронной почты или размещение в сети Интернет информации, содержащей ПДН субъектов, за исключением случаев, указанных в настоящих Правилах или установленных иными внутренними документами колледжа; Передача третьим лицам документов (иных материальных носителей), содержащих ПДн субъектов, осуществляется по письменному запросу третьего лица на предоставление ПДн субъекта.

Ответы на письменные запросы даются на бланке колледжа и в том объеме, который позволяет не разглашать излишних сведений о субъекте ПДн; Работники колледжа, передающие ПДн субъектов третьим лицам, должны передавать их с обязательным уведомлением лица, получающего эти доку-

менты, об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена, и с предупреждением об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами. Уведомление и предупреждение могут быть реализованы путем подписания акта передачи носителей ПДн, в котором приведены указанные условия;

Представителю субъекта (в том числе адвокату) ПДн передаются в порядке, установленном действующим законодательством и настоящим документом. Информация передается при наличии одного из документов:
- нотариально удостоверенной доверенности представителя субъекта;
- письменного заявления субъекта, написанного в присутствии уполномоченного работника (если заявление написано субъектом не в его присутствии, то оно должно быть нотариально заверено);

Предоставление ПДн субъекта государственным органам производится в соответствии с требованиями действующего законодательства Российской Федерации;

ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда передача ПДн субъекта без его согласия допускается действующим законодательством РФ; Документы, содержащие ПДн субъекта, могут быть отправлены посредством федеральной почтовой связи заказным письмом. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие ПДн, вкладываются в конверт, в документах делается надпись о том, что ПДн, содержащиеся в письме, являются конфиденциальной информацией и не подлежат распространению и (или) опубликованию. Лица, виновные в нарушении требований конфиденциальности, несут ответственность, предусмотренную законодательством Российской Федерации.

5.8.3. Учет переданных ПДн осуществляется в рамках принятых в колледже правил делопроизводства путем регистрации входящей и исходящей корреспонденции и запросов, как государственных органов, так и структурных подразделений колледжа о предоставлении ПДн физических (юридических) лиц либо их представителей. Фиксируются сведения о лицах, направивших такие запросы, дата выдачи ПДн, а также дата уведомления об отказе в предоставлении ПДн (в случае отказа).

5.9. Уничтожение ПДн

5.9.1. ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.9.2. Уничтожение ПДн, не подлежащих архивному хранению, осуществляется только комиссией в составе представителя подразделения (или работника), ответственного за защиту ПДн и представителя структурного подразделения, в чьем ведении находятся указанные ПДн. По результатам уничтожения должен оформляться Акт.

6. Ответственность

6.1. С правилами работы и хранения конфиденциальной информации о ПДн в обязательном порядке должны быть ознакомлены все работники колледжа, подписав лист ознакомления с настоящими Правилами.

6.2. Работник, которому в силу трудовых отношений с колледжем стала известна информация, составляющая ПДн, в случае нарушения режима защиты этих ПДн несет материальную, дисциплинарную, административную, гражданско- правовую или уголовную ответственность в порядке, установленном федеральными законами Российской Федерации.

6.3. Разглашение ПДн субъектов ПДн (передача их посторонним лицам, в том числе работникам колледжа, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих ПДн субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящими Правилами, локальными нормативными актами (приказами, распоряжениями) колледжа, может повлечь наложение на работника, имеющего доступ к ПДн, дисциплинарного взыскания, если иное не предусмотрено законодательством РФ.

6.4. Работник колледжа, имеющий доступ к ПДн субъектов и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба колледжу (п.7 ст.243 Трудового кодекса РФ).

6.5. Работники колледжа, имеющие доступ к ПДн субъектов, виновные в незаконном разглашении или использовании ПДн субъектов без согласия субъектов из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут ответственность в соответствии с законодательством РФ.

6.6. Директор колледжа за нарушение норм, регулирующих получение, обработку и защиту ПДн работника, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей ПДн работника.

**Приложение 3**

## ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ

1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор – БПОУ ВО ЧМК и филиал, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных в отношении себя, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Сведения о наличии персональных данных должны быть представлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

4. Доступ к своим персональным данным представляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с действующим законодательством Российской Федерации. Законный представитель представляет оператору документ,
подтверждающий его полномочия.

5. Субъект персональных данных имеет право на получение при обращении к оператору, следующих сведений:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место 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 законодательства Российской Федерации;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством Российской Федерации;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
10) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами Российской Федерации.

6. Если запрос субъекта персональных данных связан с внесением изменений в персональные данные субъекта в связи с тем, что персональные данные, обрабатываемые оператором, являются неполными, устаревшими, недостоверными, то в таком запросе субъект персональных данных должен указать какие именно персональные данные изменяются или уточняются. Если для внесения изменений в персональные данные необходимы подтверждающие документы, то субъект персональных данных прикладывает к своему запросу об изменении персональных данных доказательства, на основании которых оператор должен внести изменения или уточнить персональные данные. В случае отсутствия доказательств, на которые ссылается субъект персональных данных, оператор оставляет персональные данные в неизменном виде. Внесение изменений или уточнение персональных данных оператором должны быть выполнены в течение 7 рабочих дней со дня предоставления таких сведений. Изменения, уничтожение или блокирование персональных данных соответствующего субъекта осуществляется оператором на безвозмездной основе.

**Приложение 4**

## ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕ-

# РАЛЬНЫМЗАКОНОМ "О ПЕРСОНАЛЬНЫХ ДАННЫХ", ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ И ЛОКАЛЬНЫМИ АКТАМИ БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ»

Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами (далее – Правила) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152 «О персональных данных». В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в БПОУ ВО «Череповецкий многопрофильный колледж» (далее – колледж) и Шекснинском филиале БПОУ ВО «Череповецкий многопрофильный колледж» (далее филиал) организовывается проведение периодических проверок условий обработки персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных в колледже и филиале либо комиссией, созданной на основании приказа директора колледжа.

В проведении проверки не может участвовать работник колледжа или филиала, прямо или косвенно заинтересованный в ее результатах.

Проверки соответствия обработки персональных данных установленным требованиям в колледже и филиале проводятся на основании утвержденного директором ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- осуществление мероприятий по обеспечению целостности персональных данных.

Ответственный за организацию обработки персональных данных в колледже и филиале имеет право:
- запрашивать у работников колледжа и филиала информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- представлять директору колледжа предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- представлять директору колледжа предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в колледже в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении. По результатам проведенной проверки составляется Акт, в котором указывается перечень мер, необходимых для устранения выявленных нарушений.

**Приложение 5**

## ПРАВИЛА
## РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

### 1.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Перечень сокращений:
ПДн Персональные данные

НСД Несанкционированный доступ
АИС Автоматизированная информационная система
ИСПДн Информационная система персональных данных
Колледж – БПОУ ВО «Череповецкий многопрофильный колледж»
Филиал – Шекснинский филиал БПОУ ВО «Череповецкий многопрофильный колледж»

В рамках данного документа используются следующие термины и определения:

Доступ к информации – возможность получения информации и ее использования.

Защита информации от несанкционированного доступа (защита от НСД) или воздействия – деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

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

АИС колледжа – объединение информационных систем, в том числе информационных систем персональных данных, компьютерного, телекоммуникационного и офисного оборудования всех отделов (подразделений) колледжа, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Нарушение информационной безопасности – событие, при котором компрометируется один или несколько аспектов безопасности информации (доступность, конфиденциальность или целостность). Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Оператор – государственный орган, муниципальный орган, 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.

Пользователь информационной системы – работник колледжа (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в АИС колледжа в установленном порядке.

## 2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие Правила работы с обезличенными персональными данными колледжа разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 № 996 "Об утверждении требований и методов по обезличиванию персональных данных" (с приложением «Требований и методов по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ») и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

## 3. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПДн

Обезличивание ПДн должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых ПДн.

К свойствам обезличенных данных относятся:

- полнота (сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания);

- структурированность (сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания);
- релевантность (возможность обработки запросов по обработке ПДн и получения ответов в одинаковой семантической форме);
- семантическая целостность (сохранение семантики ПДн при их обезличивании);
- применимость (возможность решения задач обработки ПДн, стоящих перед оператором, осуществляющим обезличивание ПДн, обрабатываемых в ИС-ПДн, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ (далее - оператор, операторы), без предварительного деобезличивания всего объема записей о субъектах); - анонимность (невозможность однозначной идентификации субъектов ПДн, полученных в результате обезличивания, без применения дополнительной информации).

К характеристикам (свойствам) методов обезличивания ПДн (далее - методы обезличивания), определяющим возможность обеспечения заданных свойств обезличенных данных, относятся:
- обратимость (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность ПДн конкретному субъекту, устранить анонимность);
- вариативность (возможность внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);
- изменяемость (возможность внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);
- стойкость (стойкость метода к атакам на идентификацию субъекта ПДн); - возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием информации других операторов);
- совместимость (возможность интеграции ПДн, обезличенных различными методами);
- параметрический объем (объем дополнительной (служебной) информации, необходимой для реализации метода обезличивания и деобезличивания);
- возможность оценки качества данных (возможность проведения контроля качества обезличенных данных и соответствия применяемых процедур обезличивания установленным для них требованиям).

Требования к методам обезличивания подразделяются на:
- требования к свойствам обезличенных данных, получаемых при применении метода обезличивания;
- требования к свойствам, которыми должен обладать метод обезличивания.

К требованиям к свойствам получаемых обезличенных данных относятся:
- сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых ПДн);
- сохранение структурированности обезличиваемых ПДн;

- сохранение семантической целостности обезличиваемых ПДн;
- анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания как, например, k-anonymity).

К требованиям к свойствам метода обезличивания относятся:
- обратимость (возможность проведения деобезличивания);
- возможность обеспечения заданного уровня анонимности;
- увеличение стойкости при увеличении объема обезличиваемых ПДн.

Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки ПДн.

Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации. При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:
- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:
- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

## 4. Ответственность

Ответственность за осуществление общего контроля выполнения требований настоящих Правил несет ответственный за организацию обработки ПДн в колледже и филиале.

Ответственность за поддержание данного документа в актуальном состоянии несет председатель Постоянно действующей комиссии колледжа. Ответственность за доведение положений настоящего документа до всех работников колледжа и филиала, задействованных в обработке ПДн и иных лиц в части их касающейся, а также контроль соблюдения требований документа возлагается на заместителя директора по учебно-производственной работе.

Ответственность за выполнение настоящих Правил возлагается на всех работников колледжа и филиала, допущенных к обработке ПДн.

Работник колледжа и филиала несёт ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкциони-

рованного использования учетной записи другими лицами при соблюдении пользователем требований настоящих Правил.

Работники колледжа и филиала несут персональную ответственность за ущерб, причиненный колледжу и субъектам ПДн вследствие нарушения ими установленных требований в области обработки и обеспечения защиты ПДн, в соответствии с законодательством Российской Федерации. Работники, нарушающие требования настоящих Правил, могут быть подвергнуты дисциплинарным взысканиям и увольнению с работы за неоднократное грубое нарушение Правил работы в АИС колледжа

**Приложение 6**

**ПЕРЕЧЕНЬ**
**ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ» И ШЕКСНИНСКОМ ФИЛИАЛЕ БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ» В СВЯЗИ С РЕАЛИЗАЦИЕЙ СЛУЖЕБНЫХ ИЛИ ТРУДОВЫХ ОТНОШЕНИЙ, А ТАКЖЕ В СВЯЗИ СО-**

**КАЗАНИЕМ ГОСУДАРСТВЕННЫХ УСЛУГ И ОСУЩЕСТВЛЕНИЕМ ГОСУДАРСТВЕННЫХ ФУНКЦИЙ**

Перечень персональных данных, обрабатываемых в БПОУ ВО «Череповецкий многопрофильный колледж» и Шекснинском филиале БПОУ ВО «Череповецкий многопрофильный колледж»:
- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- адрес;
- семейное положение;
- образование;
- профессия;
- доходы;
- фотографическое изображение;
- данные документов удостоверяющих личность;
- данные страхового медицинского полиса;
- данные документов воинского учета;
- данные свидетельства пенсионного страхования;
- данные трудовой книжки;
- сведения о присвоении категории;
- сведения о наградах;
- ИНН;
- гражданство;
- номер телефона.

**Приложение 7**

**ПЕРЕЧЕНЬ**
**ДОЛЖНОСТЕЙ СЛУЖАЩИХ БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ» И ШЕКСНИНСКОГО ФИЛИАЛА БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ», ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В рамках реализации требований Федерального закона от 27 июля 2006 г № 152-ФЗ «О персональных данных» и постановления Правительства Рос-

сийской Федерации от 21.03.2012 № 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» в БПОУ ВО «Череповецкий многопрофильный колледж» и Шекснинском филиале БПОУ ВО «Череповецкий многопрофильный колледж» утверждается «Перечень должностей служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных».

Планово-экономический отдел
1 Начальник ПЭО
2 Экономист
3 Документовед

1. Начальник отдела МТС
2. Контрактный управляющий
1. Специалист по кадрам
Учебная часть
1.Заместитель директора по учебно-производственной работе
2. Секретарь учебной части
3. Секретарь-машинистка (филиал)

Воспитательная служба
1.Заведующий учебно-воспитательной по социальной работе
2.Социальный педагог
3. Педагог-психолог

Сектор информационной деятельности и организационной работы
1.Педагог-библиотекарь

По мере возникновения необходимости настоящий перечень подлежит своевременной корректировке.

**Приложение 8**

**ПЕРЕЧЕНЬ**
**ДОЛЖНОСТЕЙ СЛУЖАЩИХ БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ» И ШЕКСНИНСКОГО ФИЛИАЛА БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ», ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТ ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ОСУЩЕСТВЛЕНИЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ**

Перечень должностей служащих, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

Планово-экономический отдел
1 Начальник ПЭО
2 Экономист
3 Документовед

1. Начальник отдела МТС
2. Контрактный управляющий
3. Специалист по кадрам

Учебная часть
1.Заместитель директора по учебно-производственной работе
2. Секретарь учебной части
3. Секретарь-машинистка (филиал)

Воспитательная служба
1.Заведующий учебно-воспитательной по социальной работе
2.Социальный педагог
3. Педагог-психолог

Сектор информационной деятельности и организационной работы
1.Педагог-библиотекарь

**Приложение 9**

**ДОЛЖНОСТНОЙ РЕГЛАМЕНТ**
**ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**
**В БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ» И ШЕКСНИНСКОГО ФИЛИАЛА БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ»**

Ответственный за организацию обработки персональных данных обязан:

1. Организовать предоставление субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных.
2. Осуществлять внутренний текущий контроль за соблюдением требований законодательства Российской Федерации в сфере персональных данных в колледже при обработке персональных данных, в том числе требований к защите персональных данных.
3. Доводить до сведения лиц, допущенных к обработке персональных данных, положения федерального законодательства Российской Федерации о персональных данных, нормативных правовых актов колледжа по вопросам обработки персональных данных, требований к защите персональных данных.
4. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.
5. Организовать получение обязательства о прекращении обработки персональных данных у лиц, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ним договора (контракта).
6. Организовать получение согласия на обработку персональных данных у субъектов персональных данных (при необходимости).
7. Организовать разъяснение субъекту персональных данных юридические последствия отказа предоставления его персональных данных.

**Приложение 10**

## ПОРЯДОК ДОСТУПА РАБОТНИКОВ БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ» И ШЕКСНИНСКОГО ФИЛИАЛА БПОУ ВО «ЧЕРЕПОВЕЦКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ» В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Порядок доступа работников БПОУ ВО «Череповецкий многопрофильный колледж» и Шекснинского филиала БПОУ ВО «Череповецкий многопрофильный колледж» в помещения, в которых ведется обработка персональных данных

1. Персональные данные относятся к категории конфиденциальной информации. Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
2. Список работников, допущенных к обработке персональных данных, утверждается директором колледжа.
3. Порядок определяет правила доступа в помещения, где хранятся и обрабатываются персональные данные, в целях исключения несанкционированного доступа к персональным данным, а также обеспечения безопасности персональных данных от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении персональных данных.
4. В помещения, где размещены материальные носители информации, содержащие персональные данные, допускаются только работники колледжа, имеющие доступ к персональным данным.
5. Работники, имеющие доступ к персональным данным, не должны:
- оставлять в свое отсутствие незапертым помещение, в котором размещены технические средства, позволяющие осуществлять обработку персональных данных;
- оставлять в помещении посторонних лиц, не имеющих доступа к персональным данным в данном структурном подразделении, без присмотра.
6. Для помещений, в которых хранятся и обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащей персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим обеспечивается:
- оснащением здания охранной и пожарной сигнализацией;
- обязательным запиранием помещения на ключ, даже при выходе из него в рабочее время;
- отдельным хранением дубликатов ключей;
- закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные.
7. Ответственность за несоблюдение Порядка несут руководители структурных подразделений колледжа, в которых ведется обработка персональных данных и осуществляется их хранение.
8. Внутренний контроль за соблюдением в колледже порядка доступа в помещения, в которых ведется обработка персональных данных, требованиям к защите персональных данных, осуществляется лицом, ответственным за ор-

ганизацию обработки персональных данных в соответствии с «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральным законом «О персональных данных», принятыми в соответствии с ним локальными актами колледжа.

**Приложение № 11**

## РЕГЛАМЕНТ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

### 1.Общие положения

Настоящий Регламент осуществления контроля защищенности персональных данных и соблюдений условий использования средств защиты ин-

формации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах персональных данных БПОУ ВО «Череповецкий многопрофильный колледж» (далее – Регламент) и Шекснинского филиала БПОУ ВО «Череповецкий многопрофильный колледж» (далее - филиал) устанавливает и определяет единый и обязательный порядок проведения контрольных мероприятий для каждой из подсистем, входящих в систему защиты персональных данных информационных систем персональных данных (далее -ИСПДн ) БПОУ ВО «Череповецкий многопрофильный колледж» и Шекснинского филиала БПОУ ВО «Череповецкий многопрофильный колледж».

Настоящий Регламент утверждается и вводится директором БПОУ ВО «Череповецкий многопрофильный колледж» и является обязательным для исполнения.

## 2.Порядок подготовки к проведению контрольных мероприятий

Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн колледжа и филиала проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации колледжа и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;
- оценка уровня осведомленности и знаний работников колледжа и филиала в области обработки и защиты персональных данных (далее - ПДн);
- оценка обоснованности и эффективности применяемых мер и средств защиты

### 2.1.Виды контрольных мероприятий

Контрольные мероприятия подразделяются на внутренние и внешние. Внутренние контрольные мероприятия осуществляются силами работников колледжа и филиала, ответственных за обеспечение безопасности ПДн. При проведении внешних контрольных мероприятий привлекаются сторонние организации.

Контрольные мероприятия подразделяются на плановые и внеплановые. Плановые контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План) и направлены на постоянное совершенствование системы защиты персональных данных колледжа и филиала.

Внеплановые контрольные мероприятия проводятся на основании решения заместителя директора по учебно-производственной работе. Решение о

проведении внеплановых контрольных мероприятий может быть принято в следующих случаях:
- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами.

Любой работник колледжа или филиала вправе подготавливать обоснованные предложения о необходимости проведения внеплановых контрольных мероприятий и предоставить их лицу, ответственному за обеспечение безопасности ПДн

### 2.2. План проведения контрольных мероприятий

Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

План проведения внутренних контрольных мероприятий (как плановых, так и внеплановых) включает следующие сведения по каждому из мероприятий:
- цели проведения контрольных мероприятий;
- задачи проведения контрольных мероприятий,
- объекты контроля (процессы, подразделения, информационные системы и т.п.);
- состав участников, привлекаемых для проведения контрольных мероприятий;
- сроки и этапы проведения контрольных мероприятий.

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

## 3. Общий порядок проведения контрольных мероприятий

Контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы информационных систем, администраторы информационной безопасности.

Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

### 3.1.Контрольные мероприятия в подсистеме управления доступом

При проведении контрольных мероприятий в подсистеме управления доступом, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия установленных прав доступа (в прикладных системах, базах данных и т.п.) полномочиям в рамках трудовых обязанностей работника;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
-проверка процесса идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам информационных систем);
-проверка механизмов блокирования доступа к средствам защиты от несанкционированного доступа (далее - НСД) при выполнении устанавливаемого числа неудачных попыток ввода пароля;
- проверка системы смены пароля принудительным образом (по истечению срока действия пароля);
- проверка выполнения требований по стойкости пароля

### 3.2. Мероприятия в подсистеме регистрации и учета

При проведении контрольных мероприятий в подсистеме регистрации и учета, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка системных журналов на наличие зарегистрированных попыток несанкционированного доступа;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации и внутренних документах компании;

- имитация попытки несанкционированного доступа в систему, для проверки работы системы регистрации попытки НСД в системном журнале;
- проверка способов защиты системного журнала регистрации от уничтожения или модификации нарушителе;
-проверка функционирующей системы автоматического непрерывного мониторинга событий в системе, которые могут являться причиной реализации угроз (создание, редактирование, запись, компиляция объектов).

Кроме того, при проведении проверок в части учета и хранения носителей персональных данных могут выполняться следующие проверки:
-проверка мест хранения носителей ПДн, сейфов и металлических шкафов, надежность их замков;
- проверка выполнения установленного порядка учета и хранения носителей ПДн;
- проверка фактического наличия всех носителей ПДн, в том числе учетные журналы, дела, документы (поступившие, изданные, переведенные на выделенное хранение);
- проверка фактического наличия всех носителей ПДн, переданных на архивное хранение;
- проверка фактического наличия всех не подшитых в дела и поступивших документов, содержащих ПДн, независимо от даты их регистрации;
- проверка номенклатуры дел с целью выделения документов, содержащих ПДн, для передачи в архив или на уничтожение;
- проверка правильности проставления регистрационных данных носителей, документов и дел, и учетных журналов;
- проверка правильности проставления в журнале отметок о движении носителей.

### 3.3. Контрольные мероприятия в подсистеме обеспечения целостности

При проведении контрольных мероприятий в подсистеме обеспечения целостности, в зависимости от целей мероприятий, могут выполняться следующие проверки:
- проверка механизмов контроля целостности пакетов обновлений средств защиты информации с использованием контрольных сумм;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка целостности используемого программного обеспечения, путем вычисления контрольных сумм;
- проверка фактического наличия экземпляров резервных копий;
-проверка целостности сделанных резервных копий путем восстановления данных;
- имитация выполнения резервного копирования и восстановления данных при аварийном режиме функционирования системы.

### 3.4.Контрольные мероприятия в подсистеме антивирусной защиты

При проведении контрольных мероприятий в подсистеме антивирусной защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:
- проверка рабочих станций и серверов станций на наличие установленных программных средств антивирусной защиты;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка механизма своевременного обновления программных средств антивирусной защиты (в т.ч. баз данных вирусных сигнатур) на всех рабочих и серверных станциях;
-запуск полного сканирования системы в режиме реального времени антивирусным средством;
-проверка антивирусным средством используемых отчуждаемых носителей;
- проверка функционирования механизмов принудительной проверки используемых съемных носителей;
- имитация попыток заражения вредоносным программным обеспечением[1] серверных и рабочих станций;
- просмотр системных журналов и отчетов на наличие зафиксированных случаев заражения вредоносным ПО.

### 3.5.Контрольные мероприятия в подсистеме обеспечения безопасного межсетевого взаимодействия

При проведении контрольных мероприятий в подсистеме обеспечения безопасного межсетевого взаимодействия, в зависимости от целей мероприятий, могут выполняться следующие проверки:
- проверка соответствия установленных межсетевых экранов требуемому уровню защищенности;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток проникновения в «закрытый» сегмент сети из открытого, в том числе с применением специального ПО;
- проверка системных журналов на наличие зафиксированных попыток обращения к «закрытым» ресурсам.

### 3.6. Контрольные мероприятия в подсистеме анализа защищенности

При проведении контрольных мероприятий в подсистеме анализа защищенности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка выполнения своевременного обновления ПО, используемого для анализа защищенности, в т.ч. баз данных уязвимостей;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток преодоления системы защиты, проверка системных журналов на наличие зафиксированных попыток НСД.

### 3.7. Контрольные мероприятия в подсистеме обнаружения и предотвращения вторжений

При проведении контрольных мероприятий в подсистеме обнаружения и предотвращения вторжений, в зависимости от целей мероприятий, могут выполняться следующие проверки:
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.

Контрольные мероприятия в подсистеме защиты от утечек по техническим каналам

При проведении контрольных мероприятий в подсистеме защиты от утечек по техническим каналам, в зависимости от целей мероприятий, могут выполняться следующие проверки:
- проверка в помещениях, где ведется обработка ПДн, установленных на окна жалюзи, штор и т.п.;
- проверка размещения дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторы, телевизоры и т.п.) таким образом, чтобы исключалась возможность просмотра посторонними лицами текстовой и графической информации, содержащей персональные данные.

### 3.8. Контрольные мероприятия в подсистеме физической защиты

При проведении контрольных мероприятий в подсистеме физической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:
- проверка введения журналов учета посетителей, проходящих на территорию колледжа.
- проверка введения журналов посетителей, проходящих в защищаемые помещения;
- проверка электронных журналов СКУД на предмет попыток НСД в защищаемые помещения сотрудников, не имеющих права доступа в данные помещения;
- проверка наличия ключей (в том числе и электронных пропусков) от защищаемых помещений, а так же проверка сохранности вторых экземпляров ключей от защищаемых помещений;
- просмотр всех заявлений об утерянных ключах (в том числе и электронных пропусках) по которым можно получить доступ в защищаемые помещения, а

так же проверка принятых мер (блокирование электронного пропуска, смена замка);
- проверка надежности замков, установленных в защищаемых помещениях;
- имитация попытки проникновения в защищаемые помещения для проверки срабатывания сигнализации и (или) системы контроля и управления доступом.

### 3.9. Контрольные мероприятия в подсистеме криптографической защиты

При проведении контрольных мероприятий в подсистеме криптографической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.
- проверка сохранности эксплуатационной и технической документации и ключевых документов на средства криптографической защиты;
- проверка журналов учета средств криптографической защиты и используемых криптоключей на правильность их ведения и хранения;
- проверка знаний работниками, использующими средства криптографической защиты, правил применения этих средств и правил обращения с криптоключами;
- проверка функционирования средств криптографической защиты путем имитации процессов, шифровании и дешифрования информации.

**Приложение № 12**

# РЕГЛАМЕНТ ВЗАИМОДЕЙСТВИЯ С УПОЛНОМОЧЕННЫМ ОРГАНОМ ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 1. Сокращения, термины и определения

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор – государственный орган, муниципальный орган, 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.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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 (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

## 2. Общие положения

Настоящий Регламент взаимодействия с органами власти по вопросам защиты и обработки персональных данных (далее – Регламент) определяет единый и обязательный порядок взаимодействия с регулирующими органами по вопросам обработки и обеспечения защиты ПДн, а также определяет порядок реагирования на запросы, поступающие от органов власти.

Настоящий Регламент определяет порядок действий сотрудников БПОУ ВО «Череповецкий многопрофильный колледж» (далее – Оператор) при проведении плановых и внеплановых проверок регулирующими органами, а также при обработке отдельных запросов, поступивших от органов власти.

Настоящий Регламент является обязательным для исполнения сотрудниками, ответственными за взаимодействие с органами власти.

Ответственным за выполнение требований данного документа и реализацию указанных в нем процедур является ответственный за организацию обработки персональных данных.

## 2. Полномочия органов власти

3.1 Регулирующие органы власти в области контроля обработки и обеспечения защиты ПДн

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как уполномоченный орган по защите прав субъектов персональных данных осуществляет федеральный государственный контроль (надзор) за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн.

3.1.1 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Роскомнадзор и его территориальные органы уполномочены проводить плановые и внеплановые проверки с целью осуществления контроля и надзора за выполнением требований законодательства Российской Федерации, предъявляемых к обработке ПДн.

В ходе проведения проверок Роскомнадзор и его территориальные органы могут запрашивать для рассмотрения следующие документы:

- уведомление об обработке ПДн;
- документы, необходимые для проверки фактов, содержащих признаки нарушения законодательства РФ в области ПДн и изложенных в обраще-

ниях граждан и информации, поступившей в Роскомнадзор или его территориальный орган;

- документы, подтверждающие выполнение Оператором предписаний об устранении ранее выявленных нарушений законодательства Российской Федерации в области ПДн;
- письменные согласия субъекта ПДн на обработку их ПДн;
- документы, подтверждающие факты уничтожения ПДн субъектов ПДн по достижении цели обработки;
- локальные акты Оператора, регламентирующие порядок и условия обработки ПДн.
- Роскомнадзор и его территориальные органы вправе:
- запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- осуществлять проверку сведений, содержащихся в уведомлении об обработке ПДн, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
- требовать от Оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;
- принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства РФ в области ПДн;
- обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн и представлять интересы субъектов ПДн в суде;
- направлять заявление в орган, осуществляющий лицензирование деятельности Оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу ПДн третьим лицам без согласия в письменной форме субъекта ПДн;
- направлять в правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн;
- привлекать к административной ответственности лиц, виновных в нарушении законодательства Российской Федерации в области ПДн;
- исследовать (обследовать) информационные системы персональных данных, в части касающейся персональных данных субъектов персональных данных, обрабатываемых в ней.

3.1.2 Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

ФСТЭК России уполномочен проводить проверки с целью осуществления контроля и надзора выполнения требований законодательства Россий-

ской Федерации в области обеспечения защиты (некриптографическими методами) конфиденциальной информации, предотвращения ее утечки по техническим каналам и за счет несанкционированного доступа к данной информации.

При проведении проверок должностные лица ФСТЭК вправе допускаться к средствам защиты информации, техническим средствам, на которых они реализованы, оборудованию комплексов, в помещения, в которых установлены, к средствам технической защиты, предназначенным для хранения, обработки и передачи персональных и ключевых документов.

По результатам проверок ФСТЭК оценивается достаточность принятых у Оператора мер по обеспечению безопасности ПДн при их обработке в ИСПДн, а также соответствие реализованных у Оператора методов и способов защиты информации классам ИСПДн.

3.1.3 Федеральная служба безопасности (ФСБ России)

ФСБ уполномочена проводить проверки с целью осуществления контроля и надзора за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности ПДн при их обработке в ИСПДн, в частности за выполнением требований использования шифровальных (криптографических) средств, применяемых для обеспечения безопасности ПДн.

При проведении проверок должностные лица ФСБ вправе допускаться к средствам криптографической защиты информации, техническим средствам, на которых они реализованы, оборудованию комплексов, в помещения, в которых установлены криптосредства, к средствам технической защиты, предназначенным для хранения, обработки и передачи персональных данных и ключевых документов.

## 4. Органы власти, уполномоченные направлять запросы на предоставление данных о субъектах

Органы власти уполномочены направлять у Оператора мотивированные запросы с целью получения ПДн соответствующих субъектов, необходимых для выполнения возложенных на них обязанностей.

Допустимые объем и состав ПДн, запрашиваемых органами власти, определяются соответствующими законодательными актами Российской Федерации для каждого органа власти.

## 5. Проведение проверочных мероприятий

5.1 Виды проверочных мероприятий

Регулирующим органом власти в области защиты ПДн (далее – Регулятор) могут проводиться плановые и внеплановые проверки на предмет соответствия требованиям законодательства Российской Федерации в области ПДн.

Регулятором проводятся плановые и внеплановые проверки, которые в свою очередь подразделяются на документарные и выездные проверки.

При осуществлении проверочных мероприятий для оценки эффективности принимаемых Оператором технических мер по обеспечению безопасности персональных данных при их обработке в негосударственных информационных системах персональных данных, Регулятор или его территориальный орган в рамках проверки привлекают экспертов, экспертные организации, включенные в установленном порядке в реестр граждан и организаций, привлекаемых Регулятором в качестве экспертов, экспертных организаций к проведению мероприятий по контролю.

5.1.1 Плановые проверки

Плановые проверки проводятся на основании ежегодного плана проведения проверок, утвержденного руководителем Регулятора.

О проведении плановой проверки Оператор уведомляется не позднее чем в течение трех рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Регулятора почтовым отправлением с уведомлением о вручении или иным доступным способом.

5.1.2 Внеплановые проверки

Основанием для проведения внеплановых проверок являются:

- истечение срока исполнения Оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области ПДн;
- поступление обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о фактах возникновения угрозы причинения вреда жизни, здоровью граждан или фактах причинения вреда жизни, здоровью граждан;
- приказ руководителя Регулятора, изданный в соответствии с поручениями Президента РФ, Правительства РФ;
- нарушение прав и законных интересов граждан действиями (бездействием) Оператором при обработке их ПДн;
- нарушение Оператором требований законодательства Российской Федерации в области ПДн, а также несоответствия сведений, содержащихся в уведомление об обработке персональных данных, фактической деятельности.

О проведении внеплановой выездной проверки Оператор уведомляется не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом.

Если в результате деятельности Оператора причинен или причиняется вред жизни, здоровью граждан, предварительное уведомление Оператора о начале проведения внеплановой выездной проверки не требуется.

5.2 Основания для проведения проверки

Основанием для проведения проверки Регулятором является приказ, утвержденный руководителем Регулятора. В приказе о проведении проверки указываются:

- наименование органа федерального государственного контроля (надзора);
- фамилии имена отчества должностных лиц, проводящих проверку;
- наименование (фамилия, имя, отчество) Оператора;
- цели, задачи, предмет проверки и срок ее проведения;
- правовые основания проведения проверки, в том числе подлежащие проверке обязательные требования законодательства Российской Федерации в области ПДн;
- сроки проведения и перечень мероприятий по контролю, необходимых для достижения целей и задач проведения проверки;
- перечень административных регламентов проведения мероприятий по контролю;
- перечень документов, представление которых Оператором необходимо для достижения целей и задач проведения проверки;
- даты начала и окончания проведения проверки.

5.3 Порядок проведения проверок

У Оператора ответственность за организацию взаимодействия с регулирующими органами по вопросам обработки и обеспечения защиты ПДн при проведении плановых и внеплановых проверок, а также за координацию сотрудников при проведении проверок возлагается на Администратора безопасности ИСПДн и Менеджера обработки ПДн.

Перед началом проверки должностное лицо Регулятора предъявляет Менеджеру обработки ПДн копию приказа о проведении проверки, заверенную гербовой печатью Регулятора, и служебное удостоверение.

На втором экземпляре копии приказа о проведении проверки, остающейся у должностного лица Регулятора, Менеджер обработки ПДн проставляет отметку о получении копии приказа о проведении проверки с указанием должности, фамилии, имени и отчества, а также даты и времени его получения.

Проверка может проводиться только должностными лицами Регулятора, которые указаны в приказе о ее проведении.

При необходимости изменения состава должностных лиц Регулятора или ее территориального органа, проводящего проверку, Регулятор или ее территориальный орган издает соответствующий приказ.

В случае проведения проверок ФСТЭК России или ФСБ России для взаимодействия с Регуляторами привлекается Администратор безопасности ИСПДн.

5.3.1 Порядок проведения документарной проверки

Регулятором проводится проверка в отношении следующих документов:

- уведомление об обработке ПДн;
- документы, необходимые для проверки фактов, содержащих признаки нарушения законодательства РФ в области ПДн и изложенных в обращениях граждан и информации, поступившей в Роскомнадзор или его территориальный орган;
- документы, подтверждающие выполнение у Оператора предписаний об устранении ранее выявленных нарушений законодательства Российской Федерации в области ПДн;
- письменные согласия субъекта ПДн на обработку их ПДн;
- документы, подтверждающие факты уничтожения ПДн субъектов ПДн по достижении цели обработки;
- локальные акты Оператора, регламентирующие порядок и условия обработки ПДн.

При проведении документарной проверки, в случае если возникает подобная необходимость, Регулятор может запрашивать дополнительные внутренние локальные документы Оператора.

Для этого Регулятор направляет в адрес Оператора мотивированный запрос с требованием представить иные необходимые для рассмотрения в ходе проведения документарной проверки документы. К запросу прилагается заверенная печатью копия приказа руководителя или заместителя руководителя Регулятора.

Менеджер обработки ПДн зависимости от характера запрашиваемых документов перенаправляет данный запрос Администратору безопасности ИСПДн (далее – ответственный сотрудник).

В течение десяти рабочих дней со дня получения мотивированного запроса ответственный сотрудник подготавливают и направляют Регулятору указанные в запросе документы.

Указанные документы представляются в виде копий, заверенных печатью и подписью руководителя Оператора или Администратора информационной безопасности.

В случае если в ходе документарной проверки были выявлены ошибки и (или) противоречия в представленных документах либо несоответствие сведений, содержащихся в этих документах, сведениям, содержащимся в имеющихся у Регулятора документах и (или) полученным в ходе проведения государственного контроля (надзора), информация об этом направляется у Оператора с требованием представить в течение десяти рабочих дней необходимые пояснения в письменной форме.

При получении подобного запроса ответственные сотрудники подготавливают ответ и в случае необходимости представляют дополнительные документы, подтверждающие достоверность ранее представленных документов.

5.3.2 Порядок проведения выездной проверки

Менеджер обработки ПДн обязан предоставить должностным лицам Регулятора возможность ознакомиться с документами, связанными с целями, задачами и предметом выездной проверки, в случае, если выездной проверке не предшествовало проведение документарной проверки, а также обеспечить доступ должностных лиц Регулятора, проводящих выездную проверку, на территорию, в используемые при осуществлении обработки ПДн здания, строения, сооружения, помещения, к используемому оборудованию.

Менеджер обработки ПДн сопровождает уполномоченное лицо в служебных помещениях при проведении проверки, организует взаимодействие с сотрудниками, ответственными за обеспечение безопасности ПДн у Оператора. При необходимости привлекает для этих целей Администратора безопасности ИСПДн.

Регулятор не вправе осуществлять плановую или внеплановую выездную проверку в случае отсутствия при ее проведении руководителя Оператора или Менеджера обработки ПДн, за исключением случаев проведения проверки на основании поступивших запросов о том, что обработка ПДн у Оператора наносит вред здоровью или жизни субъектам.

5.4 Сроки проведения проверок

Срок проведения как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней.

В случае возникновения необходимости срок проведения проверки может быть продлен, но не более чем на двадцать рабочих дней. Основанием для продления сроков проведения проверки является приказ руководителя Регулятора.

5.5 Результаты проведения проверки

Результаты проверки оформляются актом, который составляется должностными лицами Регулятора непосредственно после завершения проверки. В акте указываются:

- дата, время и место составления акта проверки;
- наименование органа федерального государственного контроля (надзора);
- дата и номер приказа проведения проверки;
- цели, задачи и предмет проверки;
- Ф.И.О. должностных лиц, проводивших проверку;
- наименование Оператора, а также Ф.И.О. и должность лиц, присутствовавших при проведении проверки;
- дата, время, продолжительность и место проведения проверки;
- сведения о результатах проверки, в том числе о выявленных нарушениях в области ПДн, об их характере и о лицах, допустивших указанные нарушения;
- сведения об ознакомлении или отказе в ознакомлении с актом проверки руководителя, иного уполномоченного представителя Оператора, при-

сутствовавших при проведении проверки, о наличии их подписей или об отказе от совершения подписи;

- сведения о внесении в журнал учета проверок записи о проведенной проверке либо о невозможности внесения такой записи в связи с отсутствием у Оператора указанного журнала.

Акт закрепляется подписями должностных лиц Регулятора, проводивших проверку, и должен содержать одно из следующих заключений:

- об отсутствии в деятельности Оператора нарушений требований законодательства Российской Федерации в области ПДн;
- о выявленных в деятельности Оператора нарушениях требований законодательства Российской Федерации в области ПДн с указанием конкретных статей и (или) пунктов нормативных правовых актов.

Акт составляется в двух экземплярах. Один экземпляр акта с копиями приложений вручается Администратору безопасности ИСПДн под расписку об ознакомлении либо об отказе в ознакомлении с актом проверки или направляется заказным почтовым отправлением с уведомлением о вручении.

Менеджер обработки ПДн в случае несогласия с решениями, изложенными в акте проверки, а также с выводами и предложениями проверяющих, в течение 15 дней со дня получения акта проверки вправе представить письменные возражения по указанному акту в целом или по его отдельным положениям. Возражения, изложенные в письменной форме, прилагаются к акту.

К акту могут прилагаться протоколы, справки, объяснительные работникоу Оператора, на которых возложены обязанности по обработке ПДн, и другие документы, подтверждающие выявление (устранение) нарушения.

В случае выявления по результатам проверки нарушения требований законодательства Российской Федерации в области ПДн вместе с актом выдается предписание об устранении выявленных нарушений, в котором указываются:

- наименование органа федерального государственного контроля (надзора);
- дата выдачи предписания об устранении выявленных нарушений;
- номер предписания об устранении выявленных нарушений;
- наименование Оператора;
- регистрационный номер Оператора в Реестре (при наличии);
- наименование вида деятельности;
- дата и номер акта проверки;
- содержание нарушения;
- основание выдачи предписания;
- срок устранения нарушения;
- срок информирования органа федерального государственного контроля (надзора) об устранении выявленного нарушения;
- подписи должностных лиц, проводивших проверку.

После окончания проверки должностное лицо Регулятора производит запись о проведенной проверке в Журнале учета проверок. Форма Журнала учета проверок установлена Приказом Минэкономразвития России от 30.04.2009 № 141 . Журнал учета проверок должен быть прошит, пронумерован и удостоверен печатью Оператора.

У Оператора ответственным за ведение журнала учета проверок является ответственный за организацию обработки Пдн.

5.6 Ограничение прав Регулятора

При проведении проверки должностные лица Регулятора не вправе:

- проверять выполнение обязательных требований и требований, установленных нормативными правовыми актами в области персональных данных, если такие требования не относятся к полномочиям Регулятора;
- требовать представления документов, информации, если они не относятся к предмету проверки, а также изымать оригиналы таких документов;
- распространять информацию, полученную в результате проведения проверки, за исключением случаев, предусмотренных законодательством Российской Федерации;
- превышать установленные сроки проведения проверки;
- осуществлять выдачу предписаний или предложений о проведении проверки за счет Оператора.

## 6. Реагирование на запросы, поступающие от органов власти

Органами власти могут направляться мотивированные запросы у Оператора. Ответственным за реагирование на поступившие запросы является ответственный за организацию обработки ПДн.

6.1 Регистрация запросов, поступающих от органов власти

Первичная регистрация поступивших запросов от органов власти осуществляется в соответствии с правилами документооборота Оператора.

После первичной регистрации запросы передаются ответственному за организацию обработки ПДн. В его обязанности входит регистрация всех поступивших запросов в Журнале регистрации запросов органов власти в день их поступления. Ответственный за организацию обработки ПДн персональных данных является ответственным за ведение Журнала.

6.2 Виды запросов органов власти

У Оператора могут поступать следующие виды запросов от органов власти:

- запросы на предоставление информации о субъектах ПДн;
- запросы на совершение действий с ПДн (блокирование, уточнение, уничтожение).
- В запросе на предоставление информации о субъектах ПДн должно содержаться:

- наименование органа государственной власти;
- основание для предоставления информации;
- запрашиваемая информация;
- фамилия, имя, отчество лица, направившего запрос на получение информации;
- срок предоставления информации;
- вид, в котором должна предоставляться информация (бумажный, электронный носитель).
- В запросе на совершение действия с ПДн должно содержаться:
- наименование органа государственной власти;
- основание для выполнения действия с ПДн;
- действие, которое предписано выполнить (уточнение, блокирование, уничтожение);
- информация, в отношении которой необходимо выполнить действие;
- фамилия, имя, отчество лица, направившего запрос;
- срок исполнения.

Запросы на блокирование ПДн могут поступать у Оператора в случаях выявления недостоверных ПДн или неправомерных действий с ними.

Запросы на уточнение ПДн могут поступать у Оператора в случаях подтверждения фактов недостоверности обрабатываемых у Оператора ПДн. К запросам на уточнение ПДн должны прилагаться документы, подтверждающие, что ПДн, относящиеся к соответствующим субъектам, обрабатываемые у Оператора, являются неполными, устаревшими или недостоверными.

Запросы на уничтожение ПДн могут поступать у Оператора в случаях выявления неправомерных действий с ПДн и невозможности устранения допущенных нарушений.

6.3 Реагирование на запросы органов власти

Менеджер обработки ПДн отвечает за организацию и контроль предоставления информации по запросу или выполнения предписанных действий в течение семи рабочих дней с момента поступления запроса.

6.3.1 Реагирование на запросы на предоставление информации о субъектах ПДн

Для реагирования на запросы на предоставление информации о субъектах ПДн ответственный за организацию обработки ПДн оформляет служебную записку, в которой указывается информация, которую необходимо предоставить, а также срок предоставления информации и исполнитель.

Отправку ответа на поступивший запрос контролирует ответственный за организацию обработки ПДн. Ответ на запрос либо высылается заказным письмом, либо доставляется курьером.

В Журнале регистрации запросов органов власти ответственный за организацию обработки ПДн проставляет отметку об отправлении ответа на запрос.

Запросы, а также ответы на них должны храниться у Оператора в течение срока, установленного в соответствии с правилами внутреннего документооборота. Ответственным за хранение поступивших запросов и ответов на них является ответственный за организацию обработки ПДн.

6.3.2 Реагирование на запросы на совершение действий с ПДн

При получении запроса на совершение действий с ПДн ответственный за организацию обработки ПДн незамедлительно направляет служебную записку на блокирование, уточнение или уничтожение соответствующих ПДн Администратору безопасности ИСПДн.

Администратор безопасности ИСПДн обеспечивает немедленное выполнение требуемых действий в отношении ПДн субъектов ПДн, указанных в служебной записке, и сообщает об этом ответственный за организацию обработки ПДн.

Ответственный за организацию обработки ПДн подготавливает и направляет уведомление о произведенных действиях с ПДн в уполномоченный орган власти, направивший у Оператора запрос. Уведомление либо высылается заказным письмом, либо доставляется курьером.

В Журнале регистрации запросов органов власти Ответственный за организацию обработки ПДн проставляет отметку об исполнении требований запроса.

## 7. Пересмотр и внесение изменений

Пересмотр положений настоящего документа проводится в следующих случаях:

- на регулярной основе, но не реже одного раза в полгода;
- при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти РФ;
- по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности персональных данных.
- Ответственным за пересмотр настоящего Регламента является ответственный за организацию обработки ПДн.

Внесение изменений в настоящий Регламент производится на основании соответствующего приказа руководителя Оператора.

**Ж У Р Н А Л**

**учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля**

_____

(дата начала ведения Журнала)

БПОУ ВО «Череповецкий многопрофильный колледж»

(полное и (в случае, если имеется) сокращенное наименование, в том числе фирменное наименование юридического лица/фамилия, имя, отчество (в случае, если имеется) индивидуального предпринимателя)

г.Череповец ул. Гоголя,21

(адрес (место нахождения) постоянно действующего исполнительного органа, юридического лица/место жительства (место осуществления деятельности (если не совпадает с местом жительства) индивидуального предпринимателя)

ОГРН 1033500321470 , ИНН 3528011214

(государственный регистрационный номер записи о государственной регистрации юридического лица/индивидуального предпринимателя, идентификационный номер налогоплательщика (для индивидуального предпринимателя); номер реестровой записи и дата включения сведений в реестр субъектов малого или среднего предпринимательства (для субъектов малого или среднего предпринимательства))

Ответственное лицо: _____

(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала учета проверок)

_____

(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица, индивидуального предпринимателя)

Подпись: _____

**М.П.**

## Сведения о проводимых проверках

| № п/п | Тип сведений | Сведения о проверке |
|---|---|---|
| 1 | Дата начала и окончания проверки | |
| 2 | Общее время проведения проверки (для субъектов малого и среднего предпринимательства, в часах) | |

| | | |
|---|---|---|
| 3 | Наименование органа государственного контроля (надзора), наименование органа муниципального контроля | |
| 4 | Дата и номер распоряжения или приказа о проведении проверки | |
| 5 | Цель, задачи и предмет проверки | |
| 6 | Вид проверки (плановая или внеплановая) для плановой проверки – ссылка на ежегодный план проведения проверок для внеплановой проверки в отношении субъектов малого или среднего предпринимательства – дата и номер решения прокурора о согласовании проведения проверки | |
| 7 | Дата и номер акта, составленного по результатам проверки, дата его вручения представителю юридического лица, индивидуальному предпринимателю | |
| 8 | Выявленные нарушения обязательных требований (указываются содержание выявленного нарушения со ссылкой на положение нормативно-правового акта, которым установлено нарушенное требование, допустившее его лицо) | |
| 9 | Дата, номер и содержание выданного предписания об устранении выявленных нарушений | |
| 10 | Фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), проводящего (-их) проверку | |
| 11 | Фамилия, имя, отчество (в случае, если имеется), должности экспертов, представителей экспертных организаций, привлеченных к проведению проверки | |
| 12 | Подпись должностного лица (лиц), проводивших проверку | |

# ЖУРНАЛ

## регистрации запросов органов власти

| № п/п | Регистрационный номер | Дата поступления запроса | Наименование органа государственной власти | Краткое содержание запроса | Кому отправлено на исполнение | Срок исполнения (дата) | Отметка об исполнении или причина неисполнения |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Приложение № 13**

# ЖУРНАЛ ПРОВЕДЕНИЯ ИНСТРУКТАЖЕЙ ПОЛЬЗОВАТЕЛЕЙ

**ЖУРНАЛ**
**проведения инструктажей по информационной безопасности**

**Начат:**_____
**Окончен:**_____

| № п/п | Наименование ИСПДн | Дата проведения инструктажа | ФИО инструктируемого сотрудника | Краткое содержание инструктажа | Должность, ФИО, проводившего инструктаж | Подпись инструктирующего | Подпись инструктируемого |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |