АДМИНИСТРАЦИЯ
ГАЛИЧСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
КОСТРОМСКОЙ ОБЛАСТИ

Р А С П О Р Я Ж Е Н И Е

от « 24 » января 2017 года № 13-р

г. Галич

Об организации работы по защите персональных данных в администрации Галичского муниципального района Костромской области

Руководствуясь Федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлениями Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

1. Назначить ответственным должностным лицом за организацию обработки персональных данных и их безопасность в администрации Галичского муниципального района Костромской области – заведующего общим отделом Сахарову Юлию Николаевну
2. Назначить ответственного за обеспечение безопасности персональных данных в информационной системе - программиста муниципального казенного учреждения «Отраслевая служба» Галичского муниципального района Костромской области Шахова Юрия Анатольевича
3. Утвердить:
    1) Правила обработки персональных данных осуществляемой без средств автоматизации (Приложение № 1);
    2) Инструкцию по работе с обращениями субъектов персональных данных (Приложение № 2);
    3) Правила работы с обезличенными данными (Приложение № 3);
    4) Перечень информационных систем персональных данных (Приложение № 4);

5) Перечень категорий персональных данных обрабатываемых в администрации Галичского муниципального района Костромской области (Приложение № 5);

6) Перечень должностей служащих, замещение которых предусматривает обработку персональных данных (Приложение № 6);

7) Инструкцию ответственного за организацию обработки персональных данных (Приложение №7);

8)Типовое обязательство о соблюдении режима конфиденциальности персональных данных работников (Приложение № 8);

9)Типовую форму согласия на обработку персональных данных (Приложение № 9);

10) Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (Приложение № 10)

11)Порядок доступа сотрудников администрации Галичского муниципального района Костромской области в помещения, в которых ведется обработка персональных данных (Приложение № 11);

12)Инструкцию по пользованию информационной системой персональных данных (Приложение № 12);

13**)** Порядок резервирования данных и восстановления работоспособности информационной системы персональных данных (Приложение № 13);

14) Частная модель актуальных угроз и вероятного нарушителя информационной системы персональных данных администрации Галичского муниципального района (Приложение № 14);

15) Инструкцию администратора безопасности АИС (Приложение № 15)

4. Считать утратившим силу распоряжение администрации Галичского муниципального района Костромской области от 25 августа 2011 года № 300-р «О назначении О.Ю. Поваровой ответственным должностным лицом по работе с персональными данными сотрудников администрации Галичского муниципального района»

5. Контроль за исполнением настоящего распоряжения оставляю за собой.

6. Настоящее распоряжение вступает в силу со дня его подписания.

Глава
муниципального района А.Н. Потехин

Приложение №1
Утверждено
Распоряжением администрации
Галичского муниципального района
Костромской области
от « 24 » января 2017 года № 13-р

ПРАВИЛА
обработки персональных данных,
осуществляемой без использования средств автоматизации

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие Правила разработаны на основании требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 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», Положения об обработке персональных данных в администрации Галичского муниципального района Костромской области и иных нормативных документов, регламентирующих сферу документооборота в органах исполнительной власти.

Неавтоматизированной обработкой персональных данных (без применения средств автоматизации) считается обработка персональных данных без использования средств вычислительной техники. При этом обработка персональных данных не может быть признана исключительно автоматизированной только на том основании, что они содержатся в информационной системе либо были извлечены из нее.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть ознакомлены под роспись о факте обработки ими персональных данных без использования средств автоматизации, проинформированы о категориях обрабатываемых персональных данных, о правилах осуществления такой обработки, а также о некоторых особенностях, установленных в администрации Галичского муниципального района Костромской области

Места хранения материальных носителей персональных данных определяются в ходе обследования и изучения системы обработки персональных данных исходя из анализа используемых технологических процессов обработки, расположения помещений и установленного режима их охраны, с учетом необходимости дооборудования этих мест техническими и режимными мерами.

Документы, содержащие персональные данные, должны храниться в условиях, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ.

Круг лиц, допущенных к обработке персональных данных без использования средств автоматизации, а также места хранения материальных носителей информации определяются и утверждаются Распоряжением администрации Галичского муниципального района Костромской области и отражаются во внутренних нормативных документах (Перечень должностей, Порядок доступа и т.п.).

2. ОБРАБОТКА и ХРАНЕНИЕ ДОКУМЕНТОВ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

При неавтоматизированной обработке персональных данных сотрудники обязаны соблюдать следующие правила:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- при подготовке итоговых, аналитических и других документов персональные данные должны обособляться от иной информации, в частности, путём фиксации их на отдельных бумажных носителях (приложениях), в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, группируются (формируются) в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

Нельзя хранить в одном месте персональные данные, цели обработки которых различны. Формирование дел осуществляется по одному из целевых признаков обработки персональных данных. Например, личное дело сотрудника, дело с графиками отпусков, командировки сотрудников, расчет заработной платы и т.п.

Дела, законченные производством либо по достижению целей обработки персональных данных закрываются (в соответствии с требованиями правил делопроизводства) и передаются на хранение в архив организации либо, при необходимости частого обращения к материалам, хранятся в подразделении.

Режим хранения и порядок доступа к оконченным производством делам определяется внутренними нормативными документами, в которых описывается порядок доступа, перечень должностных лиц и ответственность за нарушение режима доступа.

3. ИСПОЛЬЗОВАНИЕ ТИПОВЫХ ФОРМ

Обработка документов, предполагающая наличие в них информации персонального характера либо иных данных, относящихся к субъекту ПДн, в администрации Галичского муниципального района Костромской области осуществляется с использованием Типовых форм документов.

В соответствии с требованиями законодательства при использовании типовых форм документов (анкет, бланков и т.д.) в администрации Галичского муниципального района соблюдаться следующие условия:
а) типовая форма должна содержать в себе следующие сведения:
- цель неавтоматизированной обработки персональных данных;
- наименование и адрес оператора ПДн;
- фамилию, имя, отчество и адрес субъекта персональных данных;
- источник получения персональных данных;
- сроки обработки персональных данных;
- перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
- общее описание используемых оператором способов обработки персональных данных.

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных;
в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные содержатся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4. ХРАНЕНИЕ И УНИЧТОЖЕНИЕ ДОКУМЕНТОВ

Хранение персональных данных в подразделениях и архиве администрации осуществляется не дольше, чем этого требуют цели обработки персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки либо в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Решение об уничтожении документов либо их обезличивании в целях дальнейшего использования в организации принимает созданная в администрации Галичского муниципального района Костромской области экспертная комиссия.

Состав экспертной комиссии определяется структурой конфиденциального делопроизводства в исполнительном органе и назначается распоряжением администрацией Галичского муниципального района Костромской области.

Уничтожение документов, содержащих персональные данные, цель обработки которых достигнута, производится на основании решения экспертной комиссии. По результатам работы комиссии оформляются акты об уничтожении документов (Приложение 1, 2).

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Приложение №1
к Правилам обработки персональных данных,
осуществляемой без использования средств автоматизации

УТВЕРЖДАЮ

Глава администрации Галичского
муниципального района Костромской
области

_____

«___» _____ 201_ г.

АКТ
о выделении документов на уничтожение

«__» _____ 201__ г. г. Галич

Комиссия в составе:
председатель комиссии:
члены комиссии:
секретарь комиссии:

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

1. _____
2. _____

…

Всего: _____ наименований.

Председатель комиссии: _____

Члены комиссии: _____

_____

_____

Приложение №2
к Правилам обработки персональных данных,
осуществляемой без использования средств автоматизации

УТВЕРЖДАЮ

Глава администрации Галичского
муниципального района Костромской
области

_____

«___» _____ 201_ г.

АКТ
об уничтожении документов, срок хранения которых истек

«__» _____ 201__ г. г. Галич

Комиссия в составе:
председатель комиссии:
члены комиссии:
секретарь комиссии:

составила настоящий акт в том, что согласно описи, утвержденной актом от «__» _____ 201__ года, документы, срок хранения которых истек,были уничтожены путем _____ в присутствии членов комиссии.

Председатель комиссии: _____

Члены комиссии: _____

_____

_____

Приложение №2
Утверждено
распоряжением администрации
Галичского муниципального района
Костромской области
от «24» января 2017 года № 13-р

ИНСТРУКЦИЯ
по работе с обращениями субъектов персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана на основании требований Федеральных законов РФ от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и от 27.07.2006 г. № 152-ФЗ «О персональных данных» и определяет порядок и сроки обработки обращений субъектов персональных данных и граждан, обратившихся по вопросам, входящим в сферу деятельности администрации Галичского муниципального района Костромской области.

1.2. К рассмотрению обращений субъектов ПДн и граждан в соответствии с должностными инструкциями допускаются лица, имеющие по своим должностным обязанностям доступ к обработке персональных данных.

1.3. В соответствии со ст. 14 ФЗ РФ от 27.07.2006 г. № 152-ФЗ субъект персональных данных имеет право обратиться к Оператору персональных данных на получение информации, касающейся обработки его персональных данных. Требуемые сведения предоставляются субъекту персональных данных при личном обращении или по его письменному запросу (Приложение 1).

1.4. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных (или его полномочного представителя), сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных (или его полномочного представителя).

1.5. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Оператор обязан в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных сведений, подтверждающих что эти сведения являются неполными, неточными или неактуальными, внести необходимые изменения (в том числе уничтожить) в существующие базы данных, в том числе, на материальные носители, а затем уведомить субъекта персональных данных о внесенных изменениях и предпринятых мерах.

Кроме того, при необходимости, принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были или могли быть переданы в соответствии с требованиями Федерального законодательства или существующими договоренностями.

1.6. При отзыве субъектом согласия на обработку его персональных данных Оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей их обработки, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва (при условии, что Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральным законодательством) (Приложение 2).

2. ПОРЯДОК РАССМОТРЕНИЯ ОБРАЩЕНИЙ СУБЪЕКТОВ ПДн

2.1. Поступившее обращение субъекта персональных данных (письменный запрос или устное обращение) подлежит обязательной регистрации в Журнале регистрации обращений граждан (Приложение 3) и рассмотрению в течение трех дней с момента поступления.

2.2. Руководитель организации при получении запроса от субъекта персональных данных в своей резолюции назначает лицо, ответственное за рассмотрение запроса и подготовку ответа на поступившее обращение.

2.3. При подготовке письменного ответа ответственный сотрудник от лица Оператора персональных данных обязан:

2.3.1. Сообщить заявителю информацию о порядке и сроках рассмотрения обращения, подтвердив факт обработки персональных данных Оператором;

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

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

2.3.3. Подготовить в течение тридцати дней с даты регистрации запроса письменный ответ и направить его субъекту персональных данных.

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

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

3.ПОРЯДОК РАССМОТРЕНИЯ ОБРАЩЕНИЯ ГРАЖДАН

3.1.Порядок рассмотрения обращений граждан по вопросам входящим в сферу деятельности администрации Галичского муниципального района Костромской области (выделение земельных участков, вопросы градостроительства и архитектуры, жалобы и обращения населения) регламентируется Федеральным законом РФ от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и внутренними нормативными документами.

3.2.Учёт поступивших обращений ведется в Журнале регистрации обращений граждан установленной формы (Приложение 3) заведующим общим отделом администрации Галичского муниципального района Костромской области.

3.3.Рассмотрение обращений граждан, поступивших по каналам электронных коммуникаций (эл. почта, эл.бланк размещаемый на сайте, форум и т.п.) осуществляется в соответствии с требованиями федерального законодательства .

4.ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ

4.1.Нарушение установленного законодательством Российской Федерации порядка рассмотрения обращений граждан влечёт наложение административного штрафа в размере от пяти до десяти тысяч рублей (ст. 5.59 Кодекса Российской Федерации об административных правонарушениях).

4.2.К должностным лицам нарушившим порядок рассмотрения обращений могут применятся иные меры дисциплинарного воздействия в соответствии с трудовым законодательством.

Приложение: 1. Форма Запроса на получение информации об обработке ПДн, на 1 л.;
2. Форма Заявления на отзыв ПДн, на 1 л.;
3. Форма Журнала регистрации обращений граждан.

Приложение № 1
К инструкции по работе с обращениями
субъектов персональных данных

_____
Наименование (Ф.И.О.) оператора

_____
Адрес оператора

_____
Ф.И.О. субъекта персональных данных

_____
Адрес, где зарегистрирован субъект персональных данных

_____
Номер основного документа, удостоверяющего личность

_____
Дата выдачи указанного документа

_____
Наименование органа, выдавшего документ

ЗАПРОС

на получение информации об обработке ПДн

Ранее я предоставлял согласие на обработку моих персональных данных, включая согласие на право обработки указанных персональных данных в целях исполнения требований федерального законодательства и использования в служебной деятельности.

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

1) Какие персональные данные в отношении меня имеются в распоряжении администрации Галичского муниципального района Костромской области, из каких источников и как они были получены;

2) Каким третьим лицам (физическим или юридическим лицам, государственным органам или органам местного самоуправления и т.п.) передавались мои персональные данные, какие именно персональные данные передавались и когда.

Указанную информацию прошу предоставить мне в письменной форме.

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

«___» _____ 201__ г.

_____ _____
(подпись) (расшифровка подписи)

Приложение 2
к Инструкции по работе с обращениями
субъектов персональных данных

_____
Наименование (Ф.И.О.) оператора

_____
Адрес оператора

_____
Ф.И.О. субъекта персональных данных

_____
Адрес, где зарегистрирован субъект персональных данных

_____
Номер основного документа, удостоверяющего личность

_____
Дата выдачи указанного документа

_____
Наименование органа, выдавшего документ

ЗАЯВЛЕНИЕ
(отзыв согласия на обработку персональных данных)

На основании п. 2 ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», отзываю ранее данное мной согласие на обработку персональных данных.
В случае, если согласие на обработку персональных данных давалось мной неоднократно, настоящим я отзываю все ранее данные мной согласия на обработку персональных данных.
В соответствии с п. 5 ст. 21 Федерального закона «О персональных данных», в случае отзыва субъектом персональных данных согласия на их обработку, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва.
Я уведомлен, что в, случае отзыва согласия на обработку персональных данных, администрации Галичского муниципального района Костромской области вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2÷11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
Уведомление о прекращении обработки и уничтожении моих персональных данных прошу предоставить в письменной форме.
"__" _____ 20__ г.

(подпись)	(расшифровка подписи)

Приложение 3
к Инструкции по работе с обращениями
субъектов персональных данных

Регистрационный номер, дата регистрации	**Корреспондент/ субъект ПДн**	**Краткое содержание обращения**	**Откуда поступило**	**Резолюция должностного лица/ дата**	**Ответственный исполнитель, роспись**	**Результат рассмотрения**	**Дата, номер исходящего документа**

Приложение № 3
Утверждено
распоряжением администрации
Галичского муниципального района
Костромкой области
от « 24 »января 2017 года № _13-р

ПРАВИЛА

работы с обезличенными данными

Настоящие Правила разработаны на основании требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211, приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 № 996, Положения об обработке персональных данных в администрации Галичского муниципального района Костромской области.

В целях снижения уровня конфиденциальности обрабатываемой информации ограниченного распространения, в том числе сведений персонального характера, при необходимости вызванной отсутствием возможности применения адекватных мер защиты указанной информации либо снижения актуальности угроз безопасности информации, циркулируемой в ИСПДн администрации Галичского муниципального района Костромской области, возможно применение порядка обезличивания персональных данных в соответствиями с рекомендациями, изложенными в приказе Роскомнадзора от 05.09.2013 № 996 .

Под обезличиванием персональных данных понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Перечень должностей служащих администрации Галичского муниципального района Костромской области, замещение которых предусматривает осуществление обработки персональных данных и имеющих право их обезличивания, утверждается распоряжением администрации Галичского муниципального района Костромской области.

Указанные лица, при вступлении в должность информируются под роспись в листе ознакомления о факте обработки и категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления обезличивания персональных данных, принятых в администрации Галичского муниципального района Костромской области.

Обрабатываемые персональные данные по достижении целей обработки или в случае утраты необходимости в достижении этих целей подлежат уничтожению либо обезличиванию и дальнейшему хранению и использованию, если иное не предусмотрено требованиями федерального законодательства.

При обезличивании персональных данных должны обеспечиваться возможность их дальнейшей обработки при соблюдении защиты от несанкционированного к ним доступа. После обезличивания персональные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых данных:

- 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 персональных данных и получения ответов в одинаковой семантической форме);
- семантическая целостность (сохранение значений персональных данных при их обезличивании);
- применимость (возможность решения задач обработки персональных данных, стоящих перед оператором, осуществляющим обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, 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 данных, полученных в результате обезличивания, без применения дополнительной информации).

Методы обезличивания персональных данных используемые при проведении операций над ними должны отвечать следующим характеристикам, определяющим возможность обеспечения заданных свойств обезличенных данных:

- обратимость (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных 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 персональных данных);

- возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием информации других операторов);

- совместимость (возможность интеграции персональных данных, 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).

При обработке персональных данных в процессе их обезличивания в соответствии с рекомендациями Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций могут использоваться следующие методы обезличивания:

- метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

- метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

Особенности каждого метода обезличивания и способы их реализации изложены в приказе Роскомнадзора от 05.09.2013 г. № 996.

Выбор оптимального метода осуществляется оператором персональных данных с учетом особенностей обработки ПДн в конкретных подразделениях администрации Галичского муниципального района Костромской области, характеристик ИСПДн, используемого прикладного программного обеспечения и средств технической защиты информации.

Приложение № 4
Утверждено

распоряжением администрации
Галичского муниципального
района Костромской области
от « 24» января 2017 года № 13-р

Перечень информационных систем персональных данных

1. АРМ Обращения граждан

2. Сайт администрации Галичского муниципального района

3. АРМ Единой сети обращения граждан

Приложение № 5

Утверждено

распоряжением администрации
Галичского муниципального района
Костромской области
от « 24» января 2017 года_ № _13-р

ПЕРЕЧЕНЬ

категорий персональных данных, обрабатываемых в администрации Галичского муниципального района Костромской области

- фамилия, имя, отчество, дата и место рождения, гражданство;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- владение иностранными языками и языками народов Российской Федерации;
- образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);
- послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и т.п.);
- сведения о трудовом и общем стаже;
- данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты труда, категории персонала, условия труда, продолжительность рабочей недели, система оплаты труда);
- прием на работу, перемещение по должности, увольнение;
- отпуска, периоды нетрудоспособности, командировки;
- классный чин федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатический ранг, воинское и (или) специальное звание, классный чин правоохранительной службы (кем и когда присвоены);
- аттестация;
- повышении квалификации;
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
- места рождения, места работы, паспорт (свидетельство о рождении), домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
- фамилии, имена, отчества, даты рождения, места рождения, места работы, паспорт и домашние адреса бывших мужей (жен);
- пребывание за границей (когда, где, с какой целью);
- близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей);
- адрес регистрации и фактического проживания;
- дата регистрации по месту жительства;
- паспорт (серия, номер, кем и когда выдан);

- паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);
- номер мобильного телефона или домашнего телефона;
- отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- идентификационный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- наличие (отсутствие) судимости;
- допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер и дата);
- наличие (отсутствие) заболевания, препятствующего поступлению на муниципальную службу или ее прохождению, подтвержденного заключением медицинского учреждения;
- результаты обязательных медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования;
- сведения о доходах, расходах, имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера членов семьи;
- сведения о последнем месте государственной или муниципальной службы.
- сведения об изображении лица.
- сведения об адресатах сайтов и (или) страницах сайтов в информационно – телекоммуникационной сети «Интернет» на которых муниципальными служащими, гражданами Российской Федерации, претендующими на должности муниципальной службы размещалась общедоступная информация, а также данные, позволяющие его идентифицировать

Приложение № 6
Утверждено
распоряжением администрации
Галичского муниципального района
Костромской области
от «24» января 2017 года № 13-р

ПЕРЕЧЕНЬ
должностей служащих, замещение которых
предусматривает обработку персональных данных

№ п/п	Должность	Состав персональных данных
1	Глава администрации Галичского муниципального района Костромской области	Персональные данные работников и контрагентов
2	Заместители главы администрации муниципального района Костромской области	Персональные данные работников и контрагентов
3	Управляющий делами администрации муниципального района Костромской области	Персональные данные работников и контрагентов
4	Помощнику главы муниципального района по мобилизационной работе, гражданской обороне и чрезвычайным ситуациям	Персональные данные работников и контрагентов
Общий отдел (обработка и хранение)		
5	Заведующий отделом	Персональные данные работников и контрагентов (обращения граждан)
6	Заместитель заведующего общим отделом, юрист администрации муниципального района(ответственный секретарь административной комиссии)	Персональные данные работников и контрагентов
7	главный специалист общего отдела администрации муниципального района	Персональные данные работников и контрагентов
Отдел по делам архивов		
8	Заведующий отделом	Персональные данные сотрудников отдела и контрагентов
9	Архивариус	Персональные данные контрагентов
Сектор ЖКХ		
10	Заведующий отделом	Персональные данные сотрудников сектора и контрагентов
Сектор архитектуры		
11	Заведующий отделом	Персональные данные сотрудников сектора и контрагентов
12	Главный специалист	Персональные данные контрагентов
Отдел по экономике и экономическим реформам		
13	Заведующий отделом	Персональные данные сотрудников отдела и контрагентов
14	Главный специалист	Персональные данные контрагентов
Сектор природных ресурсов и охраны труда администрации муниципального района		
15	Заведующий сектором	Персональные данные сотрудников сектора и контрагентов
16	Главный специалист по труду	Персональные данные контрагентов
Сектор по внутреннему муниципальному финансовому контролю		

№ п/п	Должность	Состав персональных данных
17	Заведующий сектором по внутреннему муниципальному финансовому контролю	Персональные данные работников и контрагентов
Комиссия по делам несовершеннолетних		
18	Ведущий специалист, ответственный секретарь комиссии по делам несовершеннолетних и защите их прав	Персональные данные контрагентов

Приложение № 7
Утверждено
распоряжением администрации
Галичского муниципального
района Костромской области
от « 24» января 2017 года № 13-р

ИНСТРУКЦИЯ

ответственного за организацию обработки персональных данных

Настоящая Инструкция разработана на основании п. 1 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии требованиями Положения об обработке персональных данных в администрации Галичского муниципального района Костромской области и иных нормативных документов.

Инструкция определяет права и обязанности сотрудника, ответственного за организацию обработки персональных данных при обработке их Оператором ПДн.

Лицо, ответственное за организацию обработки персональных данных назначается распоряжением администрации Галичского муниципального района Костромской области из числа наиболее опытных и подготовленных сотрудников администрации.

Ответственный за организацию обработки персональных данных сотрудник действует в соответствии с положениями статьи 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», разработанными организационно-распорядительными и иными нормативными документами, регламентирующими обработку в подразделениях администрации персональных данных.

В своей деятельности ответственный сотрудник руководствуется также указаниями главы администрации Галичского муниципального района Костромской области по указанным вопросам и подчиняется ему.

В соответствии с должностными обязанностями ответственный за организацию обработки персональных данных сотрудник обязан:

- изучить и знать законодательство Российской Федерации в области защиты персональных данных;
- активно участвовать в разработке документов, определяющих политику в отношении обработки персональных данных, локальных актов, устанавливающих процедуры, направленные обеспечение безопасности ПДн, на предотвращение и выявление нарушений безопасной обработки ПДн, устранение последствий таких нарушений, а также поддержание этих документов в актуальном состоянии;
- уведомлять уполномоченный орган по защите прав субъектов персональных данных об изменении сведений, касающихся обработки персональных данных в администрации Галичского муниципального района Костромской области либо в случае прекращения таковой

обработки в течение десяти рабочих дней с момента возникновения изменений;
- постоянно совершенствовать комплекс правовых, режимных, технических мер по обеспечению безопасной обработки персональных данных;
- осуществлять внутренний контроль соответствия обработки персональных данных требованиям федерального законодательства, организационно-распорядительных документов администрации в отношении обработки персональных данных;
- оценивать вред, который может быть причинен субъектам персональных данных, в случае нарушения требований к защите персональных данных, либо соотношение указанного вреда и принимаемых мер, направленных на обеспечение снижения угроз безопасности ПДн;
- своевременно доводить до сведения сотрудников администрации требования положений законодательства Российской Федерации и локальных нормативных актов по вопросам обработки персональных данных и требований к защите персональных данных;
- осуществлять внутренний контроль соблюдения Оператором ПДн и его сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к местам хранения документов, технической защите персональных данных;
- организовать приём и обработку обращений и запросов субъектов персональных данных или их законных представителей, а также осуществлять контроль приема и обработки таких обращений и запросов в администрации Галичского муниципального района Костромской области.

Ответственный за организацию обработки персональных данных имеет право:
- получать от сотрудников и руководителей структурных подразделений администрации Галичского муниципального района Костромской области информацию об изменении условий, касающихся обработки персональных данных;
- проверять деятельность сотрудников и структурных подразделений, осуществляющих обработку ПДн, на соответствие требованиям Положений Оператора ПДн в сфере обработки персональных данных;
- вносить на рассмотрение главы Галичского муниципального района Костромской области предложения по улучшению методов обработки и защиты персональных данных в подразделениях администрации;
- подавать заявки главе администрации Галичского муниципального района Костромской области о направлении его или иных сотрудников администрации на обучающие курсы по вопросам защиты конфиденциальной информации и обработки персональных данных.

Приложение № 8
Утверждено
распоряжением администрации Галичского
муниципального района Костромской области
от « 24» января 2017 года № 13-р

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО О СОБЛЮДЕНИИ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

Я, _____,
занимая муниципальную должность_____
в период трудовых отношений с администрацией Галичского муниципального района Костромской области (далее Работодатель) и после их окончания обязуюсь:

1. Не разглашать и не передавать третьим лицам и не раскрывать публично сведения, составляющие персональные данные работников, которые мне будут доверены или станут известны по работе.

2. Выполнять относящиеся ко мне требования «Положения об обработке персональных данных в администрации Галичского муниципального района Костромской области», постановлений, распоряжений и инструкций и других локальных нормативных актов по обеспечению режима конфиденциальности персональных данных работников и соблюдению правил их обработки.

3. В случае попытки посторонних лиц получить от меня сведения, составляющие персональные данные работника, немедленно сообщить_____
_____.

4. В случае моего увольнения все носители, содержащие персональные данные работников (документы, копии документов, дискеты, диски, магнитные ленты, распечатки на принтерах, черновики, кино- и фотонегативы и позитивы и пр.), которые находились в моем распоряжении в связи с выполнением мною трудовых обязанностей во время работы у Работодателя, передать _____ ___
_____.

5. Об утрате или недостаче документов или иных носителей, содержащих персональные данные работников, удостоверений, пропусков, сейфов (металлических шкафов), хранилищ, личных печатей и о других фактах, которые могут привести к разглашению персональных данных работников, а также о причинах и условиях возможной утечки сведений немедленно сообщить _____ ___
_____.

Я ознакомлен под роспись с Положением о работе с персональными данными, постановлениями, распоряжениями, инструкциями и другими локальными нормативными актами по соблюдению режима конфиденциальности персональных данных работников и соблюдению правил их обработки.

Мне известно, что нарушение мною обязанностей по охране персональных данных работников может повлечь дисциплинарную, гражданско-правовую, уголовную и иную ответственность в соответствии с законодательством РФ.

«_____»_____20___г.

_____	_____	_____
Должность	подпись	Ф.И.О.

Приложение № 9
Утверждено
распоряжением администрации
Галичского муниципального района
Костромской области
от « 24 » января 2017 года № 13-р

ТИПОВАЯ ФОРМА
согласия на обработку персональных данных

г. Галич «___» _____ 20___ г.

Я, _____ ,
(Фамилия, имя, отчество)

зарегистрированный(ая) по адресу _____

_____ ,

паспорт серия _____ № _____, выдан _____, _____
(дата) (кем выдан)

_____ ,

свободно, своей волей и в своем интересе даю согласие администрации Галичского муниципального района Костромской области, зарегистрированной по адресу: 157201, г. Галич, пл. Революции, д. 23 «а» (далее Оператор) на сбор, предоставление, обработку (автоматизированную и без использования средств автоматизации) передачу, уничтожение, удаление моих персональных данных в целях содействия мне в обеспечении кадрового учета и установленных законодательством условий работы (гарантий и компенсаций), обеспечения моей личной безопасности, обучении и должностном росте, осуществления контроля количества и качества выполняемой работы, а также в целях систематизации производственной деятельности, организации функционального взаимодействия между подразделениями и обеспечения сохранности имущества Оператора, а именно:

- использовать нижеперечисленные данные для формирования кадровых документов и для выполнения Оператором всех требований трудового, налогового, страхового, пенсионного и иного федерального законодательства;

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

- фамилия, имя, отчество, дата и место рождения, гражданство;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- владение иностранными языками и языками народов Российской Федерации;
- образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);
- послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и т.п.);
- сведения о трудовом и общем стаже;
- данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты труда, категории персонала, условия труда, продолжительность рабочей недели, система оплаты труда);
- прием на работу, перемещение по должности, увольнение;
- отпуска, периоды нетрудоспособности, командировки;
- классный чин федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатический ранг,

воинское и (или) специальное звание, классный чин правоохранительной службы (кем и когда присвоены);
- аттестация;
- повышении квалификации;
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
- места рождения, места работы, паспорт (свидетельство о рождении), домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
- фамилии, имена, отчества, даты рождения, места рождения, места работы, паспорт и домашние адреса бывших мужей (жен);
- пребывание за границей (когда, где, с какой целью);
- близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей);
- адрес регистрации и фактического проживания;
- дата регистрации по месту жительства;
- паспорт (серия, номер, кем и когда выдан);
- паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);
- номер мобильного телефона или домашнего телефона;
- отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- идентификационный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- наличие (отсутствие) судимости;
- допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер и дата);
- наличие (отсутствие) заболевания, препятствующего поступлению на муниципальную службу или ее прохождению, подтвержденного заключением медицинского учреждения;
- результаты обязательных медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования;
- сведения о доходах, расходах, имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера членов семьи;
- сведения о последнем месте государственной или муниципальной службы.
- сведения об изображении лица.
- сведения об адресатах сайтов и (или) страницах сайтов в информационно – телекоммуникационной сети «Интернет» на которых муниципальными служащими, гражданами Российской Федерации, претендующими на должности муниципальной службы размещалась общедоступная информация, а также данные, позволяющие его идентифицировать

Я ознакомлен(а), что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока муниципальной службы (работы);

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления;

3) в случае отзыва согласия на обработку персональных данных администрация Галичского муниципального района Костромской области вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4) после увольнения с муниципальной службы (прекращения трудовых отношений) персональные данные хранятся в администрации Галичского муниципального района Костромской области в течение срока хранения документов, предусмотренных действующим законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на администрацию Галичского муниципального района Костромской области функций, полномочий и обязанностей.

Дата начала обработки персональных данных: _____

(число, месяц, год)

_____

(подпись)

Приложение № 10
Утверждено
распоряжением администрации
Галичского муниципального района
Костромской области
от « 24» января 2017 года № 13-р

ТИПОВАЯ ФОРМА
разъяснения субъекту персональных данных юридических
последствий отказа предоставить свои персональные данные

Уважаемый (-ая),_____!
(инициалы субъекта персональных данных)

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена _____
(реквизиты и наименование нормативных правовых актов)
_____
_____

В случае отказа Вами предоставить свои персональные данные, оператор не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям
_____
_____
_____
(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающие его права, свободы и законные интересы)

В соответствии с законодательством в области персональных данных Вы имеете право:

на получение сведений об операторе, о месте его нахождения, о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными;

требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;

на обжалование действия или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

_____ _____
(дата) (фамилия, инициалы и подпись сотрудника оператора)

Приложение № 11

Утверждено

Распоряжением администрации

Галичского муниципального района

Костромской области

от «24» января 2017 года № 13-р

ПОРЯДОК

доступа сотрудников администрации Галичского муниципального района Костромской области в помещения, в которых ведется обработка персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Порядок доступа сотрудников администрации Галичского муниципального района в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 01.11.2012 № 1119 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», в целях обеспечения защиты конфиденциальной информации, обрабатываемой в администрации Галичского муниципального района и исключения фактов неконтролируемого пребывания в них посторонних лиц. Настоящим документом определяются границы контролируемой зоны, порядок доступа в неё работников и посетителей, а также правила обработки и хранения документов, содержащих персональные данные, и материальных носителей персональных данных.

Порядок устанавливает единые требования к обеспечению сохранности технических средств и персональных данных.

2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Неавтоматизированная обработка персональных данных – обработка персональных данных без использования средств вычислительной техники.

Технические средства – серверные станции, персональные компьютеры и ноутбуки, настроенные на доступ к программному обеспечению, хранящему и обрабатывающему персональные данные сотрудников и контрагентов.

Контролируемая зона (КЗ) – территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

Постоянная контролируемая зона – это зона, границы которой устанавливаются на длительный срок.

Временная контролируемая зона – это зона, устанавливаемая для проведения закрытых мероприятий разового характера.

3. ГРАНИЦЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

3.1. К границе контролируемой зоны, в которой ведётся обработка персональных данных с использованием средств автоматизации и без таковых относят помещения, расположенные по адресу: г. Галич, пл Революции, д. 23 а

3.2. В помещениях, определенных в соответствии с функциональными обязанностями должностных лиц, обрабатывающих персональные данные, приняты организационные меры по ограничению несанкционированного доступа к информации ограниченного распространения.

3.3. Контроль доступа на территорию контролируемой зоны объектов администрации Галичского муниципального района осуществляется сотрудниками администрации муниципального района в соответствии с внутренними должностными инструкциями.

3.4. При необходимости, в целях обеспечения защиты конфиденциальной информации за пределами постоянной контролируемой зоны и обеспечения санкционированного (контролируемого) пребывания в ней посторонних лиц, в администрации может быть организована временная контролируемая зона.

Границы временной контролируемой зоны определяются, исходя из целей планируемого мероприятия, на основании принятых нормативных документов и выполнения режимных мер.

4. ПОРЯДОК ДОСТУПА В ОХРАНЯЕМЫЕ ПОМЕЩЕНИЯ

4.1. В целях обеспечения сохранности технических средств и материальных носителей помещения, в которых осуществляется обработка персональных данных, оборудованы охранной и пожарной сигнализацией, а также прочными дверями с механическими замками.

Ключи от замков передаются и находятся на ответственном хранении у сотрудников подразделений, работающих в служебных помещениях, а также у сотрудника единой диспетчерской службы, уполномоченного хранить резервные ключи от замков всех помещений.

4.2. Сотрудникам отделов, не работающим непосредственно в данном помещении, доступ в него разрешен только в присутствии сотрудников отдела, работающих в данном помещении.

4.3. В случае, если в течение рабочего дня сотрудник отдела уходит из помещения (не остается других сотрудников этого отдела), он обязан проследить, чтобы в помещении не было посторонних лиц (в том числе сотрудников других отделов) и закрыть помещение на замок.

4.4. По окончании рабочего дня помещения, в которых осуществляется обработка персональных данных, запираются, ключи от них сдаются сотруднику единой диспетчерской службы .

4.5. Нахождение клиентов (посторонних лиц) в помещениях, где осуществляется обработка персональных данных, допускается только в присутствии сотрудников отдела, непосредственно работающих в данном помещении, с соблюдением установленных правил ограничения доступа к обрабатываемой информации.

5. ПОРЯДОК ПЕРЕДАЧИ ПОМЕЩЕНИЙ ПОД ОХРАНУ

5.1. Закрытие помещений, в которых осуществляется обработка персональных данных, производится ответственными работниками по окончании рабочего времени, проведении в нём (при необходимости) влажной уборки и осмотра его в целях выявления и устранения возможных нарушений (не выключенное оборудование, неубранные документы, незапертые хранилища, окна и т.п.), в том числе правил противопожарной безопасности (отключение электрических приборов, освещения и т.п.).

5.2. После осмотра помещения, выявления и устранения возможных недостатков, ответственный сотрудник закрывает помещение

С указанного момента помещение считается принятым под охрану.

5.3. В случаях, если за период рабочего времени произошли изменения, вследствие которых может потребоваться изменение характера охраны, ответственный работник сообщает об этом дежурному сотруднику единой диспетчерской службы.

В случае значительных изменений в режиме охраны производится корректировка руководящих документов.

5.4. При входе в помещения, в которых осуществляется обработка персональных данных, ответственный работник производит внешний осмотр на предмет выявления возможных видимых недостатков (отсутствие техники, оборудования) и нарушений (повреждение целостности дверей и т.п.). При отсутствии признаков нарушения целостности охраняемого объекта или причинения ущерба объект считается снятым с охраны.

5.5. В случае обнаружения повреждения (нарушения целостности) внешней двери помещения, в котором осуществляется обработка персональных данных, или при обнаружении попытки проникновения в него ответственный работник незамедлительно сообщает о случившемся руководителю или лицу, его замещающему, после чего должностное лицо принимает необходимые меры по локализации нарушения:

- вызывает сотрудников полиции по номеру 02 или мобильному 112 для принятия мер реагирования;
- в течение двенадцати часов с момента выявления факта нанесения ущерба организует проведение инвентаризации имущества и подтверждение размера ущерба соответствующими документами бухгалтерского учета с расчетом его стоимости;
- обеспечивает сохранность пострадавшего имущества в том виде, в каком оно находилось после нанесения ущерба.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ УСТАНОВЛЕННОГО ПОРЯДКА

6.1. Контроль выполнения требований настоящего Порядка возлагается на заведующих отделов секторов, являющихся пользователями информационной системы персональных данных администрации Галичского муниципального района. 6.2. Работник, нарушивший требования данного Порядка, может быть привлечен к дисциплинарной или правовой ответственности в соответствии с законодательством РФ и трудовым договором, если проступок не содержит состава преступления.

Приложение № 12
Утверждено

Распоряжением администрации
Галичского муниципального района
Костромской области
от « 24 » января 2017 года № 13-р

ИНСТРУКЦИЯ
по пользованию информационной системой
персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция определяет основные принципы безопасного использования информационной системы сотрудниками администрации Галичского муниципального района Костромской области в соответствии с требованиями Федеральных законов от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативных актов.

2. ОСНОВНЫЕ ПОНЯТИЯ

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

Информационные ресурсы – документы и массивы документов в информационных системах.

Пользователь – сотрудник, использующий для своих должностных обязанностей средства электронной вычислительной техники.

Автоматизированное рабочее место пользователя (АРМ) – персональный компьютер с предустановленным программным обеспечением.

Персональный компьютер (ПК) — компьютер, предназначенный для эксплуатации одним пользователем, то есть для личного использования.

3. ОБЩИЕ ПРАВИЛА РАБОТЫ НА АРМ

Для исполнения служебных обязанностей, Пользователю на период работы в администрации Галичского муниципального района Костромской области предоставляется автоматизированное рабочее место. В процессе эксплуатации ПК Пользователям запрещается:

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

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

3.3. Отключать антивирусное программное обеспечение, а также предусмотренные средства защиты;

3.4. Подключать к ПК неучтенные внешние запоминающие устройства (активное сетевое оборудование, незарегистрированные компьютеры и т.д.), если это не связано с исполнением должностных обязанностей сотрудника;
3.5. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты для организации несанкционированного доступа к информационным ресурсам компании. При обнаружении такого рода ошибок необходимо информировать своего непосредственного руководителя обо всех фактах нарушения данной Инструкции.
3.6. Осуществлять действия направленные на преодоление систем безопасности, получение несанкционированного доступа к ресурсам информационной сети и перехват информации, циркулирующей в ИС;
3.7. Оставлять переносные компьютеры и средства хранения информации без личного присмотра, в случаях, если это может привести к их краже. При наличии риска утраты ПК и (или) средств хранения информации, необходимо принять меры по его минимизации (например, убирать переносной компьютер на обеденный перерыв и после завершения рабочего дня в закрывающийся на ключ шкаф, не оставлять незакрытым помещение, в котором находится оборудование информационной системы, использовать замки для переносных компьютеров);
3.8. Осуществлять обработку конфиденциальной информации на ПК, не оснащенном принятыми в компании средствами защиты информации, а также в присутствии лиц, не имеющих права доступа к данной информации, если при этом указанные лица могут ознакомиться с обрабатываемой информацией;
3.9. Записывать и хранить конфиденциальную информацию на неучтённых носителях информации (Flash-карта, CD-диск, носимый HDD и т.п), а также оставлять без личного присмотра на рабочем месте или где бы то ни было носители информации и распечатки, содержащие подобную информацию;
3.10. Допускать к работе на ПК лиц, не имеющих прав доступа к информационным ресурсам.
3.11. Оставляя рабочее место, даже на короткое время, Пользователь обязан заблокировать экран своего монитора.
3.12. По окончании рабочего времени при отсутствии служебной необходимости обесточивать ПК и другую оргтехнику во избежание её выхода из строя и в целях обеспечения противопожарной безопасности.
3.13. Доступ к информационным ресурсам, хранящимся на жестком диске ПК Пользователя, должен быть защищен паролем.
3.14. Пользователи обязаны обеспечивать безопасное хранение пароля, исключающее возможность его утери или разглашения.
3.15. Срок использования пароля составляет не более 90 дней. При смене пароля новое значение должно отличаться от предыдущего не менее чем в трёх позициях.
3.16. В случае подозрения на компрометацию пароля доступа необходимо немедленно изменить пароль и проинформировать об этом своего непосредственного руководителя.
3.17. Пользователь обязан создавать пароль в соответствии со следующими требованиями:

- длина пароля должна быть не менее 8 символов;
- пароль должен состоять из строчных и прописных букв, а также небуквенных символов (т.е. цифр, знаков пунктуации, специальных символов);
- пароль не должен быть легко угадываемым (не должен включать повторяющуюся последовательность каких-либо символов (например, "55555555",

"aaaaaaaa", “12345678”, “qwerty”, “йцукен” и т.п.), пароль не должен включать в себя легко подбираемые сочетания символов (имена, фамилии, наименования, клички домашних животных, даты рождения и т.д.) и общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

3.18. При использовании телекоммуникационных возможностей сети Интернет пользователи обязаны выполнять следующие требования:

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

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

- запрещается использовать возможности электронной почты для отправки сообщений противозаконного, экстремистского или враждебного характера, а также содержащего в себе информацию неэтичного содержания;
- при получении электронных сообщений из незнакомого источника и/или сомнительного содержания не следует открывать файлы, вложенные в сообщение, так как они с большой долей вероятности могут содержать вирусы. Такие сообщения необходимо удалять;
- не следует отвечать на подозрительные письма и, тем более, сообщать любые данные о себе, о компании и её сотрудниках.

4. ПОРЯДОК РАБОТЫ С ИНФОРМАЦИОННОЙ СИСТЕМОЙ

4.1. Пользователь при работе с программными и техническими средствами, входящими в состав информационной системы, обязан строго выполнять установленные правила и несёт персональную ответственность за их несоблюдение.

4.2. Информационные ресурсы администрации Галичского муниципального района Костромской области считаются собственностью организации, если иное не оговорено соответствующими соглашениями. Организация оставляет за собой право протоколировать и контролировать действия работников при обработке информации в информационной системе.

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

4.4. Пользователи не должны разглашать сведения о содержании информации, ставшей известной им в ходе выполнения должностных обязанностей, а также о процедурах и технической реализации защиты информации, принятых в организации.

4.5. Пользователи должны выполнять требования общих правил работы на АРМ и информировать своего непосредственного руководителя обо всех фактах нарушения данной Инструкции.

4.6. В целях повышения эффективности служебной деятельности для обмена информационными ресурсами (служебные документы, отчеты, обращения граждан и т.п.) могут использоваться съёмные материальные носители информации (Flash-карты, переносные жесткие диски, иные устройства записи и чтения), зарегистрированные и

находящиеся на учете в администрации Галичского муниципального района Костромской области.

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

5. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОРЯДКА

5.1. Ответственность за выполнение требований настоящей Инструкции возлагается на всех работников, являющихся пользователями автоматизированной информационной системы администрации Галичского муниципального района Костромской области.

5.2. Работник, нарушивший требования данной Инструкции, может быть подвергнут дисциплинарному наказанию в соответствии с законодательством Российской Федерации и трудовым договором.

Приложение № 13
Утверждено

Распоряжением администрации
Галичского муниципального района
Костромской области
от «24 » января 2017 года № 13-р

ПОРЯДОК

резервирования данных и восстановления работоспособности
информационной системы персональных данных

1. Общие положения

Порядок резервирования данных и восстановления работоспособности в автоматизированной информационной системе администрации Галичского муниципального района, разработан в целях обеспечения защиты информации, для последующего восстановления работоспособности автоматизированных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами и (или) иными внешними воздействиями, в соответствии с требованиями Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных документов.

2. Термины и определения

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

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

Автоматизированная информационная система (АИС) – взаимосвязанная совокупность данных, оборудования, программных средств, персонала, стандартов, процедур, предназначенных для сбора, обработки, распределения, хранения, выдачи (предоставления) информации.

Съемный носитель информации – носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования.

3. Перечень информации, подлежащей резервному копированию.

В целях обеспечения бесперебойной работы АИС и восстановления её работоспособности в администрации Галичского муниципального района подлежат резервному копированию рабочие документы сотрудников, включая результаты выполненных работ, хранящиеся в электронном виде.

4. Порядок резервирования данных в АИС

4.1. Резервное копирование информационных баз и рабочих документов администрации Галичского муниципального района осуществляется на локальной машине в ручном режиме.

4.2. В качестве носителей, на которые осуществляется резервное копирование информации, используются съемные электронные носители.

5. Требования к носителям, на которые осуществляется резервирование

5.1. Носитель, используемый для осуществления резервного копирования информации, должен соответствовать следующим требованиям:

5.1.1 Доступ к носителю физически или по сети может получить только сотрудник организации ответственный за выполнение резервирования критичной информации.

5.1.2 Носитель по своим основным характеристикам должен иметь достаточный объем свободного дискового пространства для хранения резервных копий.

6. Учет резервных копий

6.1. С целью учёта создаваемых резервных копий и обеспечения сохранности информации в администрации Галичского муниципального района ведется Журнал учета съемных носителей.

6.2. Уничтожение электронных носителей либо резервных копий сохраняемой информации производится по решению экспертной комиссии на основании Актов об уничтожении конфиденциальной информации после внесения соответствующих записей в Журнал учёта съемных носителей.

7. Порядок восстановления информационных ресурсов

7.1. В случае потери (уничтожения, модификации) информации лицо, ответственное за обработку конфиденциальной информации (в том числе персональных данных), обязано сообщить о факте происшедшего сбоя в работе информационной системы и утрате критичных данных ответственному за обеспечение резервного копирования, который принимает меры по восстановлению утраченной информации в кратчайший срок.

7.2. При этом необходимо также сообщить о возможных признаках, сопутствующих отказу в работе, для накопления информации о произошедших инцидентах информационной безопасности и анализа причин сбоев в работе информационной системы.

7.3. По итогам происшедшего инцидента утраты информации лицо, ответственное за резервирование, проводит разбирательство по выявлению причин инцидента в целях предотвращения подобных фактов в дальнейшем.

8. Ответственность за нарушение Порядка

8.1. Персональная ответственность за резервное копирование, хранение информации и ведение Журнала съемных носителей возлагается на ответственного за безопасность информационной системы администрации Галичского муниципального района Нарушение требований настоящего Порядка влечёт за собой дисциплинарную ответственность в соответствии с трудовым законодательством Российской Федерации.

Приложение № 14
Утверждено
распоряжением администрации
Галичского муниципального района Костромской
области
от «24» января 2017 года № 13-р

ЧАСТНАЯ МОДЕЛЬ
актуальных угроз безопасности информации
и вероятного нарушителя информационной системы персональных данных администрации Галичского муниципального района.

1. ОБЩИЕ ПОЛОЖЕНИЯ

В соответствии со статьей 19 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», оператор персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Угрозы безопасности персональных данных при их обработке в информационной системе персональных данных (далее – ИСПДН) администрации Галичского муниципального района могут быть связаны как с преднамеренными и непреднамеренными действиями пользователей, так и со специально осуществляемыми неправомерными действиями третьих лиц (отдельных организаций и граждан), а также иными источниками угроз.

Угрозы безопасности персональных данных могут быть реализованы за счёт утечки персональных данных по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при её передаче по каналам связи, технические каналы утечки акустической (речевой) и видовой информации) либо за счёт несанкционированного доступа с использованием соответствующего программного обеспечения.

Разработка модели угроз проведена на основании исходных параметров ИСПДн, определяемых в соответствии с предложенной ФСТЭК России Методикой определения угроз безопасности персональных данных, с привлечением в качестве консультантов сотрудников, имеющих необходимую подготовку и практический опыт.

2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Вредоносная программа (ВП) – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера, входящего в состав информационной системы персональных данных – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и её использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Межсетевой экран (МСЭ) – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (НСД) (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие установленные правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами 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.

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные излучения и наводки в виде электрических и магнитных полей от средств обработки защищаемой информации, присутствующих в физической среде.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных (УБПДн) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

3. РАЗРАБОТКА АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ

Определение исходной защищенности ИСПДн

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», экспертным путём были определены характеристики исходной защищенности ИСПДн, которые сведены в таблицу 1 и имеют следующие значения:

Таблица 1

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
- распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	–
- городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	–
- корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	–	–
- локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	–	–
- локальная ИСПДн, развернутая в пределах одного здания.	–	+	–

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
2. По наличию соединения с сетями общего пользования:			
- ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	–
- ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
- ИСПДн, физически отделенная от сети общего пользования.	–	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
- чтение, поиск;	–	–	–
- запись, удаление, сортировка;	+	–	–
- модификация, передача.	–	–	–
4. По разграничению доступа к персональным данным:			
– ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект персональных данных;	+	–	–
– ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	–
– ИСПДн с открытым доступом.	–	–	–
5. По наличию соединений с другими базами персональных данных иных ИСПДн:			
- интегрированная ИСПДн (организация использует несколько баз персональных данных ИСПДн, при этом организация не является владельцем всех используемых баз персональных данных);	–	–	–
- ИСПДН, в которой используется одна база персональных данных, принадлежащая организации – владельцу данной ИСПДн.	+	–	–
6. По уровню обобщения (обезличивания) персональных данных:			
- ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	–	–	–
- ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	-	–
- ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта персональных данных).	–	+	–
7. По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
– ИСПДн, предоставляющая всю базу персональных данных;	–	–	–
– ИСПДн, предоставляющая часть персональных данных;	–	–	–
– ИСПДн, не предоставляющие никакой информации.	–	+	–
ИТОГО:	3	4	0
	42,84%	57,16%	0 %
Исходная степень защищенности имеет средний уровень	5		

Исходя из вышеизложенного:

С учетом полученных уровней защиты ИСПДн следует, что более 70 % оценок имеют средний и высокий уровень исходной защищенности ИСПДн, что позволяет определить уровень исходной защищенности информационной системы персональных данных как «средний» с коэффициентом $Y_1 = 5$.

По данным обследования ИСПДн администрации Галичского муниципального района определена как типовая модель угроз безопасности персональных данных, обрабатываемая в локальной информационной системе персональных данных, имеющая подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, доступ к ИСПДн осуществляется в соответствии с матрицей доступа сотрудников предприятия, был сформирован перечень возможных угроз (таблица 2).

При составлении перечня актуальных угроз безопасности персональных данных каждой градации вероятности возникновения угрозы ставился в соответствие числовой коэффициент Y_2, а именно:

для маловероятной угрозы - 0;
для низкой вероятности угрозы - 2;
для средней вероятности угрозы - 5;
для высокой вероятности угрозы - 10,

Наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии возможности реализации данной угрозы, которая определена по формуле:

$$Y = (Y_1 + Y_2)/20$$

По значению коэффициента реализуемости угрозы Y была сформирована вербальная интерпретация реализуемости угрозы, которая отражается следующим образом:

если $0 \le Y \le 0{,}3$, то возможность реализации угрозы признается низкой;

если $0{,}3 < Y \le 0{,}6$, то возможность реализации угрозы признается средней;

если $0{,}6 < Y \le 0{,}8$, то возможность реализации угрозы признается высокой;

если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» после определения коэффициентов реализуемости угрозы на основе мнения экспертов по каждой угрозе была определена опасность её реализации по трём значениям:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Данные показатели занесены в таблице 2.

С учётом совокупности всех показателей и оценок угроз безопасности ИСПДн, в соответствии с методикой ФСТЭК РФ, была осуществлена оценка актуальности возможных угроз, которая приведена в таблице 2.

Оценка актуальности угроз ИСПДн администрации Галичского муниципального района *Таблица 2*

№	Угрозы ИСПДн	Y_2	Коэфф. реализуемости угрозы Y	Опасность реализуемой угрозы	Актуальность угрозы
	Угрозы утечки информации по техническим каналам				
1	угрозы утечки акустической (речевой) информации	0	0,25	низкая опасность	Неактуальна
2	угрозы утечки визуальной информации	0	0,25	низкая опасность	Неактуальна
3	угрозы утечки информации по каналу ПЭМИН	0	0,25	низкая опасность	Неактуальна
	Угрозы НСД к персональным данным				
	Угрозы непосредственного доступа				
4	угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	0	0,25	Средняя опасность	Неактуальна
5	угрозы, реализуемые после загрузки операционной системы и направленные на осуществление несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)	5	0,5	Средняя опасность	Актуальна
6	угрозы внедрения вредоносных программ	5	0,5	Средняя опасность	Актуальна
	Угрозы удаленного доступа				
7	угрозы "анализа сетевого трафика" с перехватом информации, передаваемой по локальной сети, а также во внешние сети и принимаемой из внешних сетей	0	0,25	средняя опасность	Неактуальна
8	угрозы сканирования, направленные на выявление	0	0,25	высокая	Неактуальна

№	Угрозы ИСПДн	Y_2	Коэфф. реализуемости угрозы Y	Опасность реализуемой угрозы	Актуальность угрозы
	типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;			опасность	
9	угрозы получения НСД путем подмены доверенного объекта;	0	0,25	низкая опасность	Неактуальна
10	угрозы выявления паролей	0	0,25	средняя опасность	Неактуальна
11	угрозы типа "отказ в обслуживании"	5	0,5	Средняя опасность	Актуальна
12	угрозы удалённого запуска приложений	0	0,25	низкая опасность	Неактуальна
13	угрозы внедрения по сети вредоносных программ.	5	0,5	Средняя опасность	Актуальна
14	угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;	5	0,5	Средняя опасность	Актуальна
15	угрозы сканирования, направленные на выявление типа ОС ИСПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;	5	0,5	Высокая опасность	Актуальна

4. РАЗРАБОТКА МОДЕЛИ ВЕРОЯТНОГО НАРУШИТЕЛЯ

В целях определения оценки вероятности угроз безопасности конфиденциальной информации, в том числе персональных данных, в администрации Галичского муниципального района в соответствии с Положением о методах и способах защиты информации в информационных системах персональных данных разработана модель нарушителя.

Нарушитель - физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации, в том числе персональных данных, при их обработке техническими средствами. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена – внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн – внутренние нарушители.

В соответствии с Базовой моделью угроз безопасности персональных данных при обработке их в информационных системах, угрозу для ИСПДн администрации Галичского муниципального района могут представлять следующие типы предполагаемых нарушителей:

внешние нарушители:

- недобросовестные партнеры;
- внешние субъекты (физические лица).

внутренние нарушители:

- лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к персональным данным - сотрудники, действующие преднамеренно;
- зарегистрированные пользователи ИСПДн, имеющие санкционированный доступ к ресурсам персональных данных с рабочего места – сотрудники действующие непреднамеренно;
- зарегистрированные пользователи с полномочиями системного администратора ИСПДн;
- программисты – разработчики прикладного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте;
- лица, обеспечивающие эксплуатацию и ремонт технических средств на оборудовании ИСПДн.

На основании данных о предполагаемых вероятных нарушителях, параметров исходной защищенности ИСПДн и сформированных угроз безопасности был сформирован перечень действий, способствующий реализации угроз и определены методы и способы защиты персональных данных (таблица 3).

Таблица 3

№	**Действия, приводящие к реализации угроз персональным данным**	**Используемые меры защиты**
Внешние нарушители:		
1.	Осуществление несанкционированного доступа к линиям и каналам связи, выходящим за пределы служебных помещений;	Организационные меры, граница контролируемой зоны.
2.	Осуществление несанкционированного доступа через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;	**Антивирус Kaspersky, Брандмауэр**
3.	Осуществление несанкционированного доступа к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;	**Антивирус Kaspersky** Internet
4.	Осуществление несанкционированного доступа через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны;	Организационные меры
Внутренние нарушители:		
1.	Получение доступа к фрагментам информации, содержащей персональные данные и передающейся по внутренним каналам связи ИСПДн;	Организационные меры
2.	Обладание фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;	Конфиденциальная информация
3.	Знание имен и выявление учётных данных (логин+пароль) зарегистрированных пользователей;	Организационная мера, периодическая смена пароля
4.	Знание, ре, одного легальногпо меньшей мео имени доступа;	Конфиденциальная информация
5.	Обладание всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;	Организационная мера, конфиденциальная информация
6.	Может располагать конфиденциальными данными, к которым имеет доступ;	Организационные меры
7.	Может располагать информацией о топологии ИСПДн на базе локальной информационной системы, через которую он осуществляет доступ, и составе технических средств ИСПДн;	Организационные меры
8.	Возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.	Организационные меры
9.	Обладание полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;	Конфиденциальная информация, ограничение круга лиц по доступу
10.	Обладание полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;	Конфиденциальная информация, ограничение круга лиц по доступу
11.	Получение доступа к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;	Конфиденциальная информация, ограничение круга лиц по доступу
12.	Получение доступа ко всем техническим средствам сегмента (фрагмента) ИСПДн;	Конфиденциальная информация, ограничение круга лиц по доступу
13.	Обладание правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.	Ограничение круга лиц по доступу
14.	Обладание полной информацией о системном и прикладном программном обеспечении ИСПДн;	Ограничение круга лиц по доступу
15.	Обладание полной информацией о технических средствах и конфигурации ИСПДн;	Ограничение круга лиц по доступу
16.	Получение доступа ко всем техническим средствам обработки информации и данным ИСПДн;	Ограничение круга лиц по доступу

№	Действия, приводящие к реализации угроз персональным данным	Используемые меры защиты
17.	Обладание правами конфигурирования и административной настройки технических средств ИСПДн.	Ограничение круга лиц по доступу
18.	Обладание информацией об алгоритмах и программах обработки информации на ИСПДн;	Организационные меры, конфиденциальная информация
19.	Обладание возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;	Исключено на стадии закупки оборудования

5. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

При разработке системы защиты персональных данных необходимо учитывать следующие рекомендации, обеспечивающие нейтрализацию предполагаемых угроз и снижение вероятности утечки информации в соответствии с классом ИСПДн администрации Галичского муниципального района и актуальными угрозами:

Подсистема управления доступом:

– идентификация и проверка подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю сроком действия 90 суток, длиной не менее восьми буквенно-цифровых символов.

Межсетевое экранирование:

– принятие решения по фильтрации для каждого сетевого пакета независимо;
– идентификация и аутентификация администратора МСЭ при его локальных запросах на доступ, возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия;
– регистрация входа (выхода) администратора МСЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
– контроль целостности своей программной и информационной части;
– восстановление после сбоев и отказов оборудования;
– при удалённых запросах блокирование доступа не идентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату информации;
– оперативное восстановление свойств экранирования.

Защита от угроз программно-математического воздействия (ПМВ):

– идентификация и аутентификация субъектов доступа при входе в ИСПДн;
– запрет на использование прав администратора на автоматизированных рабочих местах пользователей;
– запрет на загрузку ОС АРМ со съемных носителей информации.

Подсистема регистрации и учета:

– регистрация входа (выхода) субъекта доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и её программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
– учёт всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал учета съемных носителей;
– регистрация событий проверки и обнаружения ПМВ. В параметрах регистрации указываются время и дата проверки или обнаружения ПМВ, идентификатор субъекта доступа, инициировавшего данные действия, характер выполняемых действий по проверке, тип обнаруженной вредоносной программы (ВП), результат действий средства защиты по блокированию ПМВ;
– данные регистрации должны быть защищены от их уничтожения или модификации нарушителем;
– механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов;
– механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров;
– автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать ВП);
– механизм анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением ответственного за обработку и защиту персональных данных;
– проведение нескольких видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации.

Подсистема обеспечения целостности
(при использовании средств защиты информации):

– целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ;

– средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;

– проверка целостности модулей средства защиты от ПМВ, необходимых для корректного функционирования, при его загрузке с использованием контрольных сумм;

– возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности;

– механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм;

– физическая охрана ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации;

Подсистема антивирусной защиты:

– автоматическая проверка на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа;

– работоспособность механизмов автоматического блокирования обнаруженных ВП путём их удаления из программных модулей или уничтожения;

– регулярная (при первом запуске средств защиты персональных данных от ПМВ и с устанавливаемой периодичностью) проверка на предмет наличия в них ВП;

– автоматическая проверка ИСПДн на предмет наличия ВП при выявлении факта ПМВ;

– механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.

Приложение № 15
Утверждено
распоряжением администрации
Галичского муниципального района Костромской
области
от «24» января 2017 года № 13-р

Инструкция администратора безопасности АИС

1. Общие положения

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

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

1.3. Распоряжением администрации Галичского муниципального района администратором безопасности назначается, сотрудник, имеющий соответствующую квалификацию и опыт работы с оборудованием и программным обеспечением информационных систем. Администратор безопасности обеспечивает правильное использование и функционирование установленного системного и прикладного программного обеспечения, средств технической защиты информации (далее по тексту - СЗИ) от несанкционированного доступа (далее по тексту - НСД), а также поддержание достигнутого уровня защиты АИС и её ресурсов на этапах эксплуатации и модернизации.

1.4. Администратор безопасности имеет рабочее место, размещаемое в выделенном помещении в которое исключается несанкционированный доступ посторонних лиц. Рабочее место Администратора подключается к ЛВС.

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

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

2. Администратор безопасности в своей деятельности имеет право:

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

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

2.3. Организовывать доступ пользователей к ресурсам автоматизированной информационной системы в соответствии с Перечнем должностей, имеющих право доступа к обработке конфиденциальной информации.

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

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

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

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

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

2.9. Своевременно вносить коррективы в список пользователей информационных ресурсов при приеме на работу и увольнении сотрудников. Удалять учётные записи пользователей ИС на доступ к информационным ресурсам.

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

- за соблюдением сотрудниками требований действующих нормативных и руководящих документов, регламентирующих обработку конфиденциальной информации; - за осуществлением неизменности и целостности программной среды АИС (системное и прикладное ПО), средств антивирусной защиты и межсетевого экранирования, их параметров и режимов;

- за наличием и возможным использованием на автоматизированных рабочих местах вредоносных программ и иного нелицензионного ПО, не связанного с выполнением функциональных задач;

- за соблюдением пользователями принятого в организации режима парольной политики и порядка использования учётных записей на доступ к информационным ресурсам;

- за состоянием допуска пользователей к работе с ресурсами АИС и изменением прав доступа к защищаемой конфиденциальной информации, в том числе персональным данным;

- за выполнением правил учёта, использования и хранения электронных носителей конфиденциальной информации;

- за поддержанием установленного порядка обновления антивирусных баз и антивирусной защиты информационных ресурсов;

- за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусах системных блоков АРМ, обрабатывающих информацию ограниченного доступа; - за сроками действия сертификатов и лицензий эксплуатируемого оборудования и ПО;

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

.

3. Администратор безопасности обязан:

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

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

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

3.4. Блокировать учётные записи пользователей на АРМ в случае окончания срока действия сертификата соответствия ФСТЭК России, ФСБ России на любое СЗИ, из используемых в ИСПДн, до момента его продления. В случае непродления сертификата соответствия на СЗИ администратор обязан поставить в известность орган по аттестации, проводивший аттестацию ИСПДн, для принятия дальнейшего совместного решения.

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

4. Администратор безопасности имеет право:

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

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

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

5. Администратор безопасности несёт ответственность:

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

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