



БЕЛГОРОДСКАЯ ОБЛАСТЬ

**АДМИНИСТРАЦИЯ  
АЛЕКСЕЕВСКОГО ГОРОДСКОГО ОКРУГА**  
РАСПОРЯЖЕНИЕ

Алексеевка

*«03» февраля 2011 г.*

№ *118-р*

Об утверждении документов, определяющих политику администрации Алексеевского городского округа в отношении обработки персональных данных

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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», от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и в целях совершенствования работы по обеспечению защиты персональных данных в администрации Алексеевского городского округа:

1. Утвердить и ввести в действие следующие организационно-распорядительные документы по защите персональных данных:

1.1. Правила доступа в помещения, в которых расположены элементы информационных систем персональных данных, в рабочее и нерабочее время, а также в нештатных ситуациях (приложение № 1);

1.2. Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (приложение № 2);

1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами (приложение № 3);

1.4. Правила работы с обезличенными данными в случае обезличивания персональных данных (приложение № 4);

1.5. Правила рассмотрения запросов субъектов персональных данных и их представителей (приложение № 5);

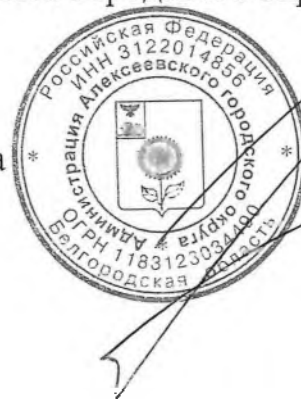
1.6. Правила оценки возможного вреда субъектам персональных данных и соотнесения указанного вреда с принимаемыми мерами (приложение № 6)

2. Лицам, исполняющим должностные обязанности, предусматривающие осуществление обработки персональных данных либо осуществление доступа к персональным данным руководствоваться положениями данного распоряжения.

3. Управлению организационно-контрольной работы и архивного дела аппарата главы администрации Алексеевского городского округа (Тратникова Т.П.) обеспечить размещение распоряжения на официальном сайте органов местного самоуправления Алексеевского городского округа.


4. Контроль за исполнением распоряжения возложить на заместителя главы администрации Алексеевского городского округа, руководителя аппарата главы администрации Алексеевского городского округа Спивакову О.В.

Глава администрации  
Алексеевского городского округа



С.В. Сергачев

ПРИЛОЖЕНИЕ № 1  
Утверждено  
распоряжением администрации  
Алексеевского городского округа  
от «05» февраля 2011 г. № 188-р



Правила доступа в помещения, в которых расположены элементы информационных систем персональных данных, в рабочее и нерабочее время, а также в нестандартных ситуациях

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие правила доступа в помещения, в которых расположены элементы информационных систем персональных данных, в рабочее и нерабочее время, а также в нестандартных ситуациях (далее – Правила) разработаны в целях выполнения требований Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. № 21, приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 в администрации Алексеевского городского округа (далее – Учреждение).

1.2 Настоящие Правила должны соблюдаться всеми сотрудниками Учреждения.

## 2. ДОСТУП В ПОМЕЩЕНИЯ В РАБОЧЕЕ ВРЕМЯ

2.1 В рабочее время доступ в помещения, в которых расположены элементы ИСПДн Учреждения, разрешен только работникам Учреждения, указанным в соответствующем перечне лиц.

2.2 В рабочее время помещения, где расположены элементы ИСПДн, должны закрываться на замок и открываться только для санкционированного прохода.

2.3 Доступ обслуживающего персонала для уборки помещения допускается только в присутствии пользователей ИСПДн.

## 3. ДОСТУП В ПОМЕЩЕНИЯ В НЕРАБОЧЕЕ ВРЕМЯ

3.1 В нерабочее время доступ в помещения, в которых расположены элементы ИСПДн Учреждения, разрешен только работникам Учреждения, указанным в соответствующем перечне лиц при наличии служебной записки, подписанной руководителем подразделения и заверенной ответственным за обеспечение безопасности ПДн с занесением записи в «Журнал доступа в помещения, где расположены элементы ИСПДн, в нерабочее время»

#### **4. ДОСТУП В ПОМЕЩЕНИЯ В НЕШТАТНЫХ СИТУАЦИЯХ**

4.1 Если перед вскрытием помещений обнаружено нарушение целостности замков, то помещения не вскрываются, составляется акт о случившемся и немедленно докладывается руководителю организации, администратору ИБ и службе безопасности, и принимаются меры по охране помещений до прибытия службы безопасности.

4.2 В дневное время суток сотрудник, обнаруживший нештатную ситуацию, должен поставить в известность непосредственного руководителя структурного подразделения – устно, администратора ИБ – устно, при необходимости – письменно.

4.3 В ночное время суток при возникновении нештатной ситуации, должна быть оповещена служба безопасности (охрана). Событие в обязательном порядке регистрируется в журнале дежурств, с указанием точного времени инцидента, краткого описания событий, с указанием Ф.И.О. оповещенных лиц, описанием действий, направленных на устранение нештатной ситуации. Если создается угроза уничтожения ПДн, то дежурный по организации вместе с подразделением охраны имеет право вскрыть помещения и принять меры к спасению технических средств и документов. При этом также составляется рапорт о случившемся и немедленно докладывается лицу, ответственному за обеспечение безопасности ПДн.



ПРИЛОЖЕНИЕ  
 Утверждено  
 распоряжением администрации  
 Алексеевского городского округа  
 от «03» февраля 2012 г. № 11/12



Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (далее – Правила) разработаны в соответствии с:

- статьей 24 Конституции Российской Федерации;
- главой 14 Трудового Кодекса Российской Федерации;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ от 21 марта 2012 г. № 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».

1.2 Настоящие Правила устанавливают в администрации Алексеевского городского округа (далее – Учреждение) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют:

- цели обработки персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- содержание обрабатываемых персональных данных;

- сроки обработки и хранения персональных данных;
- порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований.

1.3 Настоящие Правила вступают в силу с момента их утверждения и действуют бессрочно, до замены их новыми. Все изменения в Правила вносятся распоряжением.

## **2. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

2.1 Обработка персональных данных осуществляется с целью:

- выполнения возложенных на Учреждение обязанностей;
- учета персональных данных сотрудников в связи с реализацией трудовых отношений.

## **3. КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ, СРОКИ ИХ ОБРАБОТКИ И ХРАНЕНИЯ**

3.1 Категории субъектов, персональные данные которых обрабатываются:

- сотрудники Учреждения;
- субъекты ПДн, не являющиеся сотрудниками Учреждения.

3.2 Персональные данные обрабатываются в сроки, обусловленные заявленными целями их обработки.

3.3 Обработка персональных данных прекращается по достижении заявленных целей или при наступлении иных законных оснований.

3.4 Определение сроков хранения осуществляется в соответствии с требованиями архивного законодательства Российской Федерации, в том числе в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих персональные данные, срок обработки, в том числе хранения, устанавливается по максимальному сроку.

Обработка персональных данных без документально определенных и оформленных сроков обработки, в том числе хранения, не допускается.

## **4. СОДЕРЖАНИЕ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

4.1 В соответствии с целями обработки Учреждение обрабатывает персональные данные, состав которых определен в «Перечне обрабатываемых персональных данных», утвержденных руководителем Учреждения.

## **5. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ОБРАБОТКИ ИЛИ ПРИ НАСТУПЛЕНИИ ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ**

5.1 В случае достижения цели обработки персональных данных Учреждение обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим

по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами Российской Федерации.

5.2 В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Учреждение обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами Российской Федерации.

5.3 В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения. В случае, если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.4 В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 5.1-5.3, Учреждение осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом,



действующим по поручению Учреждения) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.5 После уничтожения персональных данных Учреждение обязано уведомить о факте уничтожения субъекта персональных данных и, в случае если уничтожение произведено по запросу уполномоченного органа, указанный орган.

## **6. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1 К процедурам, направленным на выявление и предотвращение нарушений законодательства в сфере персональных данных и устранение таких последствий, относятся:

- реализация мер, направленных на обеспечение выполнения Учреждением своих обязанностей;
- выполнение предусмотренных законодательством обязанностей, возложенных на Учреждение;
- обеспечение личной ответственности сотрудников, осуществляющих обработку либо доступ к персональным данным;
- организация рассмотрения запросов субъектов персональных данных или их представителей и ответов на такие запросы;
- организация внутреннего контроля соответствия обработки персональных данных требованиям к защите, установленным действующим законодательством и локальными актами;
- сокращение объема обрабатываемых данных;
- стандартизация операций, осуществляемых с персональными данными;
- определение порядка доступа сотрудников Учреждения в помещения, в которых ведется обработка персональных данных;
- проведение необходимых мероприятий по обеспечению безопасности персональных данных и носителей персональных данных;
- проведение периодических проверок условий обработки персональных данных;
- повышение осведомленности сотрудников, имеющих доступ к персональным данным, путем ознакомления с положениями законодательства Российской Федерации, локальными актами и организации обучения;
- блокирование, внесение изменений и уничтожение персональных данных в предусмотренных действующим законодательством случаях;
- оповещение субъектов персональных данных в предусмотренных действующим законодательством случаях;
- разъяснение прав субъектам персональных данных в вопросах обработки и обеспечения безопасности персональных данных;

– публикация и обеспечение доступа неограниченному кругу лиц документов, определяющих политику в отношении обработки персональных данных.

6.2 Указанный перечень процедур может дополняться.

## ПРИЛОЖЕНИЕ № 3

Утверждено  
распоряжением администрации  
Алексеевского городского округа  
от «03» сентября 2011 г. № 118-р



Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами (далее – Правила) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Алексеевского городского округа (далее – Учреждение).

1.2 Настоящие Правила разработаны в соответствии с Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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».

1.3 Внутренний контроль состояния защиты информации включает в себя:

- контроль организации защиты информации;
- контроль эффективности защиты информации.

## 2. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

2.1 В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организовывается проведение периодических проверок условий обработки персональных данных.

2.2 Проверки осуществляются ответственным за организацию обработки персональных данных, либо комиссией, созданной на основании приказа руководителя.

2.3 В проведении проверки не может участвовать сотрудник, прямо или косвенно заинтересованный в её результатах.

2.4 Проверка соответствия обработки персональных данных установленным требованиям проводится не реже одного раза в год на основании утвержденного руководителем «Плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям» или на основании письменного заявления о нарушении правил обработки.

2.5 Проведение внеплановой проверки организуется в течение 3 рабочих дней с момента поступления соответствующего заявления.

2.6 При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям полностью, объективно и всесторонне производится проверка:

- соблюдения принципов обработки персональных данных;
- соответствия локальных актов в области персональных данных действующему законодательству Российской Федерации;
- выполнения сотрудниками требований и правил обработки персональных данных;
- актуальности информации о законности целей обработки персональных данных и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований обработки и обеспечения безопасности персональных данных;
- правильности осуществления сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных;
- актуальности перечня лиц, имеющих доступ к персональным данным;
- соблюдения прав субъектов персональных данных;
- порядка взаимодействия с субъектами персональных данных, в том числе соблюдения сроков, требований по уведомлениям, порядка разъяснения субъектам необходимой информации, порядка реагирования на запросы субъектов персональных данных, порядка действий при достижении целей обработки и отзыве согласия субъекта персональных данных, наличия необходимых согласий субъектов персональных данных;
- актуальности сведений, содержащихся в уведомлении об обработке персональных данных;
- актуальности перечня информационных систем персональных данных;
- знания и соблюдения сотрудниками положений действующего законодательства Российской Федерации в области персональных данных, локальных актов Учреждения;
- соблюдения условий сотрудниками конфиденциальности персональных данных;
- соблюдения сотрудниками требований по обеспечению безопасности персональных данных;

– наличия и актуальности локальных актов, технической и эксплуатационной документации, технических и программных средств информационной системы персональных данных.

2.7 Контроль осуществляется непосредственно на месте обработки персональных данных путем опроса сотрудников и осмотра рабочих мест, участвующих в процессе обработки персональных данных.

2.8 По результатам проведения внутреннего контроля составляется протокол проведения проверки.

2.9 При выявлении нарушений в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

2.10 О результатах проведения проверки и мерах, необходимых для устранения нарушений, руководителю Учреждения докладывает ответственный за организацию обработки персональных данных.

**ПРИЛОЖЕНИЕ № 1**  
к Правилам осуществления внутреннего  
контроля соответствия обработки  
персональных данных требованиям к  
защите персональных данных,  
установленным Федеральным законом  
«О персональных данных», принятыми  
в соответствии с ним нормативными  
правовыми актами и локальными  
актами

**ПРОТОКОЛ**  
проведения внутренней проверки соответствия обработки персональных данных  
требованиям к защите персональных данных

« \_\_\_ » \_\_\_\_\_ 20\_\_ г.

г. Алексеевка

№ \_\_\_\_\_

Комиссия в составе:  
председатель комиссии

\_\_\_\_\_

(Ф.И.О., должность)

члены комиссии

\_\_\_\_\_

(Ф.И.О., должность)

\_\_\_\_\_

(Ф.И.О., должность)

провела проверку соответствия обработки персональных данных требованиям к защите персональных данных.

Проверка проводилась в соответствии с «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами».

Выявленные нарушения:

\_\_\_\_\_

Меры по устранению нарушений:

\_\_\_\_\_

Срок устранения нарушений: \_\_\_\_\_

Председатель комиссии:

Должность \_\_\_\_\_

Ф.И.О.

Члены комиссии:

Должность \_\_\_\_\_

Ф.И.О.

Должность \_\_\_\_\_

Ф.И.О.

ПРИЛОЖЕНИЕ № 4  
 Утверждено  
 распоряжением администрации  
 Алексеевского городского округа  
 от «03» февраля 2014 г. № 118-р



## Правила работы с обезличенными данными в случае обезличивания персональных данных

### 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие правила работы с обезличенными данными в случае обезличивания персональных данных (далее – Правила) определяют методы и процедуры обезличивания персональных данных, а также порядок работы с обезличенными данными в администрации Алексеевского городского округа (далее – Учреждение) и действуют постоянно.

1.2 Настоящие Правила разработаны в соответствии с Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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», Приказом Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

1.3 Свойства обезличенных данных:

полнота – сохранение всей информации о персональных данных конкретных субъектов или группах субъектов, которая имела 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 – соответствие семантики атрибутов обезличенных данных семантике соответствующих атрибутов персональных данных при их обезличивании;

применимость – возможность обработки персональных данных без предварительного деобезличивания всего объема записей о субъектах;

анонимность – невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации.

### 2. МЕТОДЫ ОБЕЗЛИЧИВАНИЯ

2.1 К методам обезличивания относятся:

– метод введения идентификаторов – замена части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия;

– метод изменения состава или семантики – изменение состава или семантики персональных данных путем замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;

– метод декомпозиции – разделение множества (массива) персональных данных на несколько подмножеств (частей) с последующим отдельным хранением подмножеств;

– метод перемешивания – перестановка отдельных значений или групп значений атрибутов персональных данных в массиве персональных данных.

2.2 Применение того или иного метода обезличивания позволит получить обезличенные данные, обладающие различными свойствами, что даст возможность осуществлять все виды обработки персональных данных.

2.3 В каждом конкретном случае необходимо применять метод, который гарантирует свойства, необходимые для решения конкретных задач обработки.

2.4 Результаты сопоставления свойства обезличенных данных с методами обезличивания приведены в Таблице 1.

Таблица 1 – Соответствие методов обезличивания свойствам обезличенных данных

<b>Метод обезличивания</b>	<b>Введение идентификаторов</b>	<b>Изменение состава и семантики</b>	<b>Декомпозиция</b>	<b>Перемешивание</b>
<b>Свойства обезличенных данных</b>				
Полнота	+	+/-	+	+
Структурированность	+	+	+	+
Релевантность	+/-	+	+	+
Семантическая целостность	+	+/-	+	+
Применимость	+	+	+	+
Анонимность	+/-	+	+/-	+
+ безусловное наличие свойства; +/- условное наличие свойства				

### 3. ПРОЦЕДУРЫ ОБЕЗЛИЧИВАНИЯ

3.1 Процедура обезличивания обеспечивает практическую реализацию метода обезличивания и задается своим описанием.

3.2 Процедура реализации метода введения идентификаторов



3.2.1 Каждому значению идентификатора должно соответствовать одно значение атрибута и каждому значению атрибута должно соответствовать одно значение идентификатора.

3.2.2 Таблицы соответствия (дополнительные данные) создаются для каждого атрибута персональных данных, значения которых заменяются идентификаторами.

3.2.3 При обезличивании персональные данные в исходном множестве заменяются идентификаторами согласно таблице соответствия. Деобезличивание достигается обратной заменой идентификаторов на значения персональных данных по таблице соответствия.

3.2.4 На этапе реализации процедуры обезличивания определяются следующие параметры:

- перечень таблиц соответствия (перечень атрибутов, для которых происходит замена значений идентификаторами);
- правила вычисления идентификаторов - наборов символов, однозначно соответствующих значениям атрибутов персональных данных субъекта;
- объемы таблицы соответствия - количество строк таблицы соответствия, содержащих идентификатор и соответствующее ему значение.

3.2.5 В качестве атрибутов, значения которых заменяются идентификаторами, как правило, выбираются атрибуты, однозначно идентифицирующие субъекта персональных данных.

3.2.6 Количество идентификаторов и объем таблиц соответствия, как правило, равны исходному количеству субъектов персональных данных. Возможны случаи, когда идентификатор вычисляется в зависимости от значения соответствующего атрибута.

3.2.7 Таблицы соответствия должны быть доступны ограниченному числу сотрудников.

3.2.8 Программное обеспечение, реализующее процедуру, должно обеспечивать внесение изменений и поддержку актуальности таблиц соответствия.

3.3 Процедура реализации метода изменения состава или семантики

3.3.1 Процедура реализации метода должна содержать правила удаления либо замены значений персональных данных субъектов на новые значения, вычисляемые по заданным правилам.

3.3.2 При замене значений атрибутов на новые требуется устанавливать правила обратной замены, если это необходимо для деобезличивания.

3.3.3 На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

- перечень атрибутов персональных данных, подлежащих удалению;
- перечень атрибутов персональных данных, подлежащих замене на новые значения;
- правила вычисления значений для замены (обратной замены) персональных данных субъектов.

3.3.4 Программная реализация процедуры должна обеспечить возможность внесения изменений и дополнений в состав обезличенных данных, динамическое вычисление значений для замены при занесении новых субъектов, проверку и поддержку актуальности данных.

#### 3.4 Процедура реализации метода декомпозиции

3.4.1 Процедура реализации метода по заданному правилу (алгоритму) производит разделение исходного массива персональных данных на несколько частей, каждая из которых содержит заданный набор атрибутов всех субъектов. Сведения, содержащиеся в каждой части, не позволяют идентифицировать субъектов персональных данных.

3.4.2 Деобезличивание осуществляется по заданному набору связей (используются таблицы связей, являющиеся дополнительными данными) между отдельно хранимыми частями.

3.4.3 На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

- перечень атрибутов, составляющих подмножества персональных данных;
- таблицы связей между подмножествами персональных данных;
- адреса хранения подмножеств персональных данных.

3.4.4 Правила разделения исходного массива данных определяются таким образом, чтобы каждая из отдельно хранимых частей не содержала сведений, позволяющих однозначно идентифицировать субъекта персональных данных.

3.4.5 Программная реализация процедуры должна обеспечивать согласованное внесение изменений и дополнений во все подмножества и таблицы связей, поиск данных о субъекте во всех подмножествах, поддержку актуальности таблиц связей, проверку полноты данных (согласование подмножеств).

#### 3.5 Процедура реализации метода перемешивания

3.5.1 Метод перемешивания реализуется путем перемешивания отдельных значений или групп значений атрибутов субъектов персональных данных между собой.

3.5.2 Перемешивание проводится по установленному правилу.

3.5.3 Деобезличивание достигается с использованием процедуры, обратной процедуре перемешивания.

3.5.4 Для реализации процедуры необходимо определить алгоритм перемешивания и его параметры.

3.5.5 На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

- набор параметров алгоритма перемешивания (дополнительные данные для обезличивания/деобезличивания);
- значения параметров алгоритма перемешивания (дополнительные данные для обезличивания/деобезличивания).

3.5.6 Выбор параметров перемешивания зависит от алгоритма перемешивания, требуемой стойкости к атакам, и объема обезличиваемых персональных данных.

3.5.7 Программная реализация процедуры должна обеспечивать возможность внесения изменений и дополнений в состав обезличенных данных, добавление новых пользователей, поддержку актуальности данных и возможность повторного перемешивания с новыми параметрами без предварительного деобезличивания.

#### **4. ОРГАНИЗАЦИЯ ОБРАБОТКИ ОБЕЗЛИЧЕННЫХ ДАННЫХ**

4.1 При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

4.2 Обезличивание персональных данных должно производиться перед внесением их в информационную систему.

4.3 Учреждение вправе обрабатывать обезличенные данные, полученные от третьих лиц.

4.4 В процессе обработки обезличенных данных, при необходимости, может проводиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

4.5 Обработка персональных данных до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с действующим законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

4.6 Обработка обезличенных данных должна осуществляться с использованием технических и программных средств, соответствующих форме представления и хранения данных.

4.7 Хранение и защиту дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания, следует обеспечить в соответствии с внутренними процедурами защиты конфиденциальной информации. При этом должно обеспечиваться исполнение установленных правил доступа пользователей к хранимым данным, резервного копирования и возможности актуализации и восстановления хранимых данных.

4.8 Процедуры обезличивания/деобезличивания должны встраиваться в процессы обработки персональных данных как их неотъемлемый элемент, а также максимально эффективно использовать имеющуюся инфраструктуру, обеспечивающую обработку персональных данных.

#### **5. ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ**

5.1 При обработке обезличенных данных следует:

– обеспечить соответствие процедур обезличивания/деобезличивания персональных данных требованиям к обезличенным данным и методам обезличивания;

- обеспечить соответствие процедур обезличивания/деобезличивания условиям и целям обработки персональных данных;

- убедиться, что при реализации процедур обезличивания/деобезличивания, а также при последующей обработке обезличенных данных не нарушаются права субъекта персональных данных.

5.2 В случае, если обработка обезличенных данных была поручена третьим лицом, следует соблюдать все требования, предъявляемые этим лицом.

5.3 При хранении обезличенных данных следует:

- организовать раздельное хранение обезличенных данных и дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания;

- обеспечивать конфиденциальность дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания.

5.4 При передаче вместе с обезличенными данными информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания следует обеспечить конфиденциальность канала (способа) передачи данных.

5.5 В ходе реализации процедуры деобезличивания следует:

- реализовать все требования по обеспечению безопасности получаемых персональных данных при автоматизированной обработке на средствах вычислительной техники, участвующих в реализации процедуры деобезличивания и обработке деобезличенных данных;

- обеспечить обработку и защиту деобезличенных данных в соответствии с требованиями Федерального закона от 26 июня 2006 г. № 152-ФЗ «О персональных данных».

## **6. РЕКОМЕНДАЦИИ ПО ВЫБОРУ МЕТОДОВ ОБЕЗЛИЧИВАНИЯ**

6.1 При выборе методов и процедур обезличивания следует руководствоваться целями и задачами обработки персональных данных.

6.2 Обезличивание персональных данных, обработка которых осуществляется с разными целями, может осуществляться разными методами.

6.3 Возможно объединение различных методов обезличивания в одну процедуру.

6.4 При выборе метода и процедуры обезличивания следует учитывать:

- объем персональных данных, подлежащих обезличиванию;
- форму представления данных;
- область обработки обезличенных данных;
- способы хранения обезличенных данных;
- применяемые меры по обеспечению безопасности данных.

6.5 В Таблице 2 приведены рекомендации по выбору метода обезличивания в зависимости от класса решаемых задач.

Таблица 2 – Сопоставление задач обработки методам обезличивания

Класс задач	Задачи обработки	Метод обезличивания
Статистическая обработка и статистические исследования персональных данных	– осуществление обработки по заявленным параметрам; – проведение исследований по заданным параметрам субъектов.	– перемешивание; – декомпозиция; – изменение состава или семантики.
Сбор и хранение персональных данных	– внесение персональных данных субъектов в информационную систему на основе анкет, заявлений и прочих документов.	– перемешивание; – декомпозиция; – введение идентификаторов.
Обработка поисковых запросов (поиск данных о субъектах и поиск субъектов по известным данным)	– поиск информации о субъектах; – печать и выдача субъектам документов в установленной форме, содержащих персональные данные; – выдача справок, выписок, уведомлений по запросам субъектов или уполномоченных органов.	– перемешивание; – декомпозиция; – введение идентификаторов.
Актуализация персональных данных	– внесение изменений в существующие записи о субъектах на основе обращений субъектов, решений судов и других уполномоченных органов; – внесение изменений в существующие записи о субъектах на основе исследований, выполнения своих функций или требований законодательства РФ.	– перемешивание; – декомпозиция; – введение идентификаторов.
Интеграция данных	– поиск информации о субъектах; – передача данных смежным организациям.	– перемешивание; – декомпозиция; – введение идентификаторов.
Ведение учета субъектов персональных данных	– прием анкет, заявлений;	– перемешивание; – декомпозиция;

	– ведение учета персональных данных в соответствии с функциями органа.	– введение идентификаторов.
--	--	-----------------------------

ПРИЛОЖЕНИЕ № 5  
Утверждено  
распоряжением администрации  
Алексеевского городского округа  
от «05» февраля 2019 г. № 118-р

## Правила рассмотрения запросов субъектов персональных данных и их представителей

### 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) регулируют отношения, возникающие при выполнении администрации Алексеевского городского округа (далее – Учреждение) обязательств, определенных требованиями ст. 14, ст. 20, ст. 21 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.2 Настоящие Правила распространяются на действия Учреждения при получении запроса от субъектов персональных данных или их законных представителей и уполномоченного органа по защите прав субъектов персональных данных. Эти действия направлены на определение порядка учета (регистрации), рассмотрения запросов, а также на подтверждение наличия, ознакомления, уточнения, уничтожения персональных данных или отзыв согласия на обработку персональных данных, а также на устранение нарушений законодательства, допущенных при обработке.

1.3 Настоящие Правила разработаны в соответствии с Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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».

### 2. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ

2.1 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных в соответствии с частью 7 ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2.2 Субъект персональных данных вправе требовать от Учреждения 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, а также принимать предусмотренные законом меры по защите своих прав.

2.3 Запрос субъекта персональных данных должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Учреждением, либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением, подпись субъекта персональных данных. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

2.4 Сведения, указанные в части 7 ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», предоставляются субъекту персональных данных Учреждением при получении запроса от субъекта персональных данных. Они должны быть предоставлены в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

2.5 Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 7 ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2.6 В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

2.7 В случае подачи субъектом персональных данных повторного запроса, в целях получения сведений, указанных в части 7 ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», необходимо руководствоваться частями 4 и 5 ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Повторный запрос наряду со сведениями, указанными в п. 2.3 настоящих Правил, должен содержать обоснование направления повторного запроса.

2.8 Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Отказ должен быть мотивированным.

2.7 Рассмотрение запросов является должностной обязанностью сотрудников, в чьи обязанности входит обработка персональных данных.

2.9 Должно обеспечиваться:



- объективное, всестороннее и своевременное рассмотрения запроса;
- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

- направление письменных ответов по существу запроса.

2.10 Все поступившие запросы регистрируются в день их поступления в «Журнале учета обращений субъектов персональных данных и их законных представителей». На запросе проставляется входящий номер и дата регистрации.

2.11 Ответы на запросы печатаются на бланке установленной формы и регистрируются за теми же номерами, что и запросы.

2.12 Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и заявителю даны исчерпывающие ответы.

### **3. ПОРЯДОК РАССМОТРЕНИЯ ЗАПРОСОВ**

3.1 При поступлении запроса субъекта персональных данных на наличие персональных данных необходимо в течение 30 дней с даты получения запроса подтвердить, в случае осуществления, обработку персональных данных.

3.2 При поступлении запроса субъекта персональных данных на ознакомление с его персональными данными необходимо в течение 30 дней с даты получения запроса предоставить их для ознакомления.

3.3 При поступлении запроса субъекта персональных данных или его представителя на уточнение персональных данных необходимо внести в них необходимые изменения в срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение обязано внести в них необходимые изменения. При этом Учреждение уведомляет субъекта персональных данных или его представителя о внесенных изменениях и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.4 При поступлении запроса субъекта персональных данных или его представителя на уничтожение персональных данных необходимо в срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уничтожить такие персональные данные. При этом Учреждение уведомляет субъекта персональных данных или его представителя о предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.5 При получении запроса на отзыв согласия субъекта персональных данных на обработку его персональных данных необходимо прекратить их обработку или обеспечить прекращение такой обработки (если обработка

персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

3.6 При выявлении неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц. В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в течение 7 рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.7 При выявлении неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий 3 рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения. В случае, если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или

его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.8 При поступлении запроса от уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано сообщить необходимую информацию в течение 30 дней с даты получения такого запроса.

#### **4. ОТВЕТСТВЕННОСТЬ**

4.1 Нарушение установленного порядка рассмотрения запросов влечет гражданскую, уголовную, административную и иную, предусмотренную законодательством Российской Федерации, ответственность.

4.2 За неисполнение или ненадлежащее исполнение сотрудниками Учреждения возложенных на них обязанностей по соблюдению установленного порядка рассмотрения запросов Учреждение вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

**ПРИЛОЖЕНИЕ № 1**  
**к Правилам рассмотрения запросов**  
**субъектов персональных данных и их**  
**представителей**

**Бланк предоставления сведений по запросу субъектов персональных данных**

Кому: \_\_\_\_\_

Адрес: \_\_\_\_\_

\_\_\_\_\_

Ответ на запрос от «\_\_» \_\_\_\_\_ 20\_\_ г.

Администрация Алексеевского городского округа подтверждает обработку следующих персональных данных:

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Персональные данные получены от: \_\_\_\_\_

\_\_\_\_\_

Цель обработки персональных данных: \_\_\_\_\_

\_\_\_\_\_

Способы обработки персональных данных: \_\_\_\_\_

\_\_\_\_\_

Срок обработки и хранения персональных данных: \_\_\_\_\_

\_\_\_\_\_

Документ выдал:

\_\_\_\_\_

(дата)

(подпись)

(Ф.И.О.)

**ПРИЛОЖЕНИЕ № 2**  
**к Правилам рассмотрения запросов**  
**субъектов персональных данных и их**  
**представителей**

**Бланк ответа на запрос в случае, если персональные данные субъекта не  
обрабатываются**

Кому: \_\_\_\_\_

Адрес: \_\_\_\_\_

\_\_\_\_\_

Ответ на запрос от «\_\_» \_\_\_\_\_ 20\_\_ г.

Уведомляем вас, что администрация Алексеевского городского округа не осуществляет обработку Ваших персональных данных.

Документ выдал:

\_\_\_\_\_  
(дата)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(Ф.И.О.)

## ПРИЛОЖЕНИЕ № 6

Утверждено  
 распоряжением администрации  
 Алексеевского городского округа  
 от «05» *сентября* 2021 г. № *118-р*

Правила оценки возможного вреда субъектам персональных данных и  
 соотнесения указанного вреда с принимаемыми мерами

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие правила оценки возможного вреда субъектам персональных данных и соотнесения указанного вреда с принимаемыми мерами (далее - Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон), и отражают соотношение указанного возможного вреда и принимаемых администрацией Алексеевского городского округа (далее - Учреждение) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

## 2. МЕТОДИКА ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА

2.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

- неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;

- неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;

- неправомерное изменение персональных данных является нарушением целостности персональных данных;

- нарушение права субъекта требовать от Учреждения уточнения его персональных данных, их блокирования или уничтожения является нарушением целостности информации;

- нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности

персональных данных;

- обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;

- неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;

- принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

2.3. Субъекту персональных данных может быть причинён вред в форме:

- убытков - расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

- морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

2.4. В оценке возможного вреда Учреждение исходит из следующего способа учёта последствий допущенного нарушения принципов обработки персональных данных:

- низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

- средний уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;

- высокий уровень возможного вреда - во всех остальных случаях.

### **3. ПОРЯДОК ПРОВЕДЕНИЯ ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА, А ТАКЖЕ СООТНЕСЕНИЯ ВОЗМОЖНОГО ВРЕДА И РЕАЛИЗУЕМЫХ МЕР**

3.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным за организацию обработки персональных данных, или комиссией в соответствии с методикой, описанной в разделе 2 настоящих Правил, и на основании экспертных значений, приведённых в Приложении 1.

3.2. Состав реализуемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом, определяется лицом, ответственным за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных в Приложении 1 мер.

3.3. По результатам оценки оформляется акт. Форма акта приведена в Приложении 2.



**ПРИЛОЖЕНИЕ № 1**  
к Правилам оценки возможного вреда  
субъектам персональных данных и  
соотнесения указанного вреда с  
принимаемыми мерами

Методика оценки вреда, который может быть причинен субъектам  
персональных данных, а также соотнесение возможного вреда и реализуемых  
мер

№ п/п	Требования, которые могут быть нарушены	Возможные нарушение безопасности информации и причинённый субъекту вред		Уровень возможного вреда	Принимаемые меры
1.	Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей (часть 2 статьи 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» - далее - Федеральный закон)	Убытки и моральный вред	+	Высокий	Определены цели обработки.
Целостность					
Доступность					
Конфиденциальность		+			
2.	Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой (часть 3 статьи 5 Федерального закона)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
Целостность					
Доступность					
Конфиденциальность		+			
3.	Обработке подлежат только персональные данные, которые отвечают целям их обработки (часть 4 статьи 5 Федерального закона)	Убытки и моральный вред	+	Высокий	Утвержден перечень обрабатываемых персональных данных.
Целостность					
Доступность					
Конфиденциальность		+			
4.	Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки (часть 5 статьи 5 Федерального закона)	Убытки и моральный вред	+		Определены цели обработки и перечень обрабатываемых персональных данных.
Целостность					
Доступность					
Конфиденциальность		+			
5.	При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных (часть	Убытки и моральный вред		Низкий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
Целостность		+			

	6 статьи 5 Федерального закона)	Доступность			
		Конфиденциальность			
6.	Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных (часть 7 статьи 5 Федерального закона)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
7.	Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
		Целостность			
		Доступность			

	Федерального закона (часть 3 статьи 6 Федерального закона)	Конфиденциальность	+		
8.	Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом (статья 7 Федерального закона)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных.  Соответствующие нормы закреплены в договорах, регламентирующих правоотношения с третьими лицами.
		Целостность			
		Доступность			
		Конфиденциальность	+		
9.	В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных (часть 1 статьи 8 Федерального закона)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
10.	Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на	Убытки и моральный вред	+	Высокий	Согласия субъектов на обработку их персональных данных фиксируются надлежащим образом, позволяющим подтвердить факт их
		Целостность			

	обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом (часть 1 статьи 9 Федерального закона)	Доступность			получения
		Конфиденциальность	+		
11.	Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона (часть 8 статьи 9 Федерального закона)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
12.	Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи (часть 1 статьи 10 Федерального закона)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных, а также в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
13.	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных, а также в Положении об обработке персональных данных.
		Целостность			
		Доступность			

	данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи (часть 1 статьи 11 Федерального закона)	Конфиденциальность	+		
14.	Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных (часть 3 статьи 12 Федерального закона)	Убытки и моральный вред	+	Высокий	Трансграничная передача персональных данных не осуществляется
		Целостность			
		Доступность	+		
		Конфиденциальность	+		
15.	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, а также принимать предусмотренные законом меры по защите своих прав (часть 1 статьи 14 Федерального закона)	Убытки и моральный вред	+	Средний	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных, а также в Положении об обработке персональных данных.
		Целостность	+		
		Доступность			
		Конфиденциальность			
16.	Субъект персональных данных имеет право на получение информации, касающейся обработки его	Убытки и моральный вред	+	Средний	Соответствующие нормы закреплены в Положении об обработке
		Целостность			
		Доступность	+		

	персональных данных (часть 7 статьи 14 Федерального закона)	Конфиденциальность			персональных данных.
17.	Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных (часть 2 статьи 16 Федерального закона)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных, а также в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		

**ПРИЛОЖЕНИЕ № 2**  
к Правилам оценки возможного вреда  
субъектам персональных данных и  
соотнесения указанного вреда с  
принимаемыми мерами

Типовая форма акта оценки возможного вреда субъектам персональных данных

«\_\_» \_\_\_\_\_ 20\_\_ г.

г. Алексеевка

№ \_\_\_\_\_

Комиссия в составе:

председатель комиссии

\_\_\_\_\_  
(Ф.И.О., должность)

члены комиссии

\_\_\_\_\_  
(Ф.И.О., должность)

\_\_\_\_\_  
(Ф.И.О., должность)

провела оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения администрацией Алексеевского городского округа обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, определила, что на основе возможных нарушений безопасности информации, уровня возможного вреда, в случае нарушения, а также соотнесении указанного вреда с принимаемыми мерами, субъектам персональных данных может быть причинен вред, который оценивает как

\_\_\_\_\_  
(уровень вреда)

Председатель комиссии:

\_\_\_\_\_  
(должность)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(Ф.И.О.)

Члены комиссии:

\_\_\_\_\_  
(должность)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(Ф.И.О.)

\_\_\_\_\_  
(должность)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(Ф.И.О.)