КЕМЕРОВСКАЯ ОБЛАСТЬ

ФИНАНСОВОЕ УПРАВЛЕНИЕ ГОРОДА КАЛТАН

П Р И К А З

|  |
| --- |
|  |

01.10.2018г. г. Калтан № 26

О реализации требований Постановления Правительства Российской Федерации от 21 марта 2012 г. N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

В целях организации работы по обработке персональных данных в финансовом управлении города Калтан, руководствуясь Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21 марта 2012 г. N 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» приказываю:

1. Утвердить и ввести в действие:

1.1. [Правила](#P53) 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 № 1);

1.2. [Правила](#P152) рассмотрения запросов субъектов персональных данных или их представителей (Приложение № 2);

1.3. [Правила](#P571) 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 (Приложение № 3);

1.4. План внутренних проверок состояния защиты персональных данных, обрабатываемых в финансовом управлении города Калтан (Приложение № 4);

1.5. [Правила](#P671) работы с обезличенными персональными данными совместно с Перечнем должностей финансового управления города Калтан, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (Приложение № 5);

1.6. [Перечень](#P745) информационных систем персональных данных, обрабатываемых в финансовом управлении города Калтан (Приложение № 6)

1.7. [Перечень](#P764) должностей финансового управления города Калтан, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, включая доступ в информационных системах (Приложение № 7);

1.8. Перечень лиц, доступ которых к персональным данным, обрабатываемых в информационной системе, необходим для выполнения ими служебных обязанностей (Приложение № 8);

1.9. Перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ (Приложение № 9)

1.10. Должностную [инструкцию](#P799), ответственного за организацию обработки персональных данных (Приложение № 10);

1.11. Должностную инструкцию лица, участвующего в обработке персональных данных (Приложение № 11);

1.12. Должностную инструкцию специалиста АСФР по обеспечению безопасности информационных систем персональных данных (Приложение № 12);

1.13. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации информационных систем персональных данных в финансовом управлении города Калтан (Приложение № 13);

1.14. Инструкцию по организации антивирусной защиты информационных систем персональных данных в финансовом управлении города Калтан (Приложение № 14);

1.15. Инструкцию по обеспечению безопасности информационных систем персональных данных (парольная защита в ИСПДн) в финансовом управлении города Калтан (Приложение № 15);

1.16. [Обязательство](#P833) о неразглашении информации, содержащей персональные данные (Приложение № 16);

1.17. [Форму](#P869) согласия на обработку персональных данных (Приложение № 17);

1.18. [Форму](#P1064) разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (Приложение № 18);

1.19. Форму Согласия на передачу персональных данных третьим лицам (Приложение № 19);

1.20. Перечень помещений, предназначенных для обработки персональных данных (Приложение № 20);

1.21. Перечень сотрудников, допущенных в помещения, предназначенные для обработки персональных данных (Приложение № 21);

1.22. Порядок доступа служащих финансового управления города Калтан в помещения, предназначенные для обработки персональных данных (Приложение № 22);

1.23. Порядок и места хранения персональных данных (материальных носителей) а так же перечень лиц, ответственных за сохранность персональных данных (Приложение № 23);

## 1.24. Журнал учета хранилищ, металлических шкафов и ключей от них (Приложение № 24);

1.25. Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (Приложение № 25);

1.26. Журнал учета средств защиты информации (Приложение № 26);

1.27. Журнал учета машинных носителей персональных данных (Приложение № 27);

1.28. Лист ознакомления с положениями законодательства РФ о персональных данных и с требованиями к защите персональных данных (Приложение № 28);

1.29. Лист ознакомления сотрудников о факте обработки ими персональных данных (Приложение № 29)

2. Главному специалисту АСФР разместить настоящий приказ на официальном сайте администрации Калтанского городского округа.

3. Приказ вступает в силу с момента подписания.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник финансового

управления города Калтан В.П. Чушкина

Приложение № 1

к приказу финансового управления

города Калтан

от «01»октября 2018 г. № 26

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. Настоящими Правилами обработки персональных данных (далее - Правила) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; содержание обрабатываемых персональных данных для каждой цели обработки персональных данных; категории субъектов, персональные данные которых обрабатываются; сроки обработки и хранения; порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2. Настоящие Правила разработаны в соответствии с Трудовым кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27 июля 2004 г. N 79-ФЗ "О государственной гражданской службе Российской Федерации", Федеральным законом от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции", Указом Президента Российской Федерации от 1 февраля 2005 г. N 112 "Об утверждении Положения о конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации", Указом Президента Российской Федерации от 30 мая 2005 г. N 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации иведении его личного дела", постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", постановлением Правительства Российской Федерации от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", постановлением Правительства Российской Федерации от 21 марта 2012 г. N 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".

3. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

5. Обработке подлежат только персональные данные, которые отвечают целям их обработки:

- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

- число, месяц, год рождения;

- место рождения;

- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

- адрес места жительства (адрес регистрации, фактического проживания);

- номер контактного телефона или сведения о других способах связи;

- реквизиты страхового свидетельства государственного пенсионного страхования;

- идентификационный номер налогоплательщика;

- реквизиты страхового медицинского полиса обязательного медицинского страхования;

- реквизиты свидетельства государственной регистрации актов гражданского состояния;

- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

- сведения о трудовой деятельности;

- сведения о воинском учете и реквизиты документов воинского учета;

- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

- сведения об ученой степени;

- информация о владении иностранными языками, степень владения;

- медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;

- фотография;

- сведения о прохождении государственной гражданской службы, в том числе: дата, основания поступления на государственную гражданскую службу и назначения на должность государственной гражданской службы, дата, основания назначения, перевода, перемещения на иную должность государственной гражданской службы, наименование замещаемых должностей государственной гражданской службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности государственной гражданской службы, а также сведения о прежнем месте работы;

- информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту;

- сведения о пребывании за границей;

- информация о классном чине государственной гражданской службы Кемеровской области;

- информация о наличии или отсутствии судимости;

- информация об оформленных допусках к государственной тайне;

- государственные награды, иные награды и знаки отличия;

- сведения о профессиональной переподготовке и (или) повышении квалификации;

- информация о ежегодных оплачиваемых отпусках, учебных отпусках, отпусках по временной нетрудоспособности и отпусках без сохранения денежного содержания;

- сведения о доходах, об имуществе и обязательствах имущественного характера (в том числе членов семьи);

- номер расчетного счета;

- номер банковской карты;

- иные персональные данные, необходимые для достижения целей.

6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

7. Субъект персональных данных имеет право на получение сведений, указанных в статье 14 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

Субъект персональных данных вправе требовать от представителя нанимателя 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.

Сведения, указанные в части 7 статьи 14 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", должны быть предоставлены субъекту персональных данных представителем нанимателя 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.

Сведения, указанные в части 7 статьи 14 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", предоставляются субъекту персональных данных или его представителю организацией при обращении либо при получении запроса субъекта персональных данных или его представителя в тридцатидневный срок. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его 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 представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и ознакомления с такими персональными данными осуществляется не ранее чем через 30 (тридцать дней) после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

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 организация обязана дать в письменной форме мотивированный ответ в срок, не превышающий 30 (тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

8. Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме сотрудника, являющегося субъектом персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации о противодействии коррупции, о государственной службе, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию и другими нормативными правовыми актами Российской Федерации.

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

9. На основе персональных данных гражданских служащих в организации формируется и ведется, в том числе на электронных носителях, реестр гражданских служащих.

10. Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера гражданского служащего, его супруги (супруга) и несовершеннолетних детей в соответствии с законодательством о государственной гражданской службе в Российской Федерации размещаются на официальном сайте организации.

11. 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.

Государственный гражданский служащий, ответственный за осуществление обработки персональных данных в организации должен принимать необходимые меры по удалению или уточнению неполных или неточных персональных данных.

12. Мерами, направленными на выявление и предотвращение нарушений, предусмотренных законодательством, являются:

1) осуществление внутреннего контроля соответствия обработки персональных данных нормам Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" (далее - Федеральный закон) и принятыми в соответствии с ним нормативными правовыми актами;

2) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых организацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

3) ознакомление государственных гражданских служащих организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение государственных гражданских служащих организации.

13. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) проведением в установленном порядке процедуры оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер по их недопущению;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

14. Целями обработки персональных данных являются:

1) обеспечение соблюдения законов и иных нормативных правовых актов;

2) использование персональных данных в уставной деятельности с применением средств автоматизации или без таких средств, включая хранение этих данных в архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним;

3) заполнение базы данных автоматизированной информационной системы в целях повышения эффективности и быстрого поиска, проведения мониторинговых исследований, формирования статистических и аналитических отчетов в вышестоящие органы.

15. 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 является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

16. В случае выявления неправомерной обработки персональных данных, ответственным за осуществление обработки персональных данных, в срок, не превышающий 3 (три) рабочих дня с даты этого выявления, он обязан прекратить неправомерную обработку персональных данных.

В случае, если обеспечить правомерность обработки персональных данных невозможно, ответственный за осуществление обработки персональных данных в срок, не превышающий 10 (десять) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных, ответственный за осуществление обработки персональных данных обязан уведомить субъект 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.

17. В случае достижения цели обработки персональных данных, ответственный за осуществление обработки персональных данных, обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 (тридцать) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между руководителем и субъектом персональных данных, либо если руководитель не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

18. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных государственный гражданский служащий, ответственный за осуществление обработки персональных данных, обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 3 (три) рабочих дня с даты поступления указанного отзыва, если иное не предусмотрено соглашением между руководителем и субъектом персональных данных.

Об уничтожении персональных данных государственный гражданский служащий, ответственный за осуществление обработки персональных данных в организации, обязан уведомить субъект персональных данных не позднее 3 (трех) рабочих дней со дня уничтожения.

19. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, государственный гражданский служащий, ответственный за осуществление обработки персональных данных в организации, осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок, не превышающий 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

Приложение N 2

к приказу финансового управления

города Калтан

от 1 октября 2018г. N 26

Правила

рассмотрения запросов субъектов персональных данных

или их представителей

1. Общие положения

1. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Федеральный закон), Трудовым кодексом Российской Федерации и определяют порядок обработки поступающих в финансовое управление города Калтан обращений субъектов персональных данных.

2. Права субъектов персональных данных

2.1. В соответствии с действующим законодательством субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;

- правовые основания и цели обработки персональных данных;

- цели и применяемые способы обработки персональных данных;

- наименование и место нахождения организации, сведения о лицах, которые имеют доступ к персональным данным или которыми могут быть раскрыты персональные данные на основании договора на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

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

- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

- информацию обосуществленной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению руководителя, если обработка поручена или будет поручена такому лицу;

- иные сведения, предусмотренные Федеральным законом или другими нормативными правовыми актами РФ.

2.2. Право субъекта персональных данных на доступ к его персональным данным ограничивается в соответствии с федеральными законами, в том числе в случаях, предусмотренных частью 8 статьи 14 Федерального закона.

2.3. 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. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

2.4. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3. Порядок работы с запросами, уведомлениями и иными

обращениями субъектов персональных данных

или их представителей

3.1. При поступлении запроса, уведомления или иного обращения субъекта персональных данных или его представителя, уполномоченными должностными лицами оператора осуществляется его регистрация в журнале регистрации и учета обращений субъектов персональных данных (Приложение 13 к Правилам).

3.2. Уполномоченные должностные лица оператора обязаны сообщить в порядке, предусмотренном статьей 14 Федерального закона N 152-ФЗ, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

3.3. 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 уполномоченные должностные лица оператора обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного нормативного правового акта РФ, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3.4. Уполномоченные должностные лица оператора обязаны предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица оператора обеспечивают внесение в них необходимых изменений.

В срок, не превышающий 7 (семи) 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, уполномоченные должностные лица оператора обязаны уничтожить такие персональные данные и уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах, принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.5. Уполномоченные должностные лица оператора обязаны сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

3.6. Документальное оформление работы с запросами, уведомлениями и иными обращениями субъектов персональных данных и их представителей осуществляется в соответствии с формами, приведенными в [приложениях 1](#P202) - 12 к настоящим Правилам.

3.7. Во всем ином, что не урегулировано настоящими Правилами, при работе с запросами, уведомлениями и иными обращениями по вопросам обработки персональных данных уполномоченные должностные лица оператора руководствуются действующим законодательством Российской Федерации.

Приложение 1

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

 В \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать уполномоченный орган)

Уведомление об уничтожении

(примерная форма)

 Настоящим уведомлением сообщаем вам, что в связи с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

персональные данные\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать персональные данные)

уничтожены.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 2

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

 В \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать уполномоченный орган)

Уведомление об устранении допущенных нарушений

(примерная форма)

 Настоящим уведомлением сообщаем вам, что допущенные нарушения приобработке персональных данных, а именно:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указать допущенные нарушения)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ устранены.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 3

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Запрос

(примерная форма)

Уважаемый(ая)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О.),

в связи с\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

у оператора возникла необходимость получения следующей информации,составляющей Ваши персональные данные \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(перечислить информацию)

Просим Вас предоставить указанные сведения в течение \_\_\_\_\_\_\_\_\_\_ рабочихдней с момента получения настоящего запроса.

В случае невозможности предоставить указанные сведения просим вуказанный срок дать письменное согласие на получение нами необходимойинформации из следующих источников \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

следующими способами\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

По результатам обработки указанной информации нами планируется принятиеследующих решений, которые будут доведены до Вашего сведения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Против принятого решения Вы имеете право заявить свои письменные

возражения в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ срок.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 4

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Уведомление о блокировании

(примерная форма)

Уважаемый(ая)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О.),

в связи с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ сообщаю Вам, что Ваши персональные данные \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать персональные данные)

заблокированы на срок\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 5

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Уведомление об уточнении

(примерная форма)

Уважаемый(ая)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О.),

в связи с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

сообщаем Вам, что Ваши персональные данные уточнены в соответствии

со сведениями: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 6

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Уведомление

(примерная форма)

Уважаемый(ая)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О.),

оператором производится обработка сведений, составляющих Ваши персональные данные: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(указать сведения)

Цели обработки: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Способы обработки: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 Перечень лиц, которые имеют доступ к информации, содержащей Вашиперсональные данные или могут получить такой доступ:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N | Должность | Ф.И.О. | Вид доступа | Примечания |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

По результатам обработки указанной информации нами планируется принятием следующих решений, которые будут доведены до Вашего сведения:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 Против принятого решения Вы имеете право заявить свои письменныевозражения в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ срок.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 7

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Уведомление об уничтожении

(примерная форма)

Уважаемый(ая)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О.),

в связи с\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

сообщаем Вам, что Ваши персональные данные \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать персональные данные)

уничтожены.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 8

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Уведомление об устранении допущенных нарушений

(примерная форма)

Уважаемый(ая)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О.),

в связи с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

сообщаем Вам, что все допущенные нарушения при обработке Ваших персональныхданных устранены.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 9

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Начальнику финансового управления

города Калтан

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Заявление

(примерная форма)

 Прошу заблокировать обрабатываемые Вами мои персональные данные:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать блокируемые персональные данные)

на срок: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать срок блокирования)

в связи с тем, что \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать причину блокирования персональных данных)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 10

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Начальнику финансового управления

города Калтан

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Заявление

(примерная форма)

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, указать цели, способы и сроки ее обработки, предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ), сведения о том, какие юридические последствия для меня может повлечь ее обработка.

В случае отсутствия такой информации прошу Вас уведомить меня об этом.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 11

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Начальнику финансового управления

города Калтан

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Заявление

(примерная форма)

 Прошу уничтожить обрабатываемые Вами мои персональные данные:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать уничтожаемые персональные данные)

в связи с тем, что \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать причину уничтожения персональных данных)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 12

к Правилам рассмотрения

запросов субъектов персональных

данных или их представителей

Начальнику финансового управления

города Калтан

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Заявление

(примерная форма)

 Прошу уточнить обрабатываемые Вами мои персональные данные в

соответствии со сведениями: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать уточненные персональные данные заявителя)

в связи с тем, что \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать причину уточнения персональных данных)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) ( Ф.И.О.)

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 13

К правилам рассмотрения

запросов субъектов персональных

данных или их представителей

# Журнал

**учета обращений субъектов персональных данных по вопросам обработки их ПДн в ИСПДн**

 Начат «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_г. На \_\_\_\_\_\_ листах

 Окончен «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_г.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 *ФИО, должность ответственного за организацию хранения и ведения подпись*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№** **п/п**  | **Дата обращения** | **Сведения о запрашивающемлице** | **Краткоесодержаниеобращения** | **Отметка о предоставлении или отказе в****предоставленииинформации****(предоставлено/ отказано)**  | **Дата передачи/отказа в предоставлении информации**  | **ФИО/Подпись запрашивающеголица** | **ФИО/Подпись ответственногоработника** |
| ***1***  | ***2***  | ***3***  | ***4***  | ***5***  | ***6***  | ***7***  | ***8***  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Приложение N 3

к приказу финансового управления

города Калтан

от 1 октября 2018г. № 26

Правила

осуществления внутреннего контроля соответствия

обработки персональных данных требования к защите персональных данных, установленных Федеральным законом

"О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора

1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с Федеральным закономот 27.07.2006 N 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 21.03.2012 N 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 определяют порядок осуществления организации 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.

2. Тематика внутреннего контроля

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

- соответствие полномочий пользователя матрице доступа;

- соблюдение пользователями информационных систем персональных данных (далее - ИСПД) оператором парольной политики;

- соблюдение пользователями ИСПД в организации антивирусной политики;

- соблюдение пользователями ИСПД оператора правил работы со съемными носителями персональных данных;

- соблюдение ответственными за криптографические средства защиты информации правил работы с ними;

- соблюдение порядка доступа в помещения оператора, где расположены элементы ИСПД;

- соблюдение порядка резервирования баз данных и хранения резервных копий;

- соблюдение порядка работы со средствами защиты информации;

- знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

- хранение бумажных носителей с персональными данными;

- доступ к бумажным носителям с персональными данными;

- доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

3. Порядок проведения внутренних проверок

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, указанным в [пункте 1.2](#P581) настоящих Правил, в финансовом управлении города Калтан организуется проведение периодических проверок условий обработки персональных данных в соответствии с Планом внутренних проверок условий обработки персональных данных в организации, а также внеплановых проверок условий обработки персональных данных.

3.2. Проверки осуществляются ответственным за организацию обработки персональных данных лицом (далее - Ответственное лицо) либо комиссией, образуемой по указанию руководителя организации (далее - комиссия).

3.3. Внеплановые проверки проводятся в случае поступления оператору сведений об имеющихся нарушениях при осуществлении обработки персональных данных.

3.4. Проверки осуществляются ответственным лицом (комиссией) непосредственно на месте обработки персональных данных путем опроса сотрудников, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных, а в иных формах в соответствии с действующим законодательством.

3.5. Для каждой проверки составляется Протокол проведения внутренней проверки условий обработки персональных данных в организации (далее - Протокол). Форма Протокола приведена в приложении 1 к настоящим Правилам.

3.6. При выявлении в ходе проверки нарушений ответственным лицом в Протоколе делается запись о необходимых мероприятиях по устранению выявленных нарушений и сроках их устранения.

3.7. Протоколы хранятся у ответственного лица в течение текущего года. Уничтожение Протоколов обеспечивается ответственным лицом самостоятельно в январе года, следующего за проверочным.

3.8. О результатах проверки и мерах, необходимых для устранения нарушений, докладывается руководителю организации ответственным.

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

Протокол

проведения внутренней проверки условий обработки

персональных данных

Настоящий Протокол составлен в том, что "\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

ответственным за организацию обработки персональных данных проведена проверка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 (тема проверки)

 Проверка осуществлялась в соответствии с требованиями

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 В ходе проверки проверено:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок устранения нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Должность ответственного \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_И.О. Фамилия

Должность проверяемого лица \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_И.О. Фамилия

Приложение № 4

к приказу финансового управления

города Калтан

от 1 октября 2018г. № 26

**План внутренних проверок**

 **состояния защиты персональных данных, обрабатываемых в финансовом управлении города Калтан**

|  |  |  |
| --- | --- | --- |
| Мероприятие | Периодичность | Исполнитель |
| Порядок и условия хранения бумажных носителей, содержащих персональные данные | Еженедельно | Начальник управленияОтветственный за организацию обработки персональных данных |
| Соблюдение правил доступа к бумажным носителям с персональными данными | Еженедельно | Начальник управленияОтветственный за организацию обработки персональных данных |
| Соблюдение условий доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными, а также в помещения, где размещены ИСПДн | Еженедельно | Начальник управленияОтветственный за организацию обработки персональных данных |
| Соблюдение режима обработки ПДн | Еженедельно | Начальник управленияОтветственный за организацию обработки персональных данных |
| Соблюдение режима защиты | Ежедневно | Главный специалист АСФР |
| Соблюдение требований антивирусной защиты | Еженедельно | Главный специалист АСФР |
| Соблюдение режима защиты при подключении к сетям общего пользования | Еженедельно | Главный специалист АСФР |
| Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн | Ежегодно | Главный специалист АСФР |
| Контроль за внесением изменений в [программное обеспечение](https://pandia.ru/text/category/programmnoe_obespechenie/), за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн | Еженедельно | Главный специалист АСФР |
| Контроль за обеспечением резервного копирования | Ежемесячно | Главный специалист АСФР |
| Соблюдение правил работы со съемными носителями персональных данных | Еженедельно | Начальник управленияГлавный специалист АСФР |
| Своевременность проведения мероприятий по обезличиванию персональных данных | Ежемесячно | Начальник управленияЗаместительНачальники отделовГлавный специалист АСФРОтветственный за организацию обработки персональных данных |
| Своевременность проведения мероприятий по уничтожению персональных данных | Ежемесячно | Начальник управленияЗаместительНачальники отделовГлавный специалист АСФРОтветственный за организацию обработки персональных данных |
| Своевременность мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним | Ежемесячно | Ответственный за организацию обработки персональных данных |
| Своевременность и эффективность проведенных дополнительных мероприятий по обеспечению безопасности ПДн. | Ежемесячно | Ответственный за организацию обработки персональных данных |
| Соответствие используемых Пользователями ИСПДн полномочий параметрам (матрице) доступа | Еженедельно | Главный специалист АСФР |
| Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз | Ежегодно |  Главный специалист АСФР |
| Поддержание в актуальном состоянии нормативно-организационных документов | Ежемесячно | Главный специалист АСФРОтветственный за организацию обработки персональных данных |
| Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных | 1 раз в три года | Начальник управления |
| Ведение журнала внутренних проверок и поддержание его в актуальном состоянии(Приложение к плану внутренних проверок) | Ежемесячно | Ответственный за организацию обработки персональных данных |

Приложение
к Плану внутренних проверок режима защиты персональных
данных в финансовом управлении города Калтан

## Журнал учета мероприятий по контролю

## за соблюдением режима защиты персональных данных

Журнал начат "\_\_\_" \_\_\_\_\_\_\_ 20\_\_ г.

Журнал завершен "\_\_\_" \_\_\_\_\_\_\_ 20\_\_ г.

Ответственный за заполнение: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Общие положения**

В настоящем журнале отмечаются мероприятия в соответствии с Планом внутренних проверок режима защиты персональных данных, носящих периодический характер.

В настоящий журнал заносится следующая информация:
- название проведенного мероприятия;
- дата проведенного мероприятия;
- исполнитель мероприятия;
- результат (отчет, действия) мероприятия (при необходимости).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| N п/п | Мероприятие | Дата | Исполнитель | Результат |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Приложение N 5

к приказу финансового управления

города Калтан

от 1 октября 2018г. № 26

Правила

работы с обезличенными персональными данными

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными в Федеральном агентстве по техническому регулированию и метрологии разработаны в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 21.03.2012 N 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 определяют порядок работы с обезличенными персональными данными.

1.3. Термины "персональные данные", "обработка персональных данных", "обезличивание персональных данных" используются в настоящих Правилах в значениях, определенных Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Федеральный закон).

2. Условия обезличивания

2.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных служащих организации и по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

2.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;

- замена части сведений идентификаторами;

- обобщение - понижение точности некоторых сведений;

- понижение точности некоторых сведений (например, "Место жительства" может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

- деление сведений на части и обработка в разных информационных системах;

- другие способы.

2.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

2.4. [Перечень](#P719) должностей финансового управления города Калтан, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в Приложении 1 к настоящим Правилам.

2.5. Начальник или Заместитель руководителя финансового управления города Калтанпринимают решение о необходимости обезличивания персональных данных.

2.6. Начальники структурных подразделений финансового управления города Калтан, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

2.7. Служащие финансового управления города Калтан, обслуживающие базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

3. Порядок работы с обезличенными персональными данными

3.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

3.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;

- антивирусной политики;

- правил работы со съемными носителями (если они используются);

- правил резервного копирования;

- правил доступа в помещения, где расположены элементы информационных систем.

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;

- правил доступа к ним и в помещения, где они хранятся.

Приложение 1

к Правилам работы с обезличенными

персональными данными

**Перечень должностей финансового управления города Калтан, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных**

1. Начальник управления;

2. Заместители руководителя – начальник бюджетного отдела;

3. Начальник отдела доходов;

4. Заместитель начальника отдела доходов;

5. Начальник отдела бухгалтерского учета и отчетности -главный бухгалтер;

6. Главный специалистотдела бухгалтерского учета и отчетности;

7. Главный специалист АСФР;

8. Главный специалист – юрисконсульт;

9. Главный специалист отдела доходов.

Приложение N 6

к приказу финансового управления

города Калтан

от 1 октября 2018г. № 26

**Перечень информационных систем персональных данных,**

 **обрабатываемых в финансовом управлении города Калтан**

Информационные системы персональных данных, обрабатываемых в финансовом управлении города Калтан (ИСПДн):

1. ИСПДн 1С: "Зарплата и кадры государственного учреждения" (1 этаж, помещение № 1, № 2).

Приложение N 7

к приказу финансового управления

города Калтан

от 1 октября 2018г. № 26

**Перечень**

**должностей служащих финансового управления города Калтан,**

**замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным**

1. К персональным данным служащих финансового управления города Калтан, обрабатываемых как неавтоматизированным, так и автоматизированным способом, для выполнения своих должностных обязанностей имеют доступ следующие служащие финансового управления города Калтан:

- Начальник финансового управления города Калтан;

- Заместитель руководителя – начальник бюджетного отдела финансового управления города Калтан;

- Начальник отдела доходов;

- Заместитель начальника отдела доходов;

- Начальник отдела бухгалтерского учета и отчетности – главный бухгалтер;

- Главный специалистотдела бухгалтерского учета и отчетности;

- Главный специалист АСФР;

- Главный специалист – юрисконсульт.

- Главный специалист отдела доходов.

2. К персональным данным граждан, обратившихся к оператору с жалобой или на личном приеме, обрабатываемых неавтоматизированным способом, для выполнения своих должностных обязанностей имеют доступ все служащие организации, в части их касающейся.

3. Каждый служащий организации имеет доступ к своим персональным данным.

4. Ответственность за работу с персональными данными несут все служащие финансового управления города Калтан.

Приложение N 8

к приказу финансового управления

города Калтан

от 1 октября 2018г. №26

**Перечень**

**лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей (автоматизированная обработка)**

1. Разрешить доступ к персональным данным, обрабатываемым в информационной системе персональных данных «1С: Зарплата и кадры государственного учреждения», лицам, которым такой доступ необходим для исполнения служебных обязанностей:

– Главный специалист АСФР Мрачковская О.Н. (Демина Н.В.) доступ с целью обеспечения работоспособности информационной системы с правами администратора.

– Сотрудники, пользователи информационной системы, с целью обработки персональных данных:

- Начальникфинансового управления города Калтан – Чушкина В.П.

- Заместитель руководителя - начальникбюджетного отдела финансового управления города Калтан – Маркус И.В.

- Начальник отдела доходов – Горкевич Е.А.

- Заместитель начальника отдела доходов - Толканова Н.Л.

- Начальник отдела бухгалтерского учета и отчетности – главный бухгалтер – Мелешкина Н.В.

- Главный специалистотдела бухгалтерского учета и отчетности – Чернова К.В.

- Главный специалист – юрисконсульт – Роженцева Е.В.

- Главный специалист отдела доходов – Демина Н.В.

2. Запретить доступ посторонних лиц и сотрудников к персональным данным, обрабатываемым в информационных системах персональных данных.

Приложение N 9

к приказу финансового управления

города Калтан

от 3 октября 2018г. № 26

**Перечень лиц,**

**осуществляющих обработку персональных данных, либо имеющих к ним доступ**

1. Разрешить доступ к персональным данным, обрабатываемым в финансовом управлении города Калтан лицам, которым такой доступ необходим для исполнения служебных обязанностей:

- Начальник финансового управления города Калтан – Чушкина В.П.

- Заместитель руководителя - начальник бюджетного отдела финансового управления города Калтан – Маркус И.В.

- Начальник отдела бухгалтерского учета и отчетности – главный бухгалтер – Мелешкина Н.В.

- Начальник отдела доходов – Горкевич Е.А.

- Заместитель начальника отдела доходов - Толканова Н.Л.

- Главный специалист отдела доходов – Демина Н.В.

- Главный специалист отдела бухгалтерского учета и отчетности – Чернова К.В.

- Главный специалист – юрисконсульт – Роженцева Е.В.

Приложение N 10

к приказу финансового управления

города Калтан

от 1 октября 2018г. №26

Должностная инструкция лица, ответственного за организацию обработки персональных данных

Общие положения

В финансовом управления города Калтан ответственность за организацию обработки персональных данных (далее - ПДН) возлагается на главного специалиста - юрисконсульта.

Его деятельность регламентируется Федеральным законом от 27.07.2006г. N 152-ФЗ и иными нормативными правовыми актами в области защиты ПДН, актами финансового управления города Калтан, Федеральной службы безопасности, нормативными правовыми актами по эксплуатации средств защиты информации, а также настоящей должностной инструкцией.

Ответственное лицо отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты информационных систем персональных данных (ИСПДн) и ее ресурсов на этапах эксплуатации и модернизации.

Ответственное лицо осуществляет методическое руководство сотрудников, имеющих санкционированный доступ к ПДН в вопросах обеспечения безопасности персональных данных.

Требования ответственного лица, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми сотрудниками, имеющими санкционированный доступ к ПДН.

Ответственное лицо несет персональную ответственность за качество проводимых им работ по контролю действий сотрудников, имеющих санкционированный доступ к ПДН, состояние и поддержание установленного уровня защиты ИСПДн.

Функции ответственного лица

Осуществление внутреннего контроля за соблюдением требований законодательства РФ при обработке ПДН в Федеральном агентстве по техническому регулированию и метрологии, в том числе требований к защите ПДН.

Доведение до сведения государственных гражданских служащих положения законодательства РФ о ПДН, локальных актов по вопросам обработки ПДН, требований к защите ПДН.

Организация приема и обработки обращений и запросов субъектов ПДН или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.

Предоставление субъекту ПДН либо его представителю по запросу информации об обработке его персональных данных.

Разъяснение субъекту ПДН юридических последствий отказа предоставить свои ПДН.

Ответственное лицо имеет право:

- на прохождение обучения по защите ПДН в учебных центрах и курсах повышения квалификации;

- вносить руководству предложения о наказании отдельных сотрудников, имеющих санкционированный доступ к ПДН, допустивших серьезные нарушения в безопасности ПДН.

Приложение N 11

к приказу финансового управления

города Калтан

от 1 октября 2018г. №26

**Должностная инструкция
работников финансового управления города Калтан,
участвующих в обработке персональных данных**

**1. Общие положения**

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность работников финансового управления города Калтан (далее – Управление), участвующих в обработке персональных данных в Управлении в соответствии со своими должностными обязанностями.

1.2. Перечень работников, участвующих в обработке персональных данных и допущенных к обработке персональных данных, устанавливается приказом начальника Управления.

1.3. Методическое руководство работниками, участвующими в обработке персональных данных, осуществляется ответственным за организацию обработки персональных данных.

**2. Обязанности**

Работник, участвующий в обработке персональных данных, обязан:

2.1. Ознакомиться с федеральными и локальными нормативными актами;

2.2. Осуществлять уточнение, блокирование или уничтожение персональных данных по запросу ответственного за организацию обработки персональных данных;

2.3. Обеспечивать сохранность находящихся у него бумажных носителей, в том числе заполняемых в настоящий момент, и не допускать ознакомления с его содержанием посторонних лиц;

2.4. При обнаружении признаков несанкционированного доступа к персональным данным немедленно сообщить об этом ответственному за организацию обработки персональных данных, начальнику Управления или его заместителю;

2.5. Осуществлять обработку персональных данных только в Управлении;

2.6. При поступлении запросов правообладателей ПДн о выполнении их законных прав в области персональных данных – направить данного субъекта персональных данных
к должностному лицу, уполномоченному исполнять подобные запросы, или исполнить запрос, если он относится к компетенции данного должностного лица.

2.7. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.8. Соблюдать Правила работы в сетях общего доступа и (или) международного обмена – Интернет и других;

2.9. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

2.10. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

**3. Права**

Работник, участвующий в обработке персональных данных, имеет следующие права:

3.1. Право на доступ к бумажным носителям, необходимым для выполнения должностных обязанностей;

3.2. Право на доступ к элементам баз данных и программным ресурсам информационных систем персональных данных, необходимым для выполнения должностных обязанностей.

**4. Работнику запрещается**

4.1.    Разглашать защищаемую информацию третьим лицам.

4.2.    Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

4.3    Самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

4.4.    Несанкционированно открывать общий доступ к своему ПК.

4.5.    Запрещено подключать к ПК личные внешние носители и мобильные устройства.

4.6.    Отключать (блокировать) средства защиты информации.

4.7.    Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

4.8.    Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

4.9.    Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за техническую защиту персональных данных.

**5. Ответственность**

Работник, участвующий в обработке персональных данных, несет ответственность за:

5.1. Полноту введенной и/или уточненной информации и ее соответствие данным, предоставленным субъектом персональных данных;

5.2. Разглашение персональных данных субъекта в соответствии с трудовым, гражданским
и уголовным законодательством РФ, а также законодательством об административных правонарушениях.

Приложение № 12

к приказу финансового управления

города Калтан

от 1 октября 2018г. №26

**Должностная инструкция**

**администратора безопасности информационных систем персональных данных финансового управления города Калтан**

1. Общие положения.

1.1. Данная Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных (далее – ИСПДн) финансового управления города Калтан (далее – Управление).

1.2. Администратор безопасности ИСПДн является штатным сотрудником Управления.

1.3. Администратором безопасности ИСПДн является главный специалист АСФР Управления.

1.4. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности администратора безопасности ИСПДн.

1.5. Администратор безопасности ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам ИСПДн.

1.6. Администратор безопасности должен иметь специальное рабочее место – рабочую станцию (PC), функционирующую постоянно при включении сети.

1. Должностные обязанности

2.1. Администратор безопасности ИСПДн обязан:

2.1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.1.2. Знать перечень установленных в подразделениях Управленияавтоматизированных рабочих мест (далее – АРМ) и перечень задач, решаемых с их использованием.

2.1.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

* программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
* аппаратных средств;
* аппаратных и программных средств защиты.

2.1.4. Обеспечивать функционирование и поддерживать работоспособность элементов ИСПДн, в том числе средств защиты информации, и локальной вычислительной сети.

2.1.5. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.1.6. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля.

2.1.7. Осуществлять контроль за порядком учета, создания, хранения

* использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.1.8. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.1.9. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ (далее – ИСПДн).

2.1.10. Осуществлять оперативный контроль за работой пользователей защищенных АРМ.

2.1.11. Осуществлять непосредственное управление режимами работы

* административную поддержку функционирования применяемых на АРМ ИСПДн специальных технических средств защиты от несанкционированного доступа (далее – НСД).

2.1.12. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов сторонними физическими лицами и организациями.

2.1.13. Периодически проверять состояние используемых средств защиты информации (далее – СЗИ) от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

2.1.14. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ.

2.1.15. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления НСД к информации и техническим средствам АРМ.

2.1.16. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению средствами защиты от НСД, установленных на АРМ ИСПДн.

2.1.17. Проводить занятия с сотрудниками и начальниками отделов по правилам работы на АРМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации.

2.1.18. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.

1. Порядок работы с ресурсами ИСПДн

3.1. Перечень работ, производимых администратором безопасности

ИСПДн.

3.1.1. Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн.

3.1.1.1. Администратор безопасности ИСПДн разрабатывает правила парольной защиты и контролирует их соблюдение.

3.1.1.2. Администратор безопасности ИСПДн сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, кодирует аппаратный идентификатор пользователя (при наличии).

3.1.1.3. Администратор безопасности ИСПДн производит изменения учетных данных пользователя по требованию начальника отдела, при согласовании с ответственным за обеспечение безопасности персональных данных, а также периодически по утвержденному плану и в случае увольнения сотрудника.

3.1.1.4. Администратор безопасности ИСПДн имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, в случае успешного взлома, администратор безопасности ИСПДн обязан потребовать у пользователя изменения пароля.

3.1.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации.

3.1.2.1. Администратор безопасности ИСПДн обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – прекратить работы.

3.1.2.2. В случае сбоя программных СЗИ, таких, как неправильная идентификация и аутентификация пользователей, администратор безопасности ИСПДн обязан прекратить работы, в случае производственной необходимости продолжения работ – отключить программное обеспечение (далее - ПО) СЗИ и лично контролировать проведение работ пользователем.

3.1.3. Антивирусная защита ресурсов ИСПДн.

3.1.3.1. Администратор безопасности ИСПДн в соответствии с инструкцией по организации антивирусной защиты разрабатывает и контролирует реализацию антивирусной политики, а именно:

* настраивает параметры антивирусной программы;
* контролирует работоспособность антивирусной программы;
* немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы;
* имеет право на проведение внеплановой проверки на присутствие вирусов;

- периодически обновляет антивирусные базы данных, а также исполняемые модули антивирусной программы.

3.1.4. Хранение дистрибутивов программного обеспечения СЗИ.

3.1.4.1. Администратор безопасности ИСПДн должен хранить дистрибутивы ПО СЗИ, установленных на АРМ ИСПДн, в месте, исключающем доступ посторонних лиц.

3.1.5. Проверка целостности системного и прикладного ПО.

3.1.5.1. Администратор безопасности ИСПДн должен периодически (не реже одного раза в квартал) производить проверку целостности системного

* прикладного программного обеспечения с использованием специальных режимов работы СЗИ от НСД.

3.1.6. Резервное копирование и восстановление информации.

3.1.6.1. В соответствии с утвержденным регламентом, а также по требованию пользователей, администратор безопасности ИСПДн проводит резервное копирование и восстановление пользовательской информации. При этом необходимо выполнять следующие требования:

* + иметь в наличии регламент резервного копирования и перечень резервируемой информации, утверждаемых приказом Управления;
	+ вне графика производить обязательное резервное копирование в случае обнаружения неисправностей в работе АРМ или отчуждаемых носителей;
	+ допускается обоснованное внеплановое резервное копирование информации по инициативе администратора безопасности ИСПДн, если это не нарушает технологию обработки информации;
	+ резервные копии хранятся на отдельных носителях в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение (ответственным за хранение является администратор безопасности ИСПДн);
	+ при устранении неисправностей АРМ администратор безопасности ИСПДн производит восстановление важной информации с резервных копий.

3.1.7. Вывод ресурсов ИС из эксплуатации.

3.1.7.1. При невозможности ремонта технических средств ИСПДн администратор безопасности ИСПДн обязан:

* + физически уничтожать любые носители, независимо от содержащейся на них информации, отразить факт уничтожения носителя в «Журнале учета машинных носителей персональных данных».
1. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. Сеансы работы с ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят реализуемые в процессе сеанса работы операции

4.1.2. Действия третьего лица, пытающегося получить доступ (или получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

4.2. При выявлении факта НСД администратор безопасности ИСПДн обязан:

4.2.1. Прекратить доступ к ИСПДн со стороны выявленного участка

НСД;

4.2.2. Доложить начальнику Управления служебной запиской о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. Проанализировать характер НСД, по результатам анализа составить письменный отчет и предоставить его начальнику Управления.

1. Права

5.1. Администратор безопасности ИСПДн имеет право:

5.1.1. Требовать от пользователей информационных ресурсов выполнения инструкций пользователя ИСПДн;

5.1.2. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

5.1.3. Вносить свои предложения по совершенствованию мер защиты

в ИСПДн.

1. Ответственность

6.1. Администратор безопасности ИСПДн несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации.

6.2. Администратор безопасности ИСПДн несет ответственность за программно-аппаратные, инженерно-технические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и информационные системы обработки информации и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

6.3. Администратор безопасности ИСПДн несет ответственность по действующему законодательству за разглашение информации, составляющей персональные данные, ставшие известными ему по роду работы.

Приложение №13

к приказу финансового управления

города Калтан

от 01 октября 2018г.№ 26

**Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в финансовом управлении города Калтан**

1. **Назначение и область действия**

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее – Инструкция), связанные с функционированием ИСПДн финансового управления г.Калтан, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

определение мер защиты от потери информации;

определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей организации, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

системы жизнеобеспечения;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

1. **Порядок реагирования на инцидент**

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

В результате непреднамеренных действий пользователей.

В результате преднамеренных действий пользователей и третьих лиц.

В результате нарушения правил эксплуатации технических средств ИСПДн.

В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

В кратчайшие сроки, не превышающие одного рабочего дня, главным специалистом АСФР предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

1. **Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов**

**3.1.Технические меры**

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

системы жизнеобеспечения;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

Все критичные помещения организации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

резервные линии электропитания в пределах комплекса зданий;

аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

кластеризация;

технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

**3.2.Организационные меры**

Резервное копирование и хранение данных должно осуществлять на периодической основе:

для обрабатываемых персональных данных – не реже раза в неделю;

для технологической информации – не реже раза в месяц;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

1. **Ответственность**

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на Администратора безопасности информации в органе исполнительной власти.

Приложение № 14

к приказу финансового управления

города Калтан

от 01 октября 2018г.№ 26

**Инструкция по организации антивирусной защиты**

**информационных систем персональных данных**

**в финансовом управлении города Калтан.**

**Список сокращений**

ИСПДн - Информационная система персональных данных

ИБ - Информационная безопасность

ПДн - Персональные данные

ПО - Программное обеспечение

ПЭВМ - Персональная электронная вычислительная машина

САЗ - Система антивирусной защиты

СВТ - Средства вычислительной техники

**Применение средств антивирусной защиты**

Антивирусная защита осуществляется при использовании KasperskyEndpointSecurity 10 дляWindows.

1. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).
2. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).
3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD(DVD)-ROM и флеш-накопителях т.п.).
4. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема.
5. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).
6. Обновление антивирусных баз проводиться регулярно, в автоматическом режиме.

**Пользователи ИСПДн в особенности и остальные пользователи СВТ:**

1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник должен провести внеочередной антивирусный контроль ПЭВМ. При необходимости он должен привлечь главного специалиста АСФР для определения факта наличия или отсутствия компьютерного вируса.
2. В случае обнаружения (подтверждения факта наличия вируса) при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:
* приостановить работу;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя финансового управления г.Калтан и главного специалиста АСФР, владельца зараженных файлов, а также других сотрудников, использующие эти файлы в работе;
* совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
* провести лечение или уничтожение зараженных файлов;
* в случае обнаружения вируса, не поддающегося лечению установленными антивирусными средствами, передать зараженный вирусом файл на съемном носителе в организацию на антивирусную поддержку;
* по факту обнаружения зараженных вирусом файлов составить служебную записку главному специалисту АСФР, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

Инструкция подлежит полному пересмотру в случае приобретения предприятием новых средств защиты, существенно изменяющих порядок работы с ними.

Приложение №15

к приказу финансового управления

города Калтан

от 01 октября 2018г.№ 26

**Инструкция**

**по обеспечению безопасности в информационных системах персональных данных (парольная защита в ИСПДн)**

**в финансовом управлении города Калтан**

**1. Общие положения**

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник организации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Политикой информационной безопасности организации, руководящими и нормативными документами ФСТЭК России и регламентирующими документами финансового управления г.Калтан.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

**2. Должностные обязанности**

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью организации, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за обеспечение защиты персональных данных.

2.8. Пользователям запрещается:

Разглашать защищаемую информацию третьим лицам.

Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

Отключать (блокировать) средства защиты информации.

Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.9. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных, в пределах возложенных на него функций.

**3. Организация парольной защиты**

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям главным специалистом АСФР.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

Пароль должен состоять не менее чем из 8 символов.

В пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

Запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранение пароля:

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

**4. Правила работы в сетях общего доступа и (или) международного обмена**

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

Осуществлять работу при отключенных средствах защиты (антивирус и других).

Передавать по Сети без использования средств защиты каналов связи.

Запрещается скачивать из Сети программное обеспечение и другие файлы.

Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).

Запрещается нецелевое использование подключения к сети.

Приложение № 16

к приказу финансового управления

города Калтан

от 01 октября 2018г.№ 26

**Обязательство**

**о неразглашении информации, содержащей персональные данные**

 Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

проживающий(ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

паспорт серия \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ N \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, выданный\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (кем и когда)

предупрежден(а) о том, что на период исполнения мною должностных

обязанностей по Служебному контракту, заключенному между мною и начальником финансового управления города Калтан, и предусматривающих работу с персональнымиданными служащих финансового управления города Калтанмне будет предоставлен доступ к указанной информации. Настоящим добровольно принимаю на себя обязательства:

- не передавать (в любом виде) и не разглашать третьим лицам и служащим финансового управления города Калтан, не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением начальника, информацию, содержащую персональные данные сотрудников (граждан) (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

- в случае попытки третьих лиц или служащих финансового управления города Калтан, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщать об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;

- не использовать информацию, содержащую персональные данные, с целью получения выгоды;

- выполнять требования закона и иных нормативных правовых актов Российской Федерации, а также внутренних документов организации, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

- после прекращения моих прав на допуск к информации, содержащей персональные данные (переход на должность, не предусматривающую доступ к персональным данным, или прекращения служебного контракта), не обрабатывать, не разглашать и не передавать третьим лицам и не уполномоченным на это служащим финансового управления города Калтан, известную мне информацию, содержащую персональные данные;

- в случае расторжения со мной Служебного контракта прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с действующим законодательством Российской Федерации.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ "\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ г.

 (подпись) (Ф.И.О.)

Приложение № 17

к приказу финансового управления

города Калтан

 от 3 октября 2018г.№ 26

**Согласие**

**на обработку персональных данных**

 Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[фамилия, имя, отчество]

проживающий(ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

основной документ, удостоверяющий личность (паспорт) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[серия, номер, дата выдачи документа, наименование выдавшего органа]

даю свое согласие допущенным к обработке персональных данных служащиморганизации на обработку своих персональных данных, включая сбор,систематизацию, накопление, хранение, уточнение (обновление, изменение),использование, распространение (в том числе передачу), обезличивание,блокирование, уничтожение персональных данных, с целью обеспечения вопросовпрохождения государственной гражданской службы.

Перечень персональных данных, на обработку которых дается согласие:

|  |  |  |
| --- | --- | --- |
| N п/п | Персональные данные | Согласие |
| ДА | НЕТ |
| 1. Общая информация |
|  | Фамилия, имя, отчество |  |  |
|  | Число, месяц, год и место рождения |  |  |
|  | Гражданство (в том числе предыдущие гражданства, иные гражданства) |  |  |
|  | ОбразованиеНаправление подготовки или специальность по дипломуКвалификация по диплому |  |  |
|  | Послевузовское профессиональное образование: аспирантура, адъюнктура, докторантураУченая степень, ученое звание |  |  |
|  | Владение иностранными языками и языками народов Российской Федерации и степень владения |  |  |
|  | Классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы (кем и когда присвоены) |  |  |
|  | Наличие судимости |  |  |
|  | Допуск к государственной тайне, оформленный за период работы, службы, учебы, его форма, номер и дата |  |  |
|  | Выполняемая работа с начала трудовой деятельности |  |  |
|  | Государственные награды, иные награды и знаки отличия |  |  |
|  | Фамилия, имя, отчество, год, число, месяц, место рождения, место работы, домашний адрес близких родственников, а также мужа (жены), в том числе бывших |  |  |
|  | Наличие близких родственников, а также мужа (жены), в том числе бывших, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство |  |  |
|  | Пребывание за границей (когда, где, с какой целью) |  |  |
|  | Отношение к воинской обязанности и воинское звание |  |  |
|  | Домашний адрес (индекс, адрес регистрации, фактического проживания), номер контактного телефона |  |  |
|  | Паспортные данные |  |  |
|  | Наличие заграничного паспорта |  |  |
|  | Реквизиты страхового свидетельства обязательного пенсионного страхования |  |  |
|  | Идентификационный номер налогоплательщика |  |  |
|  | Реквизиты страхового медицинского полиса обязательного медицинского страхования |  |  |
|  | Медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению |  |  |
|  | Сведения о прохождении государственной гражданской службы, в том числе: дата, основания поступления на государственную гражданскую службу и назначения на должность государственной гражданской службы, дата, основания назначения, перевода, перемещения на иную должность государственной гражданской службы, наименование замещаемых должностей государственной гражданской службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности государственной гражданской службы, а также сведения о прежнем месте работы; |  |  |
|  | Сведения о профессиональной переподготовке и (или) повышении квалификации |  |  |
|  | Информация о ежегодных оплачиваемых отпусках, учебных отпусках, отпусках без сохранения денежного содержания, отпусках по временной нетрудоспособности |  |  |
|  | Доходы (свои и членов своей семьи) |  |  |
|  | Имущество (свои и членов своей семьи) |  |  |
|  | Обязательства имущественного характера (свои и членов своей семьи) |  |  |
|  | Расходы (свои и членов своей семьи) |  |  |
|  | Номер расчетного счета |  |  |
|  | Номер банковской карты |  |  |
|  | (Другая информация) |  |  |
| 2. Специальные категории персональных данных |
|  | Состояние здоровья |  |  |
|  | (Другая информация) |  |  |
| 3. Биометрические данные |  |  |
|  | Фотография |  |  |
|  | (Другая информация) |  |  |

Настоящее согласие действует на период прохождения государственной гражданской службы в организации.

Субъект персональных данных вправе отозвать данное согласие на обработку своих персональных данных, письменно уведомив об этом соответствующих должностных лиц оператора.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных в письменной форме (если иной порядок отзыва не предусмотрен действующим законодательством) финансовое управление города Калтан обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

(Подпись субъекта персональных данных) (Число, месяц, год)

Приложение № 18

к приказу финансового управления

города Калтан

 от 1 октября 2018г.№ 26

**Разъяснение субъекту персональных данных юридических**

**последствий отказа предоставить свои персональные данные**

 Я,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество субъекта персональных данных)

проживающий(ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(адрес места жительства субъекта персональных данных)

основной документ, удостоверяющий личность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование и номер основного документа, удостоверяющего личность,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

сведения о дате выдачи указанного документа и выдавшем его органе)

в соответствии счастью 2 статьи 18 Федерального закона от 27 июля 2006

года N 152-ФЗ "О персональных данных" настоящим подтверждаю, что мне

разъяснены юридические последствия отказа предоставить свои персональные

данные.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ "\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

 (Ф.И.О) подпись

Приложение № 19

к приказу финансового управления

города Калтан

 от 1 октября 2018г. № 26

Согласие на передачу персональных

данных третьим лицам

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (фамилия, имя, отчество)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

зарегистрированного по адресу:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

( паспорт серия N выдан

**[СОГЛАСИЕ](http://blanker.ru/doc/soglasie-na-peredachu-personalnykh-dannykh-tretim-litsam)**

**[на передачу персональных данных третьей стороне](http://blanker.ru/doc/soglasie-na-peredachu-personalnykh-dannykh-tretim-litsam)**

 Я,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество)

даю согласие финансовому управлению города Калтан

расположенному по адресу:Кемеровская область, г. Калтан, пр-т Мира,53, на предоставление \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать третье лицо)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

моих персональных данных для рассмотрения вопроса о \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Настоящее согласие действительно в течение \_\_\_\_\_\_\_\_\_\_\_\_ с момента его получения.

\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

 (подпись) (расшифровка подписи)(дата)

Приложение № 20

к приказу финансового управления

города Калтан

 от 1 октября 2018г. № 26

**Перечень**

**помещений, предназначенных для обработки персональных данных**

|  |  |  |
| --- | --- | --- |
| **№****п/п** | **Наименование помещения** | **Адрес и место расположения** |
| 1. | Кабинет главного специалиста отдела бухгалтерского учета и отчетности, помещение № 1 | Кемеровская область, г.Калтан, пр.Мира, д.53, каб.1 |
| 2. | Приемная начальника управления,помещение № 2 | Кемеровская область, г.Калтан, пр.Мира, д.53, каб.2 |
| 3. | Кабинет начальника управления,помещение № 2 | Кемеровская область, г.Калтан, пр.Мира, д.53, каб.2 |
| 4. | Кабинет главного специалиста - юрисконсульта, помещение № 3 | Кемеровская область, г.Калтан, пр.Мира, д.53, каб.3 |

Приложение № 21

к приказу финансового управления

города Калтан

 от 1 октября 2018г. № 26

**Перечень**

**лиц, допущенных в помещения, предназначенные для обработки персональных данных**

|  |  |  |  |
| --- | --- | --- | --- |
| **№****п/п** | **№****кабинета** | **Должность** | **Фамилия и инициалы** |
| 1 | 1 | Начальник отдела бухгалтерского учета и отчетности | Мелешкина Н.Е. |
| 2 | 1 | главный специалист отдела бухгалтерского учета и отчетности | Чернова К.В. |
| 3 | 2 | Начальник управленияГлавный специалист отдела доходовГлавный специалист АСФР | Чушкина В.П.Демина Н.В.Мрачковская О.Н. |
| 4 | 3 | Начальник отдела доходов | Горкевич Е.А. |
| 5 | 3 | главный специалист бюджетного отдела | Грушецкая О.В. |
| 6 | 3 | главный специалист-юрисконсульт  | Роженцева Е.В. |

Приложение № 22

к приказу финансового управления

города Калтан

 от 1 октября 2018г. № 26

Порядок

доступа служащих финансового управления города Калтан в помещения, в которых ведется обработка персональных данных

1. Для хранения документов на бумажных носителях в помещении финансового управления города Калтан по адресу г. Калтан, пр-т Мира 53 предназначены следующие кабинеты:

- кабинет отдела бухгалтерского учета и отчетности (1 этаж, каб. 1);

- кабинет главного специалиста - юрисконсульта (1 этаж, каб.3).

2. Для размещения автоматизированных рабочих мест (далее - АРМ) информационных систем персональных данных (далее - ИСПДН) предназначены кабинеты: № 1, 2, 3.

3. Порядок доступа служащих финансового управления города Калтан в помещения, в которых ведется обработка персональных данных:

- каждая комната запирается на ключ;

- служащие финансового управления города Калтан, имеющие доступ в помещения, самостоятельно заходят в кабинеты;

- служащие финансового управления города Калтан, не имеющие доступа в помещения, где обрабатываются персональные данные, имеют право временно прибывать в указанных помещениях только в присутствии сотрудников, имеющих право доступа в эти помещения.

Приложение № 23

к приказу финансового управления

города Калтан

от «01»октября 2018 г. № 26

**Перечень мест хранения материальных носителей**

**персональных данных и ответственных лиц**

|  |  |  |  |
| --- | --- | --- | --- |
| N п/п | Категория персональных данных | Место хранения | Ответственное лицо (должность, фамилия и инициалы) |
| 1. | Бумажные носители персональных данных (трудовая книжка;журнал учета трудовых книжек; журнал учета командировокприказы по личному составу) | специально отведенный металлический шкаф в кабинете № 2 | Начальник финансового управления города Калтан В.П. Чушкина |
| 2. | Бумажные носители персональных данных (личные дела; личные карточки; материалы по награждению и поощрению). | специально отведенный металлический шкаф в кабинете № 3 | Главный специалист – юрисконсульт Роженцева Е.В. |
| 3. | Электронные носители персональных данных. Бумажные носители персональных данных (материалы по учету рабочего времени, больничные листы.) | жесткий диск,съемный носитель,специально отведенный металлический шкаф в кабинете № 1 | Главный специалист отдела бухгалтерского учета и отчетности Чернова К.В.Главный специалист АСФР |

Приложение № 24

к приказу финансового управления

города Калтан

от «01» октября 2018 г. № 26

## Журнал учета хранилищ, металлических шкафов и ключей от них

Журнал начат "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г.

Журнал завершен "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г.

Ответственный за ведение журнала \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 (должность) (подпись ) (фамилия, имя, отчество)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| Учетный номер | Наименование хранилища (сейф, металлический шкаф) | Инвентарный номер | Местонахождение (подразделение, номер комнаты) | Что находится (документы, изделия) | Фамилия ответственного за сейф (шкаф) | Кол-во комплектов ключей и их номера | Расписка ответственного за хранилище в получении ключа и дата | Расписка в приеме ключа и дата |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Приложение № 25

к приказу финансового управления

города Калтан

от «01»октября 2018 г. № 26

**Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных**

1. **Общие положения**
	1. Настоящие Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (далее - Правила) определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" (далее - ФЗ N 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ N 152-ФЗ.
	2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.
2. **Основные понятия**
	* 1. Информация - сведения (сообщения, данные) независимо от формы их представления;
		2. Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;
		3. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
		4. Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение;
		5. Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;
		6. Убытки - расходы, 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;
		7. Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом;
		8. Оценка возможного вреда - определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.
3. **Методика оценки возможного вреда субъектам персональных данных**
	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. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:
		1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;
		2. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;
		3. Неправомерное изменение персональных данных является нарушением целостности персональных данных;
		4. Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;
		5. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;
		6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;
		7. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;
		8. 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.
	3. Субъекту персональных данных может быть причинен вред в форме:
		1. 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;
		2. 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.
	4. В оценке возможного вреда исходит из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:
		1. Низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;
		2. 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;
		3. Высокий уровень возможного вреда - во всех остальных случаях.
4. **Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых Оператором мер**
	1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным за защиту информации, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведенных в Приложении 1.
	2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ N 152-ФЗ "О персональных данных", определяется лицом, ответственным за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

Приложение 1 к правилам

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N п\ п  | Требования Федерального закона "О персональных данных", которые могут быть нарушены  | Возможные нарушение безопасности информации и причиненный субъекту вред  | Уровень возможного вреда  | Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных  |
| 1  | порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных  | Убытки и моральный вред Целостность Доступность Конфиденциальность  | средний  | В соответствии с законодательство м в области защиты информации и Положением по обеспечением безопасности персональных данных  |
| 2 | порядок и условия применения средствзащиты информации | Убытки и моральный вред ЦелостностьДоступностьКонфиденциальность | средний | В соответствии с техническо документацией насистему защитыИСПД й |
| 3  | эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных  | Убытки и моральный вред Целостность Доступность Конфиденциальность | высокий  | Программа и методика испытаний систем защиты  |
| 4  | состояние учета машинных носителей персональных данных  | Убытки и моральный вред Целостность Доступность Конфиденциальность  |  | Инструкция по учету машинных носителей информации  |
| 5  | соблюдение правил доступа к персональным данным  | Убытки и моральный вред Целостность Доступность Конфиденциальность | высокий  | В соответствии с принятыми организационным и мерами и в соответствии с системой разграничения доступа  |
| 6  | наличие (отсутствие) фактов несанкционированног о доступа к персональным данным и принятие необходимых мер  | Убытки и моральный вред Целостность Доступность Конфиденциальность | средний  | Мониторинг средств защиты информации на наличие фактов доступа к ПД  |
| 7  | мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированног о доступа к ним  | Убытки и моральный вред Целостность Доступность Конфиденциальность  | низкий  | Применение резервного копирования  |
| 8  | осуществление мероприятий по обеспечению целостности персональных данных  | Убытки и моральный вред Целостность Доступность Конфиденциальность  | низкий  | Организация режима доступа к техническим и программным средствам  |

Приложение № 26

к приказу финансового управления

города Калтан

от «01»октября 2018 г. № 26

**Журнал сертифицированных средств защиты информации**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Номерп/п** | **Индекс и наименование средства защиты информации** | **Серийный (заводской) номер** | **Номер специального защитного знака** | **Наименование организации, установившей СЗИ** | **Место установки** | **Примечание** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение № 27

к приказу финансового управления

города Калтан

от «01»октября 2018 г. № 26

**Журнал учета**

 **съемных носителей конфиденциальной информации (персональных данных)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Регистрационный номер/дата | Тип/ёмкость машинного носителя персональных данных | Номер экземпляра/количество экземпляров | Место установки (использования)/дата установки | Ответственное должностное лицо (ФИО) | Расписка в получении (ФИО, подпись, дата) | Расписка в обратном приеме (ФИО, подпись, дата) | Место хранения машинного носителя персональных данных | Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата) |
| 1 |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Приложение № 28

к приказу финансового управления

города Калтан

от «01»октября 2018 г. № 26

**Лист ознакомления**

**с положениями законодательства РФ о персональных данных и с требованиями к защите персональных данных**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Ф.И.О. | Дата | Подпись |
| 1. |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение № 29

к приказу финансового управления

города Калтан

от «01»октября 2018 г. № 26

**Лист ознакомления**

**сотрудников о факте обработки ими персональных данных**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Ф.И.О. | Дата | Подпись |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |