ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
СТАВРОПОЛЬСКОГО КРАЯ «СТАВКРАЙИМУЩЕСТВО»

ПРИКАЗ

«01» апреля 2024 г. г. Ставрополь №11/1-П

Об организации обработки и
защиты персональных данных

В соответствии с Федеральным законом «О персональных данных» и Приказом ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке и защите персональных данных в государственном бюджетном учреждении Ставропольского края «Ставкрайимущество» (далее – Положение, Учреждение) (Приложение 1).
2. Назначить ответственным за организацию обработки персональных данных в Учреждении начальника юридического отдела Пустовойт Олега Ивановича.
3. Назначить ответственным за обеспечение безопасности персональных данных в информационных системах персональных Учреждения, обрабатываемых с использованием технических средств, а также администратором информационной безопасности в Учреждении главного специалиста отдела информационного обеспечения государственной кадастровой оценки управления государственной кадастровой оценки Пристинского Валентина Алексеевича.
4. Утвердить Инструкцию ответственного за организацию обработки персональных данных в Учреждении (Приложение 2).
5. Утвердить Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных Учреждения, обрабатываемых с использованием технических средств (Приложение 3).
6. Считать утратившим силу приказ государственного бюджетного учреждения Ставропольского края «Ставкрайимущество» от «09» июля 2018 года № 4/2-П «Об обработке и защите персональных данных в ГБУ СК «Ставкрайимущество».
7. Ответственному лицу, указанному в п. 3 настоящего приказа обеспечить размещение Положения на официальном сайте Учреждения в информационно-телекоммуникационной сети «Интернет».
8. Контроль за исполнением настоящего приказа возложить на заместителя директора Сахарову О.А.

Директор М.А. Сопин

Приложение 1
к приказу ГБУ СК «Ставкрайимущество»
от 01.04 2024 № 111 -П

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в государственном бюджетном учреждении Ставропольского края «Ставкрайимущество»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке и защите персональных данных в государственном бюджетном учреждении Ставропольского края «Ставкрайимущество» (далее - Положение, Учреждение) разработано на основании:

Конституции Российской Федерации;

Трудового кодекса Российской Федерации;

Гражданского кодекса Российской Федерации;

Налогового кодекса Российской Федерации;

Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

других федеральных законов и нормативно-правовых актов Российской Федерации.

1.2. Основные понятия, используемые в настоящем Положении, применяются в том же значении, что и в Федеральном законе «О персональных данных».

1.3. Настоящим Положением определяется порядок обработки, т.е. действий (операций) с персональными данными (далее - ПДн), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн клиентов и контрагентов Учреждения в связи с осуществлением Учреждением уставной деятельности с использованием средств автоматизации или без использования таких средств. Положение устанавливает требования по защите ПДн, принципы обработки ПДн в информационных системах персональных данных (далее - ИСПДн).

1.4. Целью настоящего Положения является обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты ПДн граждан.

1.5. Основные термины и определения, применяемые в настоящем Положении:

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

1.5.2. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение уточнение (обновление, изменение), извлечение, использование передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.5.3. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.5.4. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.5.5. Использование персональных данных - действия (операции) с Дн, совершаемые оператором в целях принятия решений или совершения иных действии, порождающих юридические последствия в отношении субъекта Дн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

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

1.5.7. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.5.8. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.5.9. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.5.10. Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся ее владельцем.

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

1.5.12. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими или по истечении сроков хранения, если иное не определено лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных состав персональных данных, подлежащих обработке, действия (операции),

совершаемые с персональными данными.

1.6. К субъектам персональных данных (далее - субъекты) относятся лица, ПДн которых переданы Учреждению, (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для обработки (в том числе передачи).

1.7. ПДн защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Учреждения.

1.8. Обработка ПДн субъекта без письменного его согласия не допускаются, если иное не определено законодательством РФ. ПДн относятся к категории конфиденциальной информации. Режим конфиденциальности ПДн снимается в случаях обезличивания Законодательством Российской Федерации.

1.9. Должностные лица Учреждения, в обязанности которых входит обработка ПДн субъектов, обязаны обеспечить каждому субъекту возможность ознакомления со своими ПДн, если иное не предусмотрено законодательством Российской Федерации.

1.10. ПДн не могут быть использованы в целях:

причинения имущественного и морального вреда гражданам;

затруднения реализации прав и свобод граждан Российской Федерации.

1.11. Настоящее Положение и изменения к нему утверждаются директором Учреждения, являются обязательными для исполнения всеми работниками Учреждения, имеющими доступ к ПДн субъектов ПДн.

2. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка ПДн в Учреждении осуществляется на основе следующих принципов:

законности и справедливости обработки ПДн;

законности целей и способов обработки ПДн и добросовестности;

соответствия целей обработки ПДн целям, заранее определенным и за¬явленным при сборе ПДн, а также функциям и полномочиям Учреждения;

соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн;

достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;

недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

2.2. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели их обработки. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в

достижении этих целей, если иное не предусмотрено законодательством Российской Федерации в области обработки и защиты персональных данных.

2.3. Субъект ПДн является собственником своих ПДн и самостоятельно решает вопрос передачи Учреждению своих ПДн.

2.4. Держателем ПДн является Учреждение, которому субъект ПДн передает во владение свои ПДн. Учреждение выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством Российской Федерации.

3. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Под ПДн субъектов понимается информация необходимая Учреждению для:

исполнение требований трудового законодательства и трудового договора с работником;

ведение бухгалтерского, налогового и кадрового учета; передача персональных, данных работников Учреждения в банковские организации для содействия в открытии банковских карт; начисления заработной платы работникам.

3.2. Для целей осуществления уставной деятельности в Учреждении обрабатываются следующие категории персональных данных заявителей, клиентов и контрагентов:

фамилия, имя, отчество; пол;

место, год и дата рождения; адрес регистрации (проживания);

паспортные данные (серия, номер паспорта, кем и когда выдан);

ИНН;

адрес электронной почты;

телефонный номер (домашний, рабочий, мобильный);

иные сведения, указанные субъектом персональных данных.

3.3. Документы, содержащие ПДн, являются конфиденциальными.

4. ПОЛУЧЕНИЕ, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Учреждение получает сведения о ПДн субъектов ПДн из следующих источников:

паспорта или иного документа, удостоверяющего личность; заявлений, заполняемых гражданами.

Субъект ПДн обязан предоставлять Учреждению достоверные сведения о себе. Учреждение имеет право проверять достоверность указанных сведений в порядке, не противоречащем законодательству Российской Федерации.

4.2 При определении состава обрабатываемых ПДн субъектов Учреждение руководствуется Конституцией Российской Федерации, Трудовым кодексов Российской Федерации, иными федеральными законами.

4.3. ПДн субъекта Учреждение получает непосредственно от субъекта.

Ответственный работник Учреждения принимает от субъекта материальные носители ПДн (документы, копии документов), сверяет копии документов с подлинниками.

4.4. Условием обработки ПДн субъекта ПДн является его письменное согласие. Письменное Согласие в письменной форме субъекта персональных

данных на обработку его персональных данных должно включать в себя в частности:

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

фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

цель обработки персональных данных;

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

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

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

срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено законодательством Российской Федерации;

подпись субъекта персональных данных.

Согласие на обработку ПДн может быть отозвано субъектом ПДн в соответствии с положением статьи 9 Федерального закона «О персональных данных».

4.5. Для обработки ПДн, содержащихся в согласии в письменной форме субъекта на обработку его ПДн, дополнительное согласие не требуется.

4.6. В случае недееспособности субъекта ПДн согласие на обработку его персональных данных в письменной форме дает его законный представитель.

В случае смерти субъекта согласие на обработку его ПДн при необходимости дает в письменной форме один из его наследников, если такое согласие не было дано субъектом ПДн при его жизни.

4.7. Защита ПДн субъекта от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном законодательством Российской Федерации.

4.8. Субъекты ПДн и их представители должны быть ознакомлены под подпись с документами Учреждения, устанавливающими порядок обработки ПДн, а также об их правах и обязанностях в этой области.

4.9. Основным источником, содержащим ПДн граждан, является база данных ПДн Учреждения.

4.10. При обработке ПДн директор Учреждения, руководствуясь обоснованными предложениями ответственного за организацию обработки персональных данных в Учреждении и ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных Учреждения, обрабатываемых с использованием технических средств, вправе определять способы обработки, документирования, хранения и защиты ПДн, в том числе на базе современных информационных технологий.

4.11. Перечень лиц, допущенных к обработке ПДн, определяется приказом директора Учреждения.

4.12. Обработка ПДн, осуществляются уполномоченными работниками Учреждения, определенными приказом директора Учреждения, которые действуют на основании инструкций, предусматривающих выполнение комплекса мероприятий по обеспечению безопасности ПДн.

4.13. Помещения, в которых обрабатываются и хранятся ПДн субъектов, оборудуются надежными замками. Должно быть исключено бесконтрольное пребывание посторонних лиц в этих помещениях.

Для хранения ПДн используются специально оборудованные шкафы или сейфы, которые запираются на ключ.

Помещения, в которых обрабатываются и хранятся ПДн субъектов, в рабочее время при отсутствии в них работников должны быть закрыты.

Проведение уборки помещений, в которых хранятся ПДн, должно производиться в присутствии соответствующих работников.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Субъект персональных данных обязан:

передать Учреждению комплекс достоверных, документированных ПДн. своевременно сообщать Учреждению об изменении своих ПДн.

5.2. Субъект ПДн имеет право:

на получение сведений о Учреждении, о месте его нахождения, о наличии у Учреждения ПДн, относящихся к соответствующему субъекту ПДн, а также на ознакомление с такими ПДн, за исключением случаев, если предоставление ПДн нарушает конституционные права и свободы других лиц;

на свободный бесплатный доступ к своим ПДн, включая право на получение копии любой записи, содержащей ПДн, за исключением случаев, предусмотренных законодательством Российской Федерации;

получать информацию, касающуюся обработки его ПДн, в том числе содержащую:

подтверждение факта обработки Учреждением; правовые основания и цели обработки ПДн;

цели и применяемые способы обработки ПДн, применяемые оператором;

наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании законодательства Российской Федерации в области обработки и защиты персональных данных;

обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством Российской Федерации; сроки обработки ПДн, в том числе сроки их хранения; порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом «О персональных данных»;

сведения о том, какие юридические последствия для него может повлечь за собой обработка его ПДн;

обжаловать в судебном порядке любые неправомерные действия или бездействие Учреждения при обработке и защите ПДн;

требовать об извещении Учреждения всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;

требовать от Учреждения исключения, исправления или уточнения своих персональных данных, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

при отказе оператора исключить или исправить ПДн субъекта заявить в письменной форме Учреждению о своем несогласии с соответствующим обоснованием такого несогласия, при отклонении оператором указанного обращения (несогласия), обжаловать действия оператора в порядке, предусмотренном действующим законодательством Российской Федерации.

Сведения о ПДн должны быть предоставлены субъекту в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

5.3. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, не может быть принято на основании исключительно автоматизированной обработки его ПДн.

5.4. Учреждение обязано разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов.

5.5. Учреждение обязано рассмотреть возражение субъекта ПДн в течение 30 (тридцати) рабочих дней со дня его получения и уведомить его о

результатах рассмотрения такого возражения.

5.6. Если обязанность предоставления ПДн субъектом установлена федеральным законодательством Российской Федерации (включая налоговое, трудовое право), Учреждение обязано разъяснить субъекту ПДн юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

5.7. Учреждение обязано безвозмездно предоставить субъекту ПДн возможность ознакомления с ПДн, относящимися к нему, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие ПДн по предоставлении субъектом сведений, подтверждающих, что ПДн яв-ляются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

5.8. Учреждение обязано сообщить в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа в установленные нормативно-правовыми актами Российской Федерации сроки.

5.9. В случае подтверждения факта неточности ПДн Учреждение на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязан уточнить ПДн либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение 7 (семи) рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

5.10. В случае выявления неправомерной обработки ПДн, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, прекращает неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению учреждения. В случае, если обеспечить правомерность обработки ПДн невозможно, учреждение в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки ПДн, уничтожает такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Учреждение уведомляет субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

5.11. В случае достижения цели обработки ПДн Учреждение обязано незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий 30 (тридцати) рабочих дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта

ПДн на основаниях, предусмотренных законодательством Российской Феде¬рации в области обработки и защиты персональных данных.

5.12. В случае отзыва субъектом согласия на обработку своих ПДн Учреждение обязано прекратить обработку ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн в срок, не превышающий 30 (тридцати) рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон и (или) законодательством Российской Федерации в области обработки и защиты персональных данных. Об уничтожении ПДн оператор обязан уведомить субъекта ПДн.

5.13. В случае невозможности уничтожения ПДн в течение вышеуказанного срока Учреждение должно осуществить блокирование таких ПДн персональных или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение ПДн в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

5.14. До начала обработки ПДн Учреждение обязано уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев установленных законодательством Российской Федерации.

5.15. Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации об электронной подписи. Уведомление должно содержать следующие сведения:

наименование (фамилия, имя, отчество), адрес Учреждения;

цель обработки ПДн;

описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

дата начала обработки персональных данных;

срок или условие прекращения обработки персональных данных;

сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

фамилия, имя, отчество физического лица или наименование юридического лица, имеющих доступ и (или) осуществляющих на основании договора обработку персональных данных, содержащихся в государственных и муниципальных информационных системах;

сведения об обеспечении безопасности персональных данных в

соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

6. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СУБЪЕКТА И ИХ ПЕРЕДАЧА

6.1. Внутренний доступ (доступ внутри Учреждения) к ПДн субъектов имеют работники структурных подразделений Учреждения, которым эти данные необходимы для выполнения должностных обязанностей.

После прекращения юридических отношений с субъектом ПДн документы, содержащие его ПДн, хранятся в Учреждении в течение сроков, установленных архивным и иным законодательством Российской Федерации,

6.2. Внешний доступ к ПДн субъектов имеют массовые потребители ПДн и контрольно-надзорные органы.

6.2.1. К числу массовых потребителей ПДн вне Учреждения относятся следующие государственные и негосударственные структуры:

ПФР, У ФНС и ФСС России;

правоохранительные органы;

органы прокуратуры, МВД и ФСБ России.

6.2.2. Контрольно-надзорные органы имеют доступ к информации исключительно в сфере своей компетенции.

6.3. Внешний доступ со стороны третьих лиц к ПДн субъекта осуществляется с его письменного согласия.

6.4. Учреждение обязано сообщать ПДн субъекта по надлежаще оформленным запросам суда, прокуратуры иных правоохранительных органов.

6.5. ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта ПДн.

6.6. При передаче ПДн Учреждение должно соблюдать следующие требования:

не сообщать ПДн субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в случаях, установленных законодательством Российской Федерации в области обработки и защиты персональных данных;

не сообщать ПДн субъекта в коммерческих целях без его письменного согласия;

предупреждать лиц, получающих ПДн субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено, за исключением случаев, когда обмен ПДн осуществляется в порядке, установленном законодательством Российской Федерации;

не запрашивать информацию о состоянии здоровья субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

разрешать доступ к ПДн, исключительно специально уполномоченным лицам (при этом указанные лица должны иметь право получать лишь те ПДн, которые необходимы для выполнения конкретных функций);

в должностных инструкция уполномоченных лиц должны быть прописаны обязательства по неразглашению и выполнению требований нормативных документов по обработке и обеспечению безопасности персональных данных.

6.7. Передача ПДн от держателя или его представителей в другие учреждения и организации может допускаться только при наличии письменного согласия субъекта ПДн в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.8. Ответы на правомерные письменные запросы других учреждений и организаций даются с разрешения директора Учреждения в письменной форме, в том объеме, который позволяет не разглашать излишний объем ПДн.

6.9. Не допускается передача ПДн по открытым каналам связи, в том числе по телефону, факсу.

6.10. Сведения, передаваемые в письменной форме, должны иметь пометку о конфиденциальности. В сопроводительном письме к таким документам указывается, что в прилагаемых документах содержатся ПДн субъектов.

6.11. Учреждением не допускается осуществление трансграничной передачи персональных данных.

7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Учреждение в процессе своей деятельности реализует комплекс мер по защите ПДн, направленный на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности ПДн и обеспечение безопасности информации.

7.2. Учреждение при обработке ПДн принимает необходимые организационные и технические меры, в том числе использует шифровальные (криптографические) средства для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИСПДн.

7.3. Мероприятия по защите ПДн определяются настоящим Положением, локальными актами Учреждения,

7.4. Для защиты ПДн в Учреждении применяются следующие принципы и правила:

ограничение и регламентация состава работников Учреждения, функциональные обязанности которых требуют доступа к информации, содержащей ПДн;

строгое избирательное и обоснованное распределение документов и

информации между работниками Учреждения;

рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

знание работниками требований нормативно-методических документов по защите ПДн;

распределение персональной ответственности между работниками, участвующими в обработке ПДн, за выполнение требований по обеспечению безопасности ПДн.

установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности ПДн при работе с конфиденциальными документами и базами данных;

исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка ПДн и находится соответствующая вычислительная техника;

организация порядка уничтожения информации;

своевременное выявление нарушений требований разрешительной системы доступа;

воспитательная и разъяснительная работа с работниками структурных подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн;

ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся ПДн.

создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией;

резервирование защищаемых данных (создание резервных копий).

8. ДОПУСК ПЕРСОНАЛА К ОБРАБОТКЕ ПДН

8.1. При допуске к обработке ПДн необходимо руководствоваться приказом Учреждения о допуске к работе с ПДн.

8.2. Перечни должностных лиц составляются и ведутся владельцами ИСПДн и процессов обработки ПДн на основании данных о должностных лицах, допущенных к ПДн.

9. ОБУЧЕНИЕ ПЕРСОНАЛА, УЧАСТВУЮЩЕГО В ОБРАБОТКЕ ПДН

9.1. Должно проводиться регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн с учетом актуализации законодательства по данным вопросам.

9.2. Для различных категорий работников форматы обучения должны отличаться.

Определены следующие форматы обучения:

полные курсы (длительностью 5 дней и более);

кратковременные курсы (длительностью от 1 до 3 дней);

внешние и внутренние семинары;

конференции;

инструктажи.

9.2.1. Полные и кратковременные курсы, конференции, внешние семинары проводятся во внешних специализированных организациях для следующих категорий работников:

ответственный за обеспечение безопасности и обработки ПДн; администратор информационной безопасности ИСПДн.

9.2.2. Для обучения остальных категорий работников, участвующих в процессах обработки ПДн, должны проводиться:

внутренние семинары и инструктажи.

Внутренние семинары проводятся ответственным за обеспечение безопасности и обработки ПДн, а также могут проводиться приглашенными специалистами или другими подготовленными лицами.

Инструктажи проводятся в отношении отдельных лиц, по мере необходимости АИБ ИСПДн, ответственным за обеспечение безопасности и обработки ПДн.

При необходимости могут разрабатываться инструкции, описывающие особенности обработки ПДн в каждой ИСПДн, для отдельных категорий (групп) персонала.

10. ОРГАНИЗАЦИЯ РАБОТЫ С НОСИТЕЛЯМИ ПДН

10.1. Для организации документооборота, связанного с ПДн в Учреждении, должны быть упорядочены и регламентированы следующие работы, связанные с ПДн:

учет носителей, содержащих ПДн;

обращение с носителями, содержащими ПДн;

систематизация носителей, содержащих ПДн;

хранение носителей, содержащих ПДн;

подготовка носителей, содержащих ПДн для передачи их в архив;

подготовка носителей, содержащих ПДн для их уничтожения;

проверка наличия носителей, содержащих ПДн;

распечатка ПДн.

Должны регламентироваться работы с ПДн в виде документов на следующих носителях:

бумажных носителях;

электронных съемных носителях;

электронных несъемных носителях, используемых в технических средствах ИСПДн.

10.2. Порядок работ с носителями ПДн должен быть регламентирован в соответствующих внутренних нормативных документах.

11. УНИЧТОЖЕНИЕ ПДН

11.1. В соответствии с нормативными актами Российской Федерации ПДн должны быть уничтожены:

по требованию субъекта ПДн, в определенных законодательством Российской Федерации случаях;

при истечении срока хранения;

в случае выявления неправомерных действий с ПДн и невозможности устранения допущенных нарушений;

в случае достижения цели обработки ПДн;

в случае утраты необходимости достижения цели обработки.

Контроль сроков хранения, целей обработки ПДн производится на основании допустимых сроков хранения и допустимых целей.

11.2. Решение об уничтожении ПДн, организацию и проведение уничтожения принимают и осуществляют владельцы ИСПДн и процессов обработки ПДн.

11.3. Порядок уничтожения ПДн должен быть регламентирован в локальных документах Учреждения.

Об уничтожении ПДн должен быть уведомлен субъект ПДн.

11.4. После проведенного уничтожения должен быть подготовлен акт об уничтожении ПДн.

12. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ДОСТУПА К ЭЛЕМЕНТАМ ИСПДН

12.1. Мероприятия по физическому контролю доступа включают: контроль доступа в помещения с оборудованием ИСПДн; контроль доступа к техническим средствам ИСПДн; контроль перемещений физических компонентов ИСПДн.

12.2. Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн должны иметь прочные входные двери с надежными замками. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода работников.

Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками.

12.3. Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие работники), должно допускаться только в присутствии работников, участвующих в соответствующих технологических процессах.

12.4. Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не являющихся пользователями ИСПДн.

12.5. В нерабочее время, по окончании рабочего дня двери помещений должны быть закрыты на замок.

12.6. При выносе устройств, хранящих ПДн, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

12.7. В отношении некоторых ИСПДн возможны дополнительные, либо более низкие требования по физической защите. Состав таких требований определяется по результатам разработки Модели угроз и нарушителя и ТЗ (СТЗ, ЧТЗ) на создание СЗПДн. Мероприятия по защите таких ИСПДн определяются эксплуатационной (проектной) документацией.

13. РЕЗЕРВИРОВАНИЕ ПДН

13.1. Резервирование ПДн должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

В регламенте процесса резервирования должны быть учтены следующие вопросы:

порядок резервирования;

ответственные за резервирование;

порядок восстановления информации после аварий;

порядок хранения резервных копий.

Резервированию должна подвергаться информация на серверах ИСПДн.

Резервирование должно осуществляться на магнитные ленты или другие носители информации с соответствующим уровнем надежности и долго¬вечности.

13.2. Хранение резервных копий должно осуществляться в сейфах (запираемых шкафах, ящиках). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

13.3. Доступ к резервным копиям должен быть строго ограничен.

14. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ

14.1. Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн, в Учреждении должны быть регламентированы следующие вопросы:

порядок определения нештатной ситуации;

порядок оповещения работников при возникновении различных нештатных ситуаций;

порядок действий работников Учреждения в нештатных ситуациях.

В Учреждении должны проводиться расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями.

В рамках данного процесса должны решаться следующие задачи:

расследование инцидентов, связанных с безопасностью ПДн;

ликвидация последствий инцидентов связанных с безопасностью ПДн;

принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

15. ОТВЕТСТВЕННОСТЬ РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

15.1. Персональная ответственность является одним из главных требований к организации функционирования СЗПДн и обязательным условием обеспечения эффективности функционирования данной системы.

15.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

15.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

15.4. Каждый работник Учреждения, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность полученной информации.

15.5. Должностные лица, в обязанность которых входит обработка ПДн, обязаны обеспечить каждому субъекту ПДн, возможность ознакомления с документами и материалами, если иное не предусмотрено законодательством Российской Федерации.

Неправомерный отказ в предоставлении собранных в установленном порядке ПДн, либо несвоевременное их предоставление в случаях, предусмотренных законодательством Российской Федерации, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного наказания в порядке, установленном Кодексом Российской Федерации об административных правонарушениях.

15.6. В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, содержащую ПДн, обязаны возместить причиненные убытки; такая же обязанность возлагается и на работников, не обладающих правом доступа к ПДн.

15.7. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения влечет наложение наказания

в порядке, предусмотренном Уголовным кодексом Российской Федерации.

15.8. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию ПДн может быть установлена в судебном порядке.

16. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

Особенности обработки персональных данных, осуществляемой без использования средств автоматизации:

16.1. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

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

16.3. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

16.4. При составлении типовых форм необходимо, чтобы каждый субъект ПДн, чьи ПДн указаны в документе, имел возможность ознакомиться со своими ПДн, содержащими в документе, не нарушая прав и законных интересов иных лиц.

Приложение 2
к приказу ГБУ СК «Ставкрайимущество»
от 01.04 20__ №111-П

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в государственном бюджетном учреждении Ставропольского края «Ставкрайимущество»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за организацию обработки персональных данных в государственном бюджетном учреждении Ставропольского края «Ставкрайимущество» (далее – Ответственный) назначается приказом государственном бюджетном учреждении Ставропольского края «Ставкрайимущество» (далее – Учреждение) и отвечает за организацию, обеспечение своевременного и квалифицированного выполнения работниками Учреждения законодательства Российской Федерации о персональных данных (далее – ПДн), в том числе требований к обработке и защите ПДн.

1.2. Ответственный должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.

1.3. В своей деятельности Ответственный руководствуется Политикой государственном бюджетном учреждении Ставропольского края «Ставкрайимущество» в отношении обработки и защиты ПДн, настоящей Инструкцией.

2. ОСНОВНЫЕ ФУНКЦИИ И ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Функции Ответственного:

2.1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по организации обработки ПДн при решении следующих основных вопросов:

– организация доступа к ПДн и учет работников Учреждения, допущенных к обработке ПДн, как в программных комплексах, входящих в состав информационных систем персональных данных (далее – ИСПДн), так и на бумажных носителях;

– контроль за поддержанием в актуальном состоянии действующих локальных актов, журналов и форм учета по работе с ПДн;

– контроль за обеспечением соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;

– организация работы по заключению договоров на работы по защите ПДн;

– контроль за поддержанием в актуальном состоянии уведомления об обработке ПДн;

– рассмотрение предложений по совершенствованию действующей системы защиты ПДн, предоставленных Ответственным за обеспечение безопасности ПДн в информационных системах персональных данных Учреждения;

– осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

Ответственный обязан:

2.2. Знать цели обработки ПДн в Учреждении и перечень обрабатываемых ПДн;

2.3. Соблюдать требования Политики в отношении обработки персональных данных в государственном бюджетном учреждении Ставропольского края «Ставкрайимущество» и иных локальных актов Учреждения, устанавливающих порядок работы с ПДн;

2.4. Обеспечивать доведение до сведения работников Учреждения норм действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн, локальных актов Учреждения по вопросам обработки ПДн;

2.5. Осуществлять внутренний контроль за соблюдением работниками Учреждения норм действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;

2.6. Контролировать ведение документации, предусмотренной локальными актами Учреждения в части обеспечения безопасности ПДн;

2.7. Обеспечивать доработку нормативно-методических документов по защите ПДнУчреждения;

2.8. Расследовать нарушения по вопросам защиты информации, имевшие место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений;

2.9. Обеспечивать организацию проведения занятий со специалистами Учреждения по организационным вопросам обработки ПДн (проводить инструктаж работников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в Учреждении);

2.10.Обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов согласно п. 3 ч. 4 ст. 22.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. ПРАВА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственный имеет право:

3.1. Знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него задач;

3.2. Проводить проверки соблюдения режима обеспечения безопасности ПДн в структурных и (или) территориальных подразделениях Учреждения (при их наличии);

3.3. Требовать от работников Учреждения соблюдения требований Политики в отношении обработки персональных данных в Учреждении, а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обработки ПДн;

3.5. Требовать от работников Учреждения письменных объяснений при проведении служебных расследований по вопросам нарушений требований по обработке и защите ПДн;

3.6. Вносить предложения директору Учреждения об отстранении от выполнения служебных обязанностей работников, систематически нарушающих требования по обработке и защите ПДн;

3.7. Давать работникам Учреждения обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации и требованиями Учреждения;

3.8. Привлекать в установленном порядке специалистов, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.

4. ОТВЕТСТВЕННОСТЬ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственный в соответствии с возложенными на него обязанностями несет ответственность за:

4.1. Несоблюдение требований локальных актов Учреждения, устанавливающих порядок работы с ПДн, в пределах, установленных трудовым договором (служебным контрактом);

4.2. Разглашение ПДн, в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

С инструкцией ознакомлен:

Должность ФИО

Приложение 3
к приказу ГБУ СК «Ставкрайимущество»
от 01.04 2024 №11/1 -П

ИНСТРУКЦИЯ
Ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных государственного бюджетного учреждения Ставропольского края «Ставкрайимущество», обрабатываемых с использованием технических средств.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных государственного бюджетного учреждения Ставропольского края «Ставкрайимущество», обрабатываемых с использованием технических средств (далее – Ответственный) назначается приказом государственного бюджетного учреждения Ставропольского края «Ставкрайимущество» (далее – Учреждение) и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн) Учреждения.

1.2. Ответственный должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.

1.3. В своей деятельности Ответственный руководствуется Политикой государственного бюджетного учреждения Ставропольского края «Ставкрайимущество» в отношении обработки и защиты ПДн, настоящей Инструкцией, рекомендациями Ответственного за организацию обработки персональных данных (далее – Ответственный за организацию обработки ПДн).

1.4. Методическое руководство работой Ответственного осуществляет Ответственный за организацию обработки ПДн.

2. ОСНОВНЫЕ ФУНКЦИИ И ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Функции Ответственного:

2.1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по защите ПДн при решении следующих основных вопросов:

– проведение аналитической работы по комплексной защите и предупреждению утечки ПДн;

– подготовка решений в отношении сведений о работах, выполняемых Учреждением, подлежащих защите;

– рассмотрение проектов технических заданий, нормативных актов и указаний, договоров на выполнение работ, отчетной документации, с целью определения достаточности предусмотренных в них требований и мероприятий по комплексной защите ПДн, при научных исследованиях, при проведении других работ;

– координация внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами;

– проведение работ по контролю эффективности принимаемых мер по выявлению и закрытию возможных каналов утечки ПДн;

– подготовка предложений по совершенствованию действующей системы защиты ПДн с последующим предоставлением Ответственному за организацию обработки ПДн Учреждения и (или) директору Учреждения;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

– обеспечение соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;

– осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

Ответственный обязан:

2.2. Соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;

2.3. Знать состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн;

2.4. Осуществлять общее техническое сопровождение ИСПДн:

– контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;

– контролировать сохранность пломб на оборудовании автоматизированных рабочих мест;

– вести журнал учета и выдачи используемых материальных носителей ПДн;

– контролировать использование съемных материальных носителей информации, в том числе запрещать использование неучтенных носителей информации;

– проводить инструктаж работников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ИСПДн Учреждения (далее – Пользователи ИСПДн) по правилам работы в ИСПДн;

2.5. Осуществлять настройку и сопровождение подсистемы регистрации и учета ИСПДн:

– реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка работников, допущенных к работе в ИСПДн;

– назначать пароли Пользователей ИСПДн;

– контролировать плановую смену паролей Пользователями ИСПДн для доступа в ИСПДн;

– вводить в базу данных системы защиты от несанкционированного доступа (далее – НСД) описания событий, подлежащих регистрации в системном журнале;

– регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа к ИСПДн;

– своевременно информировать Ответственного за организацию обработки ПДн о несанкционированных действиях персонала для организации расследования попыток НСД;

2.6. Сопровождать подсистему обеспечения целостности рабочего программного обеспечения (ПО) ИСПДн:

– обеспечивать регулярное и своевременное обновление антивирусного программного обеспечения Учреждения;

– обеспечивать поддержание установленного порядка эксплуатации антивирусного программного обеспечения;

– обеспечивать регулярное и своевременное создание резервных копий ИСПДн Учреждения;

– осуществлять настройку и сопровождение системы защиты от НСД в ИСПДн;

2.7. Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИСПДн;

2.8. Требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

2.9. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований фактов НСД;

2.10. Участвовать при проведении внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн;

2.11. Контролировать выполнение Пользователями ИСПДн требований Инструкции пользователя информационных систем персональных данных Учреждения, а также установленных требований для обеспечения уровней защищенности ПДн;

2.12. Контролировать правильность применения Пользователями ИСПДн средств защиты информации;

2.13. В случае получения от Пользователей ИСПДн информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности ПДн в пределах своих полномочий;

2.14. Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИСПДн:

– антивирусного программного обеспечения;

– средств защиты от несанкционированного доступа;

2.15. В случае нарушения работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности;

2.16. Своевременно информировать Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ИСПДн.

3. ПРАВА ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственный имеет право:

3.1. Знакомиться с локальными актами Учреждения, регламентирующими процессы обработки и защиты ПДн;

3.2. Вносить предложения директору Учреждения по совершенствованию существующей системы защиты информации;

3.3. Привлекать по согласованию с Ответственным за организацию обработки ПДн и директором Учреждения к работе по созданию и совершенствованию системы защиты ПДн других работников Учреждения;

3.4. Требовать от Пользователей ИСПДн соблюдения требований Инструкции пользователя информационных систем персональных данных Учреждения, а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;

3.5. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность ПДн, вносить свои предложения по совершенствованию организационных и технических мер защиты ПДн в ИСПДн;

3.6. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн;

3.7. Требовать прекращения работы в ИСПДн, как в целом, так и отдельных Пользователей ИСПДн, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИСПДн;

3.8. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.

4. ОТВЕТСТВЕННОСТЬ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственный в соответствии с возложенными на него обязанностями несет ответственность за:

4.1. Несоблюдение требований локальных актов Учреждения, устанавливающих порядок работы с ПДн в пределах, установленных трудовым договором;

4.2. Разглашение ПДн в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

С инструкцией ознакомлен:

Должность ФИО