Муниципальное образование «Бирофельдское сельское поселение»

Биробиджанского муниципального района

Еврейской автономно области

АДМИНИСТРАЦИЯ СЕЛЬСКОГО ПОСЕЛЕНИЯ

ПОСТАНОВЛЕНИЕ

 24.06.2019 № 67

с. Бирофельд

Об утверждении организационных документов по сбору, обработке, защите и хранению персональных данных в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области

В целях исполнения Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальнымиорганами» администрация сельского поселения

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые к настоящему постановлению:

1.1. Политику администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области в отношении обработки персональных данных согласно приложению № 1.

1.2. Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области согласно приложению № 2.

1.3. Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области согласно приложению № 3.

1.4. Перечень информационных систем персональных данных в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области согласно приложению № 4.

1.5. Перечень персональных данных, обрабатываемых в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области в связи с реализацией трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций согласно приложению № 5.

1.6. Перечень должностей служащих администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно приложению № 6.

1.7. Положение по обработке персональных данных без использования средств автоматизации в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области согласно приложению № 7.

1.8. Положение об организации и обеспечении защиты персональных данных при их обработке в информационных системах персональных данных администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области согласно приложению № 8.

2. Признать утратившими силу постановление администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области от 07.11.2007 № 37 «Об утверждении порядка хранения и использования персональных данных муниципальных служащих в администрации Бирофельдского сельского поселения и определении должностных лиц, уполномоченных на их получение, обработку, хранение и использование».

3. Настоящее постановление довести до ответственных лиц в части их касающейся.

4. Контроль за исполнением настоящего постановлениявозложить на заместителя главы администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области Васильеву Т.А.

5. Опубликовать настоящее постановление в Информационном бюллетене Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области.

6. Настоящее постановление вступает в силу после дня его официального опубликования.

Глава администрации

сельского поселения М.Ю. Ворон

ПРИЛОЖЕНИЕ № 1

к постановлению администрации

Бирофельдского сельского поселения

от 24.06.2019 № 67

**ПОЛИТИКА**

**в администрации Бирофельдского сельского**

**поселения Биробиджанского муниципального района**

**Еврейской автономной области**

 **в отношении обработки персональных данных**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

## 1.1. Термины и определения:

- персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

- автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

- распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

1.2.Политика администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области (далее по тексту – Администрация) в отношении обработки персональных данных определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Администрация в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

1.3. Законодательной основой настоящей Политики являются [Конституция Российской Федерации](http://securitypolicy.ru/index.php/%D0%9A%D0%BE%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%86%D0%B8%D1%8F_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8),  [Трудовой кодекс](http://securitypolicy.ru/index.php/%D0%92%D1%8B%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B8_%D0%B8%D0%B7_%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%BE%D0%B3%D0%BE_%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8) Российской Федерации, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, акты ФСТЭК и ФСБ России.

1.4. Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных Администрации позволит оптимизировать затраты на ее построение.

1.5. При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

## 1.6. Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

## 2. ОБЪЕКТЫ ЗАЩИТЫ

Основными объектами системы безопасности персональных данных в Администрации являются:

- информационные ресурсы с ограниченным доступом, содержащие персональные данные;

- процессы обработки персональных данных в информационной системе персональных данных Администрации, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

## - информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

## 3. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 3.1. Субъектами информационных отношений при обеспечении безопасности персональных данных Администрации являются:

## 3.1.1 Администрация, как собственник информационных ресурсов;

## 3.1.2 руководство и служащие Администрации, в соответствии с возложенными на них функциями;

## 3.1.3 физические лица, состоящие с Администрацией в гражданско-правовых отношениях (граждане);

## 3.2. Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

## 3.2.1 своевременного доступа к необходимым им персональным данным (их доступности);

## 3.2.2 достоверности (полноты, точности, адекватности, целостности) персональных данных;

## 3.2.3 конфиденциальности (сохранения в тайне) персональных данных;

## 3.2.4 защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;

## 3.2.5 разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;

##  3.2.6 возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;

## 3.2.7 защиты персональных данных от незаконного распространения.

3.3. Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Администрации от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

3.3.1 доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем Администрации, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);

3.3.2 целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах Администрации и передаваемой по каналам связи;

3.3.3 конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

## 3.4. Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

3.5. Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности Администрации должна обеспечивать эффективное решение следующих задач:

3.5.1 своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Администрации;

3.5.2 создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

3.5.3 создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

3.5.4 защиту от вмешательства в процесс функционирования информационных систем Администрации посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

3.5.5 разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Администрации (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

3.5.6 обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

3.5.7 защиту от несанкционированной модификации используемых в информационных системах Администрации программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

## 3.5.8 защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.6. Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

3.6.1 строгим учетом всех подлежащих защите ресурсов информационных систем Администрации (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

3.6.2 журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационной системы;

3.6.3 полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Департамента по вопросам обеспечения безопасности информации;

3.6.4 подготовкой должностных лиц (служащих), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;

3.6.5 наделением каждого служащего (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Администрации;

3.6.6 четким знанием и строгим соблюдением всеми пользователями информационных систем Администрации требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

3.6.7 персональной ответственностью за свои действия каждого служащего, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Администрации;

3.6.8 непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Администрации;

3.6.9 применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

3.6.10 эффективным контролем над соблюдением пользователями информационных ресурсов Администрации требований по обеспечению безопасности информации;

## 3.6.11 юридической защитой интересов Администрации при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

## 4. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ

## БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Построение системы, обеспечения безопасности персональных данных Администрации, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;

- системность;

- комплексность;

- непрерывность;

- своевременность;

- преемственность и непрерывность совершенствования;

- разумная достаточность (экономическая целесообразность);

- персональная ответственность;

- минимизация полномочий;

- исключение конфликта интересов;

- взаимодействие и сотрудничество;

- гибкость системы защиты;

- открытость алгоритмов и механизмов защиты;

- простота применения средств защиты;

- обоснованность и техническая реализуемость;

- специализация и профессионализм;

- обязательность контроля.

## 4.2. Законность предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных Администрации в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи информационной системы Администрации должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

4.3. Системный подход к построению системы защиты информации в Администрации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

## При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем Администрации, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

## 4.4. Комплексность заключается в использовании методов и средств защиты компьютерных систем, предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

## 4.4. Непрерывность защиты (обеспечение безопасности персональных данных) – это процесс, осуществляемый руководством Администрации, администратором безопасности информационной системы и служащими Администрации. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри Администрации и каждый служащий Администрации должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности Администрации. И ее эффективность зависит от участия руководства Администрации в обеспечении информационной безопасности персональных данных.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

## 4.5. Своевременность предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

## Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

## 4.6. Преемственность и совершенствование предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Администрации и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

## 4.7. Разумная достаточность (экономическая целесообразность) предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем Администрации. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

## Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока персональные данные находятся в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

## 4.8. Персональная ответственность предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого служащего Администрации в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей служащих Администрации строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

## 4.9. Минимизация полномочий означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо для выполнения должностных обязанностей.

## 4.10. Исключение конфликта интересов (разделение функций) предполагает четкое разделение обязанностей служащих Администрации и исключение ситуаций, когда сфера их ответственности допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один служащий Администрации не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение полномочиями, порождающими конфликт интересов, дает возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования персональными данными и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными служащими Администрации. Необходимо проводить периодические проверки обязанностей, функций и деятельности служащих Администрации, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между ними.

## 4.11. Взаимодействие и сотрудничество предполагает создание благоприятной атмосферы в коллективе Администрации. В такой обстановке служащие Администрации должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственным за организацию обработки персональных данных.

## Важным элементом эффективной системы обеспечения безопасности персональных данных в Администрации является высокая культура работы с информацией. Руководство Администрации несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности Администрации. Все служащие Администрации должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

## 4.12. Гибкость системы защиты информационной безопасности заключается в способности реагировать на изменения внешней среды и условий осуществления Администрацией своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры Администрации;

- изменение существующих или внедрение принципиально новых информационных систем;

- новые технические средства.

## Свойство гибкости системы о защиты информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

## 4.13. Открытость алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

## 4.14. Простота применения средств защиты состоит в том, что механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

## 4.15. Обоснованность и техническая реализуемость заключается в том, что информационные технологии, технические и программные средства, средства и меры защиты персональных данных должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

## 4.16. Специализация и профессионализм предполагает привлечение к разработке средств и реализации мер защиты персональных данных специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными служащими Администрации (ответственными за обработку персональных данных).

## 4.17. Обязательность контроля предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных, на основе используемых систем и средств защиты персональных данных, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

4.18. Эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

## 4.19. Недостатки системы обеспечения информационной безопасности, выявленные служащими Администрации должны немедленно доводиться до сведения главы Администрации и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

## 5. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО

## УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

5.1. Все меры обеспечения безопасности информационных систем подразделяются на:

- правовые (законодательные);

- морально-этические;

- технологические;

- организационные (административные);

- физические;

- технические (аппаратурные и программные).

5.2. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями информационных систем.

5.3. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в Администрации. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или Администрации в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

5.4. К технологическим мерам защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

## 5.5. Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

5.6. Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым персональным данным, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов информационных систем Администрации необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки персональных данных, на:

- наличие специально внедренных закладных устройств;

- введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки персональных данных;

## - оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

5.7. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности персональных данных по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства разграничения доступа к данным;

- средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;

- средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Advantor, Touch Memory, Smart Card и т.п.);

- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

- защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

5.8. Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности персональных данных (отражающую подходы к защите персональных данных) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

5.9. Политику в области обеспечения безопасности персональных данных в Администрации целесообразно разбить на два уровня.

К верхнему уровню относятся решения руководства, затрагивающие деятельность Администрации в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности персональных данных и детализирует (регламентирует) эти правила:

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных;

- кто имеет права доступа к персональным данным, кто и при каких условиях может читать и модифицировать персональные данные и т.д.

Политика нижнего уровня должна:

- предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

- определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к персональным данным;

## - выбирать программно-технические (аппаратные) средства противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

5.10. Компоненты информационных систем Администрации должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.). Уборка таких помещений должна производиться в присутствии ответственного служащего Администрации, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Во время обработки персональных данных в таких помещениях должен присутствовать только персонал, допущенный к работе с персональными данными. Запрещается прием посетителей в помещениях, когда осуществляется обработка персональных данных.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем Администрации, должны запираться на ключ.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

5.11. В рамках разрешительной системы доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами Администрации и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

- каждый служащий Администрации пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с ответственными за организацию обработки персональных данных;

- глава Администрации имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все служащие Администрации и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый служащий Администрации (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению персональных данных Администрации.

5.12. В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест служащих Администрации, с которых возможен доступ к ресурсам информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

## В компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

5.13. Оборудование информационной системы, используемое для доступа и хранения персональных данных, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

5.14. Обеспечение безопасности персональных данных возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами Администрации. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационных систем Администрации, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи информационных систем Администрации должны быть ознакомлены с организационно - распорядительными документами по обеспечению безопасности персональных данных Департамента, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности персональных данных. Доведение требований указанных документов до лиц, допущенных к обработке защищаемых персональных данных, должно осуществляться под роспись.

5.15. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с персональными данными, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению главы Администрации.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;

- проверка подлинности пользователей (аутентификация) на основе паролей;

## - реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

5.16. В целях предотвращения работы с ресурсами информационных систем Администрации посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

- путем проверки знания ими паролей;

## - путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

5.17. Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

- на контролируемую территорию;

- в отдельные помещения;

- к компонентам информационной среды Администрации и элементам системы защиты персональных данных (физический доступ);

- к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);

- к активным ресурсам (прикладным программам, задачам и т.п.);

## - к операционной системе, системным программам и программам защиты.

## 5.18. Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации персональных данных должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);

- средствами электронной подписи;

## - средствами подсчета контрольных сумм (для используемого программного обеспечения).

5.19. Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);

- получения твердой копии (печати) журнала регистрации событий безопасности;

- упорядочения журналов, а также установления ограничений на срок их хранения;

- оперативного оповещения ответственного за организацию обработки персональных данных о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

- дата и время события;

- идентификатор субъекта, осуществляющего регистрируемое действие;

- действие (тип доступа).

5.20. Контроль эффективности защиты персональных данных осуществляется с целью своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение персональных данных, разрушение средств информатизации.

Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

## Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

ПРИЛОЖЕНИЕ № 2

к постановлению администрации

Бирофельдского сельского поселения

от 24.06.2019 № 67

**ПРАВИЛА**

**обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны в соответствии с:

- Трудовым кодексом Российской Федерации;

- Федеральным законом Российской Федерации от 27.07.2006 N 152-ФЗ «О персональных данных»;

- Федеральным законом Российской Федерации  от 02.03.2007 № 25-ФЗ «О муниципальнойслужбе в Российской Федерации»;

- Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации»;

- Федеральным законом от 21.11.1996 № 129-ФЗ «О бухгалтерском учёте»;

- Федеральным законом от 28.03.1998 № 53-ФЗ «О воинской обязанности и воинской службе»;

- Федеральным законом от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;

- Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращения граждан Российской Федерации»;

- Федеральным законом от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»;

- Федеральным законом от 21.07.2005 № 94- ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд»;

- Федеральным законом от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

- Федеральным законом от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования»;

- Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

- постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных, на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановлениемПравительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПД»;

- приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей гостайну, содержащейся в государственных информационных системах»;

- распорядительными и методическими документами ФСТЭК России.

1.2. Данные Правила определяют порядок обработки персональных данных служащих администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области (далее по тексту настоящих Правил – Администрация) и третьих лиц, чьи персональные данные обрабатываются Администрации.

1.3. Правила являются внутренним нормативным документом, регламентирующим деятельность Администрации в сфере обработки персональных данных (далее по тексту настоящих Правил – ПДн). Правила являются обязательным для выполнения всеми служащими, состоящими с Администрацией в трудовых отношениях.

1.4. Защита ПДн субъекта ПДн от неправомерного их использования или утраты обеспечивается Администрацией в порядке, установленном законодательством Российской Федерации, за счет своих средств.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ СЛУЖАЩИХ АДМИНИСТРАЦИИ БИРОФЕЛЬДСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ БИРОБИДЖАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА

ЕВРЕЙСКОЙ АВТОНОМНОЙ ОБЛАСТИ

2.1. Под ПДн служащих Администрации понимается информация, необходимая Администрации в связи с возникновением трудовых отношений и касающаяся конкретного служащего Администрации.

2.2. Субъектами ПДн, обработка персональных данных которых осуществляется Администрацией, в соответствии с принципами работы, определенными в настоящих правилах, являются служащие администрации.

2.3. Целями получения и обработки ПДн служащих являются учет прохождения муниципальной службы сотрудниками Администрации, формирование кадрового резерва для замещения должностей муниципальной службы, ведение трудовых книжек муниципальных служащих, ведение личных дел муниципальных служащих, ведение реестра муниципальных служащих, оформление и выдача служебных удостоверений муниципальных служащих, проведение конкурса на замещение вакантных должностей муниципальной службы и включение муниципальных служащих в кадровый резерв, проведение аттестации муниципальных служащих, проведение квалификационных экзаменов муниципальных служащих администрации в целях присвоения им классных чинов, установление надбавок за выслугу лет на муниципальной службе, присвоение иных надбавок и доплат, проверка достоверности и полноты сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых муниципальными служащими Администрации, чьи должности включены в утвержденный перечень должностей, поощрение и награждение муниципальных служащих, применении к ним дисциплинарных взысканий, заключение трудовых договоров с гражданами при приеме их на работу, составление табеля учета рабочего времени, графика ежегодных оплачиваемых отпусков, оформления документов для выезда в служебные командировки, определение стажа муниципальной службы, установления доплат к трудовым пенсиям муниципальным служащим, имеющим на это право, увольняемым из администрации, анализ уровня профессионального образования муниципальных служащих, его соответствия квалификационным требованиям, предъявляемым к замещаемым ими должностям муниципальной службы, в целях проведения работы по планированию направления муниципальных служащих для прохождения дополнительного профессионального образования, подготовка материалов по представлению к награждению государственными наградами Российской Федерации, области и главы Бирофельдского сельского поселения, ведение учета лиц, награжденных наградами главы Бирофельдского сельского поселения, бухгалтерский и налоговый учет, начисление и перечисления заработной платы.

2.4. Доступ к ПДн служащих Администрации имеют:

- глава Администрации;

- заместитель главы Администрации;

- ведущий специалист-эксперт 2 разряда, главный бухгалтер Администрации в целях исполнения возложенных должностных обязанностей;

- ведущий специалист-эксперт 2 разряда Администрации в целях исполнения возложенных должностных обязанностей;

- инспектор военно-учетного стола Администрации в целях исполнения возложенных должностных обязанностей.

2.5. Информационные ресурсы, содержащие ПДн субъектов, создаются путём:

-копирования оригиналов документов, содержащих ПДн (например, паспорт, страховое свидетельство государственного пенсионного страхования);

-внесения сведений в учётные формы на бумажных носителях (личная карточка по форме Т-2ГС (МС);

-внесения сведений в базы данных;

-получения оригиналов необходимых документов (трудовая книжка, автобиография, анкета, заявления).

2.6. К ПДн служащих относятся:

2.6.1 информация, содержащаяся в документах базы данных о служащих (заявлениях, ксерокопиях паспорта, военного билета, документах об образовании, документах о составе семьи; документах о состоянии здоровья; документах, подтверждающих право на дополнительные гарантии и компенсации; личном листке по учету кадров; анкете; резюме; обязательствах; контрольном листе прохождения инструктажа по технике безопасности, сведениях о доходах и др.);

2.6.2 информация, содержащаяся в трудовой книжке служащего;

2.6.3 информация, содержащаяся в служебном контракте и дополнительных соглашениях;

2.6.4 информация, содержащаяся в личной карточке служащего (унифицированная форма Т-2ГС (МС), личной карточке служащего (военнообязанного):

- фамилия, имя, отчество;

- дата рождения;

- место рождения;

- гражданство;

- знание иностранных языков;

- сведения о полученном образовании;

- профессия;

- стаж работы;

- состояние в браке;

- состав семьи;

- паспортные данные;

- адрес места жительства (по паспорту, фактический);

- номер личного телефона;

- сведения о воинском учете;

- сведения о приеме на работу и переводах на другую работу;

- сведения об аттестации;

- сведения о повышении квалификации;

- сведения о профессиональной переподготовке;

- сведения о поощрениях и наградах;

- сведения об отпусках;

- сведения о социальных льготах служащего;

- дата увольнения;

2.6.5 информация, содержащаяся в приказах по личному составу, приказах о предоставлении отпусков, приказах о взысканиях, приказах о поощрении и премировании;

2.6.6 информация, содержащаяся в графике отпусков, служебных характеристиках, рекомендациях и т.п.

3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ СЛУЖАЩИХ АДМИНИСТРАЦИИ БИРОФЕЛЬДСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ БИРОБИДЖАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА

ЕВРЕЙСКОЙ АВТОНОМНОЙ ОБЛАСТИ

3.1. Все ПДн служащего получаются у него самого. Администрация сообщает служащему о целях получения ПДн и последствиях отказа служащего дать письменное согласие на их получение.

3.2. Администрация не имеет права получать и обрабатывать ПДн о политических, религиозных и иных убеждениях и частной жизни служащего.

3.3. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации Администрация вправе получать и обрабатывать данные о частной жизни служащего только с его письменного согласия.

3.4. Администрация не имеет права получать и обрабатывать ПДн о членстве служащего в объединениях и/или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами.

3.5. Администрация не имеет права запрашивать информацию о состоянии здоровья служащего, за исключением тех сведений, которые относятся к вопросу о возможности выполнения служащим служебных обязанностей.

4. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИХ ЛИЦ

4.1. Под ПДн третьих лиц понимается информация, необходимая Администрации в связи с договорными отношениями, с оказанием муниципальных услуг или выполнением муниципальных функций и касающимися конкретного лица.

4.2. Субъектами ПДн, обработка персональных данных которых осуществляется Администрацией, в соответствии с принципами работы, определенными в настоящих Правилах, являются:

- третьи лица – депутаты Собрания депутатов Бирофельдского сельского поселения, работники муниципального казенного учреждения «Поселенческий Дом культуры с. Бирофельд» муниципального образования «Бирофельдское сельское поселение» Биробиджанского муниципального района, контрольно-счётного органа муниципального образования – контрольно-ревизионная комиссия Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области, лица, претендующие на замещение должностей муниципальной службы;

- третьи лица – физические лица, юридические лица, индивидуальные предприниматели, отдельные граждане с которыми Администрация имеет договорные отношения или чьи персональные данные обрабатываются Администрацией в связи с оказанием муниципальных услуг или выполнением муниципальных функций.

4.3. Обработка ПДн третьих лиц может осуществляться только в целях, не выходящих за рамки обеспечения деятельности, указанной в настоящих Правилах.

Такими целями могут быть:

4.3.1 формирование кадрового резерва для замещения должностей муниципальной службы;

4.3.2 проведение конкурса на замещение вакантных должностей муниципальной службы и включение муниципальных служащих в кадровый резерв;

4.3.3 проведение проверки достоверности ПДн и иных сведений, представляемых гражданами, претендующими на замещение должностей муниципальной службы, на замещение иных должностей назначение на которые и освобождение от которых, осуществляет глава Администрации;

4.3.4 проведение проверки достоверности и полноты сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых лицами, претендующими на замещение должностей муниципальной службы, а также сведений о доходах, об имуществе и обязательствах имущественного характера членов их семей;

4.3.5 проведение проверки достоверности и полноты сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых лицами, поступающими на работу, на должность руководителя муниципального казенного учреждения, а также сведений о доходах, об имуществе и обязательства имущественного характера членов их семей;

4.3.6 осуществление учета участников референдума, проживающих на территории Бирофельдского сельского поселения муниципального образования Биробиджанского муниципального района Еврейской автономной области;

4.3.7 приём граждан по жилищным вопросам;

4.3.8 проведение спортивных мероприятий;

4.3.9 организация награждения победителей и призеров, официальных физкультурно-спортивных мероприятий, физических лиц за высокие спортивные достижения на территории Бирофельдского сельского поселения;

4.3.10 исполнение государственных полномочий по применению законодательства об административных правонарушениях;

4.3.11 подготовка статистического отчета;

4.3.12 рассмотрение жалоб и заявлений граждан Бирофельдского сельского поселения,

4.3.13 сбор и обработка данных об избирателях для последующей передачи их в муниципальную избирательную комиссию;

4.3.14 подготовка и выдача разрешений на строительство, реконструкцию объектов капитального строительства;

4.3.15 выдача документа, подтверждающего проведение основных работ по строительству (реконструкции) объекта индивидуального жилищного строительства, осуществляемому с привлечением средств материнского (семейного) капитала;

4.3.16 подготовка, утверждение и выдача градостроительных планов земельных участков;

4.3.17 подготовка и выдача разрешений на ввод объектов в эксплуатацию при осуществлении строительства, реконструкции объектов капитального строительства;

4.3.18 приём и рассмотрение заявлений и документов на проведение конкурса на пассажирские перевозки;

4.3.19 кадровое обслуживание муниципального казенного учреждения «Поселенческий Дом культуры с. Бирофельд» муниципального образования «Бирофельдское сельское поселение» Биробиджанского муниципального района;

4.3.20 кадровое обслуживание аппарата Собрания депутатов Бирофельдского сельского поселения муниципального образования Биробиджанского муниципального района Еврейской автономной области;

4.3.21 кадровое делопроизводство на руководителя муниципального казенного учреждения «Поселенческий Дом культуры с. Бирофельд» муниципального образования «Бирофельдское сельское поселение» Биробиджанского муниципального района;

4.3.22 бухгалтерское обслуживание муниципального казенного учреждения «Поселенческий Дом культуры с. Бирофельд» муниципального образования «Бирофельдское сельское поселение» Биробиджанского муниципального района;

4.3.23 ведение учёта молодых семей-участников подпрограммы «Обеспечение жильём молодых семей», изъявивших желание получить социальную выплату по муниципальному образованию «Бирофельдское сельское поселение» Биробиджанского муниципального района Еврейской автономной области;

4.3.24 приём и ведение документов по многодетным семьям муниципального образования «Бирофельдское сельское поселение» Биробиджанского муниципального района Еврейской автономной области;

4.3.25 участия в расследованиях тяжелых, смертельных и групповых, с тяжелыми последствиями, несчастных случаев на производстве в Администрации, муниципальном казенном учреждении «Поселенческий Дом культуры с. Бирофельд» муниципального образования «Бирофельдское сельское поселение» Биробиджанского муниципального района;

4.3.26 заключение контрактов для муниципальных нужд;

4.3.27 проверка соответствия требованиям, установленным в соответствии с законодательством РФ к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся объектом закупки;

4.3.28 проверка правомочности участника закупки заключать контракт;

- проверка не проведения ликвидации участника закупки - юридического лица и отсутствия решения арбитражного суда о признании участника закупки – юридического лица или индивидуального предпринимателя несостоятельным (банкротом) и об открытии конкурсного производства;

4.3.29 проверка не приостановления деятельности участника закупки в порядке, установленном Кодексом РФ об административных правонарушениях, на дату подачи заявки на участие в закупке;

4.3.30 проверка отсутствия у участника закупки недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы РФ;

4.3.31 проверка отсутствия в реестре недобросовестных поставщиков (подрядчиков, исполнителей) информации об участнике закупке - юридическом лице, в том числе информации об учредителях, о членах коллегиального исполнительного органа, лице, исполняющем функции единоличного исполнительного органа участника закупки;

4.3.32 проверка отсутствия у участника закупки - физического лица либо у руководителя, членов коллегиального исполнительного органа или главного бухгалтера юридического лица - участника закупки судимости за преступления в сфере экономики;

4.3.33 проверка обладания участников закупки исключительными правами на результаты интеллектуальной деятельности;

4.3.34 включение в реестр недобросовестных поставщиков (подрядчиков, исполнителей) информации об участниках закупок, уклонившихся от заключения контрактов, с которыми контракт был, расторгнут по решению суда или в связи с односторонним отказом Заказчика от исполнения контракта.

4.4. Доступ к ПДн третьих лиц, обрабатываемых в Администрации, имеют:

- глава Администрации;

- заместитель главы Администрации;

- ведущий специалист-эксперт 2 разряда, главный бухгалтер Администрации;

- ведущий специалист-эксперт 2 разряда Администрации;

- специалист-эксперт, юрист;

- специалист 1 разряда, землеустроитель Администрации;

- инспектор военно-учетного стола Администрации.

4.5. К ПДн третьих лиц относятся:

4.5.1 информация, содержащаяся в договоре и дополнительных соглашениях;

4.5.2 информация, необходимая Администрации для выполнения требований законодательства Российской Федерации и Еврейской автономной области:

- дата, месяц, год рождения;

- фамилия, имя, отчество;

- место рождения;

- адрес проживания; должность;

- сведения о составе семьи;

- сведения о рождении детей;

- сведения о заключении брака;

- сведения о признании за гражданином права пользования жилым помещением;

- сведения о праве пользования жилым помещением;

- сведения о доходах всех членов семьи за год;

- сведения из документа, удостоверяющего личность гражданина, подающего заявление о принятии на учёт, и из документов, удостоверяющих личность членов его семьи;

- сведения о наличии родственных отношений либо иных обстоятельств, свидетельствующих о принадлежности гражданина к семье заявителя;

- сведения о зарегистрированных по месту жительства гражданах;

- сведения из налоговых деклараций о доходах за расчетный период, заверенные налоговыми органами;

- сведения о размере пенсии; сведения о социальных выплатах, сведения о дееспособности/недееспособности;

- дата окончания срока отбывания наказания; о смерти, о судимости.

5. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИХ ЛИЦ

5.1. Администрация получает ПДн в рамках выполнения требований законодательства Российской Федерации и Еврейской автономной области с письменного согласия субъекта ПДн на обработку его персональных данных.

5.2. Администрация не имеет права получать и обрабатывать ПДн о политических, религиозных и иных убеждениях и частной жизни третьих лиц.

5.3. Администрация не имеет права получать и обрабатывать ПДн о членстве третьих лиц в общественных объединениях и/или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

6. СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

НА ОБРАБОТКУ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка ПДн осуществляется только с письменного согласия (приложение № 5) субъекта ПДн.

Письменное согласие на обработку ПДн должно включать в себя:

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

- наименование оператора, получающего согласие субъекта ПДн;

- цель обработки ПДн;

- перечень ПДн, на обработку которых дается согласие субъекта ПДн;

- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

- срок, в течение которого действует согласие, а также порядок его отзыва;

- подпись субъекта ПДн.

Согласие на обработку ПДн может быть в любой момент отозвано.

7. ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В АДМИНИСТРАЦИИ БИРОФЕЛЬДСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ БИРОБИДЖАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА

ЕВРЕЙСКОЙ АВТОНОМНОЙ ОБЛАСТИ

7.1. Администрация обязана обеспечивать безопасность ПДн при их обработке, осуществлять защиту ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

7.2. Создание, изменение и чтение ПДн, обрабатываемых в Администрации, доступно только служащим, определенным настоящими Правилами.

7.3. Документы, содержащие персональные данные в Администрации, создаются:

7.3.1 в виде записей баз данных, ведущихся с использованием технических и программных средств автоматизированных систем, входящих в информационную систему персональных данных (далее по по тексту настоящих Правил – ИСПДн);

7.3.2 в виде отдельных файлов (doc, xls и т.п.), создаваемых ответственными лицами;

7.3.4 на бумажных носителях.

7.4. Доступ к техническим и программным средствам автоматизированных систем, входящих в ИСПДн, предоставляется на основании распоряжения главы Администрации.

7.5. Создание и хранение документов с ПДн в виде отдельных файлов (doc, xls и т.п.) допускается только на зарегистрированных отчуждаемых носителях ответственных лиц, с реализацией механизма разграничения доступа к ним.

8. ОРГАНИЗАЦИЯ ХРАНЕНИЯ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В АДМИНИСТРАЦИИ БИРОФЕЛЬДСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ БИРОБИДЖАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ЕВРЕЙСКОЙ АВТОНОМНОЙ ОБЛАСТИ

8.1. Бумажные документы, содержащие Пдн, обязаны храниться в местах хранения, запирающихся на ключ, сейфах, металлических шкафах и т.п.

8.2. При работе с документами, содержащими ПДн, запрещается:

8.2.1 хранить документы в ящиках стола, оставлять без присмотра;

8.2.2 брать документы для работы и на хранение домой;

8.2.3 выносить документы из помещений Администрации без разрешения главы Администрации;

8.2.4 держать документы вне сейфа без необходимости в процессе работы;

8.2.5 передавать документы на хранение лицам, не имеющим права доступа к данным документам.

8.3. Текущее хранение кадровых документов, содержащих Пдн, организует заместитель главы Администрации.

8.4. Текущее хранение бухгалтерских документов, содержащих ПДн, организует ведущий специалист 2 разряда, главный бухгалтер Администрации.

8.5. Текущее хранение документов воинского учета, содержащих Пдн, организует инспектор военно-учетного стола Администрации.

8.6. Все остальные документы, содержащие ПДн, должны храниться с соблюдением номенклатурных сроков и требованиями пункта 8.2 настоящих Правил хранения у должностных лиц Администрации, на которых нормативными правовыми или организационно-распорядительными актами Администрации возложено выполнение отдельных муниципальных функций, предусматривающих, помимо прочего, сбор, обработку и т.п. ПДн.

8.7. Подготовка документов к последующему хранению в архиве Администрации включает экспертизу практической ценности документов, оформление и описание дел, составление актов о выделении к уничтожению документов и передачу их в архив.

8.8. Экспертизу документов проводит постоянная экспертная комиссия. Передача дел в архив осуществляется по графику, утвержденному главой Администрации не реже, чем один раз в три года.

9. УНИЧТОЖЕНИЕ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В АДМИНИСТРАЦИИ БИРОФЕЛЬДСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ БИРОБИДЖАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ЕВРЕЙСКОЙ АВТОНОМНОЙ ОБЛАСТИ

9.1. Документы, содержащие ПДн временного хранения, как правило, в архив не передаются, а по истечении срока хранения уничтожаются.

9.2. К документам, содержащим ПДн временного характера, относятся документы, которые не должны храниться в архиве в обязательном порядке.

9.3. Для решения вопроса об уничтожении документов, содержащих ПДн временного характера, один раз в год собирается экспертная комиссия в составе не менее 2-х человек, определяемая распоряжением главы Администрации. Итоги работы комиссии оформляются актами об уничтожении документов, содержащих ПДн временного хранения.

9.4. В акте указывается дата и место его составления, состав комиссии, наименование уничтожаемых документов, их количество, количество страниц документов, предусмотренный срок хранения, подписи членов комиссии (не менее 2-х человек), ответственных за уничтожение документов, содержащие ПДн временного хранения.

9.5. Уничтожение документов, содержащих ПДн временного хранения, производится любым способом, исключающим ознакомление посторонних лиц с уничтожаемыми материалами и возможность восстановления их текста.

9.6. Акты об уничтожении документов, содержащих ПДн временного хранения, составляются и подшиваются в соответствующее дело.

10. РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИЕЙ БИРОФЕЛЬДСКОГО СЕЛЬСКОГО

ПОСЕЛЕНИЯ БИРОБИДЖАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ЕВРЕЙСКОЙ АВТОНОМНОЙ ОБЛАСТИ

10.1. По запросу служащего (приложение № 1 к настоящим Правилам) Администрация обязана не позднее 3-х дней со дня получения такого запроса выдать служащему копии документов на бумажном носителе, связанные с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы, выписки из трудовой книжки, периода работы у данного работодателя и др.). Предоставление ПДн служащих Администрации фиксируются в журнале учета выдачи/передачи ПДн служащих Администрации.

Копии документов, связанных с трудовой деятельностью в Администрации, заверяются надлежащим образом и предоставляются служащему Администрации безвозмездно.

10.2. В случае получения запроса от третьих лиц согласно приложению № 2 к настоящим Правилам, а в случае подачи запроса представителем – приложению № 3 к настоящим Правилам, на предоставление ПДн, Администрация обязана предоставить такие данные в сроки, установленные Правилами рассмотрения запросов субъектов персональных данных или их представителей в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области, утвержденными настоящим Постановлением.

10.3. Передача ПДн контрольно-надзорным органам и в государственные ИСПДн осуществляется в соответствии с действующим законодательством Российской Федерации.

10.4. Доступ к ПДн на основании и во исполнение федеральных законов предоставляется:

- Федеральной инспекции труда и федеральным органам исполнительной власти, осуществляющим функции по контролю и надзору в установленной сфере деятельности;

- Федеральной налоговой службе и межрегиональным инспекциям и управлениям ФНС РФ по субъектам Российской Федерации;

- Федеральной службе государственной статистики и её территориальным органам;

- Федеральному фонду обязательного медицинского страхования и его территориальным органам;

- Военным комиссариатам;

- Фонду социального страхования РФ;

- Пенсионному фонду РФ.

10.5. Передача ПДн муниципального служащего Администрации страховым компаниям, банкам, благотворительным организациям, негосударственным пенсионным фондам, посольствам, другим организациям; родственникам, членам семьи и другим лицам осуществляется по письменному запросу о их предоставлении на имя главы Администрации с указанием цели предоставления и запрашиваемого перечня ПДн. Передача ПДн осуществляется только при условии получения письменного согласия муниципального служащего Администрации, данные которого запрашиваются (отметка о согласии должна быть проставлена служащим на запросе), либо по его письменному заявлению.

10.6. Обо всех запросах о предоставлении ПДн должен быть уведомлен ответственный Администрации за организацию обработки и хранение персональных данных.

10.7. При обработке ПДн третьих лиц должны соблюдаться следующие требования:

- передача ПДн третьей стороне осуществляется на основании действующего законодательства Российской Федерации;

- обеспечение третьей стороной конфиденциальности и безопасности ПДн при их обработке (в договоре, если таковой имеется должны быть прописаны обязанности сторон по защите полученных ПДн);

- наличие письменного согласия субъекта ПДн.

10.8. Порядок действий с запросами от субъекта ПДн или его законного представителя на подтверждение наличия, ознакомление, уточнение, уничтожение или отзыв согласия на обработку ПДн дополнительно определен в Правилах рассмотрения запросов субъектов персональных данных или их представителей в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области, утвержденными настоящим Постановлением.

11. ПРАВА СУБЪЕКТОВ ПДН В ОТНОШЕНИИ

 СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Субъекты ПДн в отношении своих персональных данных имеют право на:

11.1.1 полную информацию о своих ПДн и их обработке;

11.1.2 свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, за исключением случаев, предусмотренных федеральным законом;

11.1.3 определение своих представителей для защиты своих ПДн;

11.1.4 требование об исключении или исправлении неверных или неполных ПДн, а также данных, обработанных с нарушением требований законодательства;

11.1.5 требование об извещении Администрацией лиц, неверно или неправильно извещенных о персональных данных субъекта ПДн, а также произведенных в них исключениях, исправлениях или дополнениях;

11.1.6 обжалование в суде любых неправомерных действий или бездействия Администрации при обработке или защите его ПДн.

11.2. При обработке ПДн Администрация обязана:

11.2.1 обеспечить защиту ПДн от их неправомерного использования или утраты в порядке, установленном законодательством Российской Федерации и требованиями регулирующих органов;

11.2.2 ознакомить субъекта ПДн или его законных представителей с его правами в области защиты ПДн на официальном сайте Администрации: E-mail adbirofeld@mail.ru;

11.2.3 осуществлять передачу ПДн третьих лиц только в соответствии с настоящими Правилами и законодательством Российской Федерации;

11.2.4 обеспечить субъекту ПДн доступ к своим персональным данным.

11.3. Нахождение в помещениях, в которых ведется обработка ПДн, третьих лиц, указанных в пункте 4.2. настоящих Правил, возможно только в присутствии муниципального служащего (должностного лица) Администрации, уполномоченного на обработку ПДн, и на время, ограниченное необходимостью решения вопросов, связанных с предоставлением персональных данных, предоставлением муниципальных услуг, осуществлением муниципальных функций.

11.4. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на муниципального служащего (должностного лица) Администрации, уполномоченного на обработку ПДн.

11.5. Право внутреннего доступа к персональным данным имеют только те муниципальные служащие Администрации, которым это необходимо для выполнения своих должностных обязанностей в рамках служебного контракта. Доступ к ИСПДн осуществляется на основании разрешительной системы доступа служащих Администрации к ИСПДн.

11.6. Ответственным за поддержание «Разрешительной системы допуска служащих Администрации к ИСПДн» в актуальном состоянии является заместитель главы Администрации.

11.7. Служащими Администрации, получающими доступ к ПДн, должна обеспечиваться конфиденциальность указанных данных.

11.8. Факт доступа служащих Администрации к ПДн, а также факты предоставления ПДн по запросам регистрируются автоматизированными средствами ИСПДн.

11.9. При обнаружении нарушений порядка предоставления ПДн субъекта ПДн служащий Администрации незамедлительно приостанавливает предоставление ПДн до выявления причин нарушений и устранения этих причин.

12. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ

РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

12.1. Пункты настоящих Правил обязательны для исполнения служащими Администрации, в обязанности которых входит обработка и защита персональных данных. Ознакомление служащих Администрации с настоящими Правилами организует заместитель главы Администрации.

12.2. Принципы работы с персональными данными в Администрации являются:

- постоянный контроль за состоянием работы с ПДн, осуществляемой служащими Администрации со стороны главы и заместителя главы Администрации;

- персональная ответственность служащих Администрации, в обязанности которых входит обработка и защита персональных данных, за нарушение настоящих Правилами.

12.3. Все служащие Администрации, должностные обязанности которых подразумевают возможность ознакомления с ПДн, при приеме на работу обязаны подписывать обязательство о неразглашении ПДн, ставших ему известными в связи с исполнением должностных обязанностей, согласно приложению № 4 к настоящим Правилам.

12.4. Обязанность по исполнению требований по нераспространению сведений, содержащих ПДн, сохраняется за бывшими служащими Администрации в течение всего срока действия конфиденциальности сведений.

12.5. Ответственным за информационную безопасность является заместитель главы Администрации, исполняющим следующие обязанности:

- ведение, обеспечение нормального функционирования и контроль за работой средств защиты информации в составе системы защиты информационных систем персональных данных;

- выборочный периодический контроль за соблюдением порядка обмена электронными копиями файлов, содержащими персональные данные.

- учет фактов утраты документов и разглашения сведений, содержащих персональные данные, анализ причин и разработка мер по предупреждению таких инцидентов;

- обеспечение учета сейфов, металлических шкафов, специальных хранилищ и помещений (а также ключей к ним), в которых осуществляется хранение и работа с документами, содержащими персональные данные.

12.6. На муниципальных служащих Администрации, осуществляющих обработку персональных данных, возлагаются следующие обязанности:

- принятие мер по предотвращению разглашения и утечки сведений, содержащих персональные данные;

- выполнение правил обращения с документами, содержащими персональные данные;

- соблюдение установленного порядка копирования учета, хранения и использования документов, содержащих персональные данные;

- соблюдение правил рассылки документов, содержащих персональные данные.

12.7. Служащие Администрации, в обязанности которых входит обработка и защита персональных данных, виновные в нарушении правил, регулирующих получение, обработку и защиту персональных данных, могут быть привлечены к ответственности в соответствии с действующим законодательством Российской Федерации.

13. ВЗАИМОДЕЙСТВИЕ С УПОЛНОМОЧЕННЫМИ ОРГАНАМИ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. В соответствии с законодательством Российской Федерации в области обеспечения безопасности персональных данных функции контроля и надзора за соответствием порядка обработки персональных данных требованиям действующего законодательства возлагаются на федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, контроля и надзора в сфере информационных технологий и связи.

13.2. Взаимодействие с уполномоченными органами организуется в пределах:

13.2.1 с территориальными органами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) по вопросам:

- предоставления информации, необходимой для реализации полномочий;

- осуществления проверочных и контрольных мероприятий в пределах предоставленных полномочий;

- выполнения требований об уточнении, блокировании или уничтожении недостоверных или полученных незаконным путем ПДн;

- принятия в установленном законодательством Российской Федерации порядке мер по приостановлению или прекращению обработки ПДн.

13.2.2 с территориальными органами Федеральной службы по техническому и экспортному контролю (ФСТЭК России) по вопросам:

- предоставления информации, необходимой для реализации полномочий и осуществления проверочных и контрольных мероприятий;

- организации и проведения мероприятий, направленных на обеспечение безопасности ПДн при их обработке в ИСПДн.

13.2.3 с территориальными органами Федеральной службы безопасности (ФСБ России) по вопросам:

- предоставления информации, необходимой для реализации полномочий и осуществления проверочных и контрольных мероприятий;

- организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для обеспечения безопасности персональных данных при их обработке в ИСПДн.

13.3. Организация взаимодействия с уполномоченными органами в области обеспечения безопасности ПДн возлагается на заместителя главы Администрации.

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящие Правила доводятся до всех служащих Администрации под роспись при приеме на работу.

Приложение № 1

к Правилам обработки персональных данных,

устанавливающих процедуры, направленные на выявление

 и предотвращение нарушений законодательства Российской

Федерации в сфере персональных данных в администрации

Бирофельдского сельского поселения Биробиджанского

муниципального района Еврейской автономной области

Главе администрации

Бирофельдского сельского поселения

Биробиджанского муниципального района
Еврейской автономной области

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность, фамилия, имя, отчество)

**ЗАПРОС**

Я, состою в трудовых отношениях с администрацией Бирофельдского сельского поселения на основании трудового контракта от \_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_.

С целью\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать цель обращения

прошу Вас предоставить мне следующую информацию о персональных данных:

1)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;2)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;3)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;4)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_ года \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

Приложение № 2

к Правилам обработки персональных данных,

устанавливающих процедуры, направленные на выявление

 и предотвращение нарушений законодательства Российской

Федерации в сфере персональных данных в администрации

Бирофельдского сельского поселения Биробиджанского

муниципального района Еврейской автономной области

Главе администрации

Бирофельдского сельского поселения

Биробиджанского муниципального района
Еврейской автономной области

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (фамилия, имя, отчество)

проживающего по адресу:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**ЗАПРОС**

С целью\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать цель обращения

прошу Вас предоставить мне следующую информацию о персональных данных:

1)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;2)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;3)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;4)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

документ, удостоверяющий личность \_\_\_\_\_\_\_\_\_\_\_\_\_\_ серия \_\_\_\_\_\_\_\_\_\_\_ №\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_выдан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 (наименование органа, выдавшего документ и дата его выдачи)

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_ года \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

Приложение № 3

к Правилам обработки персональных данных,

устанавливающих процедуры, направленные на выявление

 и предотвращение нарушений законодательства Российской

Федерации в сфере персональных данных в администрации

Бирофельдского сельского поселения Биробиджанского

муниципального района Еврейской автономной области

Главе администрации

Бирофельдского сельского поселения

Биробиджанского муниципального района
Еврейской автономной области

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (фамилия, имя, отчество,

действующего в интересах:\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя отчество)

проживающего по адресу:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

 (указать адрес представляемого лица)

**ЗАПРОС**

С целью\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать цель обращения

прошу Вас предоставить следующую информацию о персональных данных:

1)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;2)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;3)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;4)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

документ, удостоверяющий личность представляемого лица \_\_\_\_\_\_\_\_\_\_\_\_\_\_ серия \_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_\_\_\_\_\_выдан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 (наименование органа, выдавшего документ и дата его выдачи)

Приложение: доверенность на \_\_\_\_\_ л. в 1 экз.

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_ года \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

Приложение № 4

к Правилам обработки персональных данных,

устанавливающих процедуры, направленные на выявление

 и предотвращение нарушений законодательства Российской

Федерации в сфере персональных данных в администрации

Бирофельдского сельского поселения Биробиджанского

муниципального района Еврейской автономной области

**ТИПОВОЕ ОБЯЗАТЕЛЬСТВО**

**муниципального служащего администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области, непосредственно осуществляющего обработку**

**персональных данных, о неразглашении ставших известными**

**ему в связи с исполнением должностных обязанностей**

**в случае расторжения с ним трудового договора**

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

 (фамилия, имя, отчество)

оформляясь на должность\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать должность)

администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области (далее –Администрация), поставлен (а) в известность о том, что по роду своей деятельности и должностным обязанностям буду допущен (а) к обработке персональных данных.

В соответствии с Законом Российской Федерации «О персональных данных» и иными нормативными правовыми актами о персональных данных, с которыми меня ознакомили и разъяснили, принимаю на себя обязательство по неразглашению доверенных мне сведений содержащих персональные данные сотрудников администрации и иных субъектов.

Принимаю на себя обязательства по соблюдению требований законодательства Российской Федерации о персональных данных, а в случае попытки посторонних лиц получить информацию конфиденциального характера – немедленно сообщить об этом главе Администрации.

Я предупрежден (а) о том, что случае даже однократного нарушения принятых на себя обязательств буду отстранен (а) от работы со сведениями, содержащими персональные данные, а трудовой договор со мной может быть расторгнут.

Мне известно, что в случае отстранения от работы с персональными данными я не освобождаюсь от взятых обязательств по неразглашению сведений, содержащих персональные данные.

Обязуюсь добросовестно выполнять свои обязательства, строго охранять доверенные мне сведения, содержащие персональные данные.

Я предупрежден (а), что за разглашение сведений содержащих персональные данные, или утрату носителей сведений, содержащих персональные данные, а также за нарушение режима конфиденциальности буду привлечен (а) к ответственности в соответствии с законодательством Российской Федерации.

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_ года \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

Приложение № 5

к Правилам обработки персональных данных,

устанавливающих процедуры, направленные на выявление

 и предотвращение нарушений законодательства Российской

Федерации в сфере персональных данных в администрации

Бирофельдского сельского поселения Биробиджанского

муниципального района Еврейской автономной области

Главе администрации

Бирофельдского сельского поселения

Биробиджанского муниципального района
Еврейской автономной области

**ТИПОВОЕ СОГЛАСИЕ**

**на обработку персональных данных субъекта**

«Я (ФИО полностью), паспорт (иной документ, удостоверяющий личность) серия\_\_\_\_\_\_№\_\_\_\_\_\_\_\_\_\_, выдан (кем и когда), проживающий по адресу\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ года рождения, контактный телефон\_\_\_\_\_\_\_\_\_\_\_\_ настоящим подтверждаю свое согласие на обработку администрацией Бирофельдского сельского поселения (далее – Администрация), моих персональных данных в целях \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, а также в целях соблюдения требований действующего законодательства.

Мои персональные данные включают в себя: фамилию, имя, отчество, дату рождения, адрес проживания, контактный телефон, паспортные данные, ИНН и СНИЛС.

Я даю согласие на получения моих персональных данных у третьей стороны, в случае возникновения необходимости.

Администрация вправе осуществлять все необходимые действия с моими персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (УФНС, ПФР, ФСС и т.д.), обезличивание, блокирование, уничтожение, внесение в информационную систему, обработку с использованием средств автоматизации или без использования таких средств.

Передача моих персональных данных иным лицам или их разглашение может осуществляться только с моего письменного согласия.

Администрация может осуществлять обработку моих персональных данных в течение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_срока.

Я вправе отозвать свое согласие на обработку персональных данных посредством соответствующего письменного заявления.

Данное согласие передано мной в момент подписания Трудового договора.

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_ года \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

ПРИЛОЖЕНИЕ № 3

к постановлению администрации

Бирофельдского сельского поселения

от 24.06.2019 № 67

**ПРАВИЛА**

**рассмотрения запросов субъектов персональных данных**

**или их представителей в администрации Бирофельдского сельского поселения** **Биробиджанского** **муниципального** **района**

**Еврейской автономной области**

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящие Правила разработаны в соответствии с Конституцией РФ, Гражданским кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и иными нормативными правовыми актами Российской Федерации в области защиты персональных данных.

1.2. Настоящие Правила регулирует отношения, возникающие при выполнении администрацией Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области (далее по тексту настоящих Правил – Администрация) обязательств согласно требованиям статей 14, 20 и 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Положения настоящих Правил распространяются на действия Администрации при обращении либо при получении запроса субъекта персональных данных или его представителя. Эти действия направлены на подтверждение наличия, ознакомление, уточнение, уничтожение или отзыв согласия на обработку персональных данных, а также на устранение нарушений законодательства, допущенных при обработке персональных данных.

2. ОТВЕТСТВЕННОСТЬ

2.1. Ответственность за корректировку, проверку и пересмотр настоящих Правил несет специалист-эксперт, юрист Администрации.

2.2. Ответственность за организацию и проведение работ по ответам на запросы, устранению нарушений, а также уточнению, блокированию, уничтожению персональных данных (далее по тексту настоящих Правил – ПДн) и правильное применение настоящих Правил возлагается на муниципальных служащих Администрации, осуществляющих обработку ПДн, в должностные обязанности которых входит их обработка.

3. ДЕЙСТВИЯ В ОТВЕТ НА ЗАПРОСЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Субъект ПДн или его представитель имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение обработки ПДн, а также цель такой обработки;

- способы обработки ПДн;

- сведения о лицах, которые имеют доступ к ПДн;

- перечень обрабатываемых ПДн и источник их получения;

- сроки обработки ПДн, в том числе сроки их хранения;

- юридические последствия для субъекта ПДн обработки его ПДн.

3.2. В случае поступления нижеуказанного запроса субъекта ПДн или его представителя (приложение № 2 и № 3 к настоящим Правилам) необходимо выполнить следующие действия:

3.2.1 при получении запроса на наличие ПДн необходимо в течение 30 дней (согласно части 1 статьи 20 Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) подтвердить обработку ПДн в случае ее осуществления. Если обработка ПДн субъекта не ведется, то в течение 30 дней (согласно части 2 статьи 20 Закона № 152-ФЗ) необходимо отправить уведомление об отказе подтверждения обработки ПДн;

3.2.2 при получении запроса на ознакомление с ПДн необходимо в течение 30 дней (согласно части 1 статьи 20 Закона № 152-ФЗ) предоставить для ознакомления ПДн в случае осуществления обработки этих ПДн. Если обработка ПДн субъекта не ведется, то в течение 30 дней (согласно части 2 статьи 20 Закона № 152-ФЗ) необходимо отправить уведомление об отказе предоставления информации по ПДн.

3.2.3 при получении запроса на уточнение ПДн в срок не превышающий 7 рабочих дней необходимо внести в них необходимые изменения, по предоставлению субъектом ПДн или его представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно части 3 статьи 20 Закона № 152-ФЗ) и отправить уведомление о внесенных изменениях. Если обработка ПДн субъекта не ведется или нет сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, то необходимо отправить уведомление об отказе осуществления изменения ПДн;

3.2.4 при получении запроса на уничтожение ПДн в срок, не превышающий 7 рабочих дней необходимо их уничтожить, по предоставлению субъектом ПДн или его представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно части 3 статьи 20 Закона №152-ФЗ) и отправить уведомление об уничтожении, а если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в силу необходимости обработки ПДн по требованиям иных законодательных актов, то необходимо отправить уведомление об отказе уничтожения ПДн;

3.2.5 при получении запроса на отзыв согласия на обработку ПДн в срок не превышающий 30 дней необходимо их уничтожить (согласно части 5 статьи 21 Закона № 152-ФЗ) и отправить уведомление об уничтожении, а если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в силу необходимости обработки ПДн по требованиям иных законодательных актов, то необходимо отправить уведомление об отказе уничтожения;

3.2.6 при выявлении недостоверности ПДн при обращении или по запросу субъекта ПДн или его представителя необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Закона 152-ФЗ); если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его законным представителем, необходимо уточнить ПДн и снять их блокирование; если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения ПДн;

3.2.7 при выявлении неправомерных действий Администрации с ПДн при обращении или по запросу субъекта ПДн или его законного представителя необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Закона152-ФЗ); если факт неправомерности действий с ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его законным представителем, необходимо в течение 3 рабочих дней (согласно части 3 статьи 21 Закона 152-ФЗ) устранить допущенные нарушения; если невозможно устранить допущенные нарушения Администрации, то в срок, не превышающий 3 рабочих дней с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн.

3.3. В случае поступления нижеуказанного запроса Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее по тексту настоящих Правил – Уполномоченный орган) необходимо выполнить следующие действия:

3.3.1 при получении запроса необходимо в течение 30 дней (согласно части 4 статьи 20 Закона 152-ФЗ) предоставить информацию, необходимую для осуществления деятельности указанного органа;

3.3.2 при выявлении недостоверных ПДн при обращении или по запросу Уполномоченного органа необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Закона 152-ФЗ); если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его представителем, необходимо уточнить ПДн и снять их блокирование; если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения;

3.3.3 при выявлении неправомерных действий Администрации с ПДн при обращении или по запросу Уполномоченного органа необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно части 1 статьи 21 Закона 152-ФЗ); если факт неправомерности действий с ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его законным представителем, необходимо в течение 3 рабочих дней (согласно части 3 статьи 21 152-ФЗ) устранить допущенные нарушения; если невозможно устранить допущенные нарушения Администрации, то в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн.

3.4. При достижении целей обработки ПДн Администрация обязана незамедлительно прекратить обработку ПДн, уничтожить соответствующие ПДн в течение 30 дней с даты достижения цели обработки ПДн (согласно части 4 статьи 21 Закона 152-ФЗ), если иное не предусмотрено федеральными законами, и отправить уведомление об уничтожении ПДн.

3.5. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в подпунктах 3.2.4, 3.2.5, 3.2.7 и 3.3.3 настоящих Правил, осуществляется блокирование таких ПДн и обеспечивается их уничтожение в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

3.6. Сводная таблица действий Администрации в ответ на запрос ПДн указана в приложении № 1 настоящими Правилами.

4. ПРИЕМ ЗАПРОСОВ ОТ СУБЪЕКТА ПЕРСОНАЛЬНЫХ

ДАННЫХ ИЛИ ЕГО ПРЕДСТАВИТЕЛЕЙ, А ТАКЖЕ

ОТ УПОЛНОМОЧЕННОГО ОРГАНА

4.1. При получении запросов, перечисленных в разделе 3 настоящих Правил, служащий Администрации, в чьи должностные обязанности входит прием входящей корреспонденции или служащий Администрации, уполномоченный на обработку и хранение соответствующих ПДн по запросу, выполняют следующие действия:

4.1.1 в случае поступления запроса субъекта ПДн или его представителя необходимо зарегистрировать запрос в «Журнале учета входящей корреспонденции»;

4.1.2 при личном обращении субъекта ПДн в Администрацию, принимает запрос в произвольной форме и сверяет сведения, указанные в запросе, с предоставленными ему документами.

4.2. В подаваемом субъектом ПДн запросе указываются следующие сведения и данные:

- фамилия, имя и отчество субъекта ПДн;

- номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, собственноручная подпись субъекта персональных данных или его законного представителя;

- состоит ли субъект ПДн в договорных отношениях с Администрацией;

- сведения о заключенных договорах между Администрацией и субъектом ПДн.

- иные сведения о взаимоотношениях субъекта ПДн с Администрацией.

4.3. При подачи неправильно заполненной формы запроса служащие, отмеченные в пункте 4.1 настоящих Правил, указывают на это обстоятельство подающему запрос. При отказе субъекта ПДн или его представителя привести запрос в надлежащую форму, принимают запрос и делают соответствующую отметку в «Журнале учета входящей корреспонденции».

4.4. Отсутствия документов, удостоверяющих личность субъекта ПДн или его представителя, при подаче запроса является основанием для отказа в его приеме.

4.5. Запрос, поданный в надлежащей форме, после регистрации в «Журнале учета входящей корреспонденции» передается служащему Администрации, уполномоченному за обработку и хранение персональных данных, в случае его приема и регистрации служащим Администрации, в чьи должностные обязанности входит прием входящей корреспонденции.

4.6. Поступивший запрос Уполномоченного органа регистрируется в «Журнале учета входящей корреспонденции» и передается служащему, указанному в пункте 4.5 настоящих Правил, в случае его приема и регистрации служащим Администрации, в чьи должностные обязанности входит прием входящей корреспонденции или регистрируется и принимается для отработки служащим Администрации, уполномоченный на обработку и хранение соответствующих ПДн по запросу.

Приложение № 1

к Правилам рассмотрения запросов субъектов

персональных данных или их представителей

в администрации Бирофельдского сельского поселения

Биробиджанского муниципального района

Еврейской автономной области

**СВОДНАЯ ТАБЛИЦА**

**действий в ответ на запросы персональных данных**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | НАИМЕНОВАНИЕ ЗАПРОСА  | ДЕЙСТВИЯ ПО ОБРАБОТКЕ | СРОК ИСПОЛНЕНИЯ | ОТВЕТ НА ЗАПРОС |
| 1.Запрос Субъекта персональных данных (далее по тексту настоящей таблицы – ПДн) или его Представителя |
| 1.1. | Наличие ПДн  | Подтверждение обработки ПДн  | 30 дней (пункт 1 статьи 20)\* | Подтверждение обработки ПДн  |
| Отказ подтверждения обработки ПДн  | 30 дней (пункт 2 статьи 20) | Уведомление об отказе подтверждения обработки ПДн  |
| 1.2. | Ознакомление с ПДн  | Предоставление информации по ПДн  | 7 дней (пункт 3 статьи 20) | 1. Подтверждение обработки ПДн, а также цель такой обработки  |
| 2. Способы обработки ПДн  |
| 3.Сведения о лицах, которые имеют доступ к ПДн  |
| 4. Перечень обрабатываемых ПДн и источник их получения  |
| 5. Сроки обработки ПДн, в том числе сроки их хранения  |
| 6. Юридические последствия для субъекта ПДн обработки его ПДн  |
| Отказ предоставления информации по ПДн  | 7 дней (пункт 3 статьи 20) | Уведомление об отказе предоставления информации по ПДн  |
| 1.3. | Уточнение ПДн | Блокировка ПДн Изменение ПДн Снятие блокировки ПДн | Период проверки достоверности ПДн  | Уведомление о внесенных изменениях  |
| Отказ изменения ПДн  | По предоставлению сведений по ПДн, подтверждающих неполноту, устаревание, недостоверность, незаконность получения или отсутствие необходимости для заявленных целей обработки  | Уведомление об отказе предоставления изменения ПДн  |
| 1.4. | Уничтожение ПДн  | Блокировка ПДн Уничтожение ПДн  | Период проверки достоверности ПДн  | Уведомление об уничтожении  |
| Отказ уничтожения ПДн |  | Уведомление об отказе уничтожения ПДн  |
| 1.5. | Отзыв согласия на обработку ПДн  | Блокировка ПДн Уничтожение ПДн  | 30 дней (пункт 5 статьи 21) | Уведомление о прекращении обработки и уничтожении ПДн  |
| Отказ прекращения обработки и уничтожения ПДн  | 30 дней (пункт 5 статьи 21) | Уведомление об отказе прекращения обработки и уничтожения ПДн  |
| 1.6. | Недостоверность ПДн Субъекта  | Блокировка ПДн Изменение ПДн Снятие блокировки ПДн  | Период проверки достоверности ПДн  | Уведомление о внесенных изменениях  |
| Отказ изменения ПДн  | Период проверки достоверности ПДн  | Уведомление об отказе изменения ПДн  |
| 1.7. | Неправомерность действий с ПДн Субъекта  | Устранение нарушений  | 3 рабочих дня (пункт 3 статьи 21) | Уведомление об устранении нарушений  |
| Уничтожение ПДн  | 3 рабочих дня (пункт 3 статьи 21) | Уведомление об уничтожении ПДн  |
| 1.8. | Достижение целей обработки ПДн Субъекта  | Блокировка ПДн Уничтожение ПДн  | 30 дней (пункт 4 статьи 21) | Уведомление об уничтожении ПДн  |
| 2. Запрос уполномоченного органа по защите прав Субъекта ПДн |
| 2.1. | Информация для осуществления деятельности уполномоченного органа  | Предоставление затребованной информации по ПДн  | 30 дней (пункт 4 статьи 20) | Предоставление затребованной информации по ПДн  |
| 2.2. | Недостоверность ПДн Субъекта  | Блокировка ПДн Изменение ПДн Снятие блокировки ПДн  | Период проверки достоверности ПДн  | Уведомление о внесенных изменениях  |
| Отказ изменения ПДн  | Период проверки достоверности ПДн  | Уведомление об отказе изменения ПДн  |
| 2.3. | Неправомерность действий с ПДн Субъекта  | Устранение нарушений  | 3 рабочих дня (пункт 3 статьи 21) | Уведомление об устранении нарушений  |
| Уничтожение ПДн  | 3 рабочих дня (пункт 3 статьи 21) | Уведомление об уничтожении ПДн  |
| 2.4. | Достижение целей обработки ПДн Субъекта  | Блокировка ПДн Уничтожение ПДн  | 3 рабочих дня (пункт 4 статьи 21) | Уведомление об уничтожении ПДн  |

\*Ссылки на пункты и номера статей приведены для Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Приложение № 2

к Правилам рассмотрения запросов субъектов

персональных данных или их представителей

в администрации Бирофельдского сельского поселения

Биробиджанского муниципального района

Еврейской автономной области

Главе администрации

Бирофельдского сельского поселения

Биробиджанского муниципального района
Еврейской автономной области

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (фамилия, имя, отчество)

проживающего по адресу:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**ЗАПРОС**

С целью\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать цель обращения

прошу Вас (указать нужное):

- предоставить следующую информацию о наличии ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; - предоставить следующие документы на ознакомление с ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_; - уточнить следующие сведения ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

- уничтожить ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

- отозвать согласие на обработку ПДн;

- произвести следующие изменения в ПДн,в связи с их недостоверностью\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

- устранить следующие допущенные нарушения неправомерными действиями Администрации с ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Документ, удостоверяющий личность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_серия \_\_\_\_\_\_ \_\_\_\_\_\_\_№\_\_\_\_\_\_\_\_\_\_ выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 (наименование органа, выдавшего документ и дата его выдачи)

Сведения о взаимоотношениях субъекта ПДн с Администрацией\_\_\_\_\_\_\_

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

 (договорные отношения с указанием данных договора или иные)

Приложение: документы, подтверждающие основания для внесения изменений в ПДн или неправомерность действий Администрации (предоставляются подавшим запрос).

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_ года \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

Приложение № 3

к Правилам рассмотрения запросов субъектов

персональных данных или их представителей

в администрации Бирофельдского сельского поселения

Биробиджанского муниципального района

Еврейской автономной области

Главе администрации

Бирофельдского сельского поселения

Биробиджанского муниципального района
Еврейской автономной области

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (фамилия, имя, отчество,

действующего в интересах:\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя отчество)

проживающего по адресу:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

 (указать адрес представляемого лица)

**ЗАПРОС**

С целью\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (указать цель обращения

прошу Вас (указать нужное):

- предоставить следующую информацию о наличии ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; - предоставить следующие документы на ознакомление с ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_; - уточнить следующие сведения ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

- уничтожить ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

- отозвать согласие на обработку ПДн;

- произвести следующие изменения в ПДн,в связи с их недостоверностью\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

- устранить следующие допущенные нарушения неправомерными действиями Администрации с ПДн\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Документ, удостоверяющий личность представляемого лица\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_серия \_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_\_\_\_\_\_ выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

 (наименование органа, выдавшего документ и дата его выдачи)

Сведения о взаимоотношениях субъекта ПДн с Администрацией\_\_\_\_\_\_\_

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

 (договорные отношения с указанием данных договора или иные)

Приложение:

1. Доверенность на \_\_\_\_\_ л. в 1 экз.

2. Документы, подтверждающие основания для внесения изменений в ПДн или неправомерность действий Администрации (предоставляются подавшим запрос).

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_ года \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

ПРИЛОЖЕНИЕ № 4

к постановлению администрации

Бирофельдского сельского поселения

от 24.06.2019 № 67

**ПЕРЕЧЕНЬ**

**информационных систем персональных данных в администрации**

**Бирофельдского сельского поселения Биробиджанского**

**муниципального района Еврейской автономной области**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №п/п  | Наименование ИС  | Перечень ИСПДн, входящих в состав ИС  | Масштаб/количество АРМ в ИС  | Адрес объекта  | Должность, ответственного за работу ИС  |
| 1  | «Бухгалтерия» | «Смета», «ДОК ПУ 5», «Налогоплательщик ЮЛ». | объектовый/2АРМ N 1; N 2  | с. Бирофельд, ул. Центральная,дом 45 |  Ведущий специалист 2 разряда, главный бухгалтер; ведущий специалист 2 разряда  |
| 2  | «Вопросы семьи и молодежи» | «Списки», «Акты», «Ответы на обращения граждан», «Характеристики», «Протоколы КДН и ЗП», ПостановленияКДН и ЗП», «Списки» | объектовый/1АРМ N 3  | с. Бирофельд, ул. Центральная,дом 45 | Заместитель главы  |
| 3  | Административная комиссия  | «Административныепротоколы, контрактная и договорная деятельность» | объектовый/1АРМ N 4  | с. Бирофельд, ул. Центральная,дом 45 | Специалист-эксперт, юрист |
| 4  | «Кадры» | «Кадры» | объектовый/1АРМ N 3  | с. Бирофельд, ул. Центральная,дом 45 | Заместитель главы |
| 5 | «Обращения граждан» | «Обращения граждан» | объектовый/1АРМ N 3  | с. Бирофельд, ул. Центральная,дом 45 | Заместитель главы |
| 6  | «ЖКХ» | «Письма» | объектовый/1АРМ N 3  | с. Бирофельд, ул. Центральная,дом 45 | Заместитель главы |
| 7 | «Воинский учет» | «Отчеты, списки военнообязанных, снятых с учета» | объектовый/1АРМ N 4  | с. Бирофельд, ул. Центральная,дом 45 | Инспектор ВУС |
| 8. | «Торги, муниципальные контракты, суды» | «Отчеты, муниципальные контракты, услуги, документы для суда» | объектовый/1АРМ N 5  | с. Бирофельд, ул. Центральная,дом 45 | Специалист-эксперт, юрист |
| 9. | «Документация о регистрации права собственности» | «Свидетельства, выписки из ЕГРН» | объектовый/1АРМ N 5  | с. Бирофельд, ул. Центральная,дом 45 | Специалист 1 разряда, землеустроитель |

ПРИЛОЖЕНИЕ № 5

к постановлению администрации

Бирофельдского сельского поселения

от 24.06.2019 № 67

**ПЕРЕЧЕНЬ**

**персональных данных, обрабатываемых в администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области в связи с реализацией трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Должность сотрудника, осуществляющего обработку ПДн | Способ обработки | Состав ПДн | Цель обработки | Основание обработки | Сроки обработки |
| 1. | Заместитель главы | Смешанный | ФИО, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, копия паспорта, паспортные данные, пол, гражданство, сведения о регистрации по месту жительства и временной регистрации по месту пребывания, номер телефона, адрес электронной почты, место работы или учебы членов семьи и родственников, должность, стаж работы, сведения о наградах (поощрениях), почетных званиях, сведения о социальных гарантиях, сведения о признании за гражданином права пользования жилым помещением, сведения о праве пользования жилым помещением, сведения о размере пенсии, сведения о социальных выплатах, о смерти, дата смерти, о судимости, сведения о дееспособности/недееспособности, ИНН физического лица, ИНН индивидуального предпринимателя, сведения из страхового свидетельства обязательного пенсионного страхования, копия паспортаФИО, дата рождения, паспортные данные, номер телефона, место работы, должность, ИНН физического лицаФИО, дата и место рождения, паспортные данные, сведения о регистрации по месту жительства и о временной регистрации по месту пребывания, сведения о воинском учете, сведения и призыве на военную службу, сведения о смерти, дата смерти, сведения о дееспособности/недееспособностиФИО, год рождения, месяц рождения, дата рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, анкетные и биографические данные, сведения о рождении детей, паспортные данные,, фото на анкете в личном деле, пол, гражданство, сведения о регистрации по месту жительства и временной регистрации по месту пребывания, номер телефона, специальность, место работы или учебы членов семьи и родственников, должность, стаж работы, сведения о повышении квалификации, сведения о профессиональной переподготовке, сведения о прохождении курсов подготовки специалистов, знание иностранного языка, сведения о наградах (поощрениях), почетных званиях, сведения об отпусках, сведения о социальных гарантиях, сведения из трудовой книжки, сведения из страхового свидетельства обязательного пенсионного страхования, сведения из свидетельства по постановке физического лица на учет в налоговом органе, медицинское заключение об отсутствии заболевания, препятствующего поступлению на муниципальную службу, сведения о доходах всех членов семьи за год, сведения из налоговых деклараций о доходах за расчетный период, сведения о социальных выплатах.ФИО, номер телефона, должность, сведения о повышении квалификации | Рассмотрение обращений гражданПроведение спортивных мероприятий, заключение договоров по аренде спортивного зала, организация награждения победителей и призеров, официальных физкультурно-спортивных мероприятий, физических лиц за высокие спортивные достижения на территории поселенияОсуществление учета участников референдума, проживающих на территории Бирофельдского сельского поселения, сбор и обработка данных об избирателях для последующей передачи их в участковую избирательную комиссию Учет прохождения муниципальнойслужбы служащими администрации Бирофельдского сельского поселения, формирование кадрового резерва для замещения должностей муниципальнойслужбы, ведение трудовых книжек муниципальныхслужащих, ведение личных дел муниципальныхслужащих, ведение реестра муниципальныхслужащих, оформление и выдача служебных удостоверений муниципальных служащих, проведение конкурса на замещение вакантных должностей муниципальнойслужбы и включение муниципальныхслужащих в кадровый резерв, проведение аттестации муниципальных служащих, проведение квалификационных экзаменов муниципальных служащих администрации в целях присвоения им классных чинов, установление надбавок за выслугу лет на муниципальной службе, присвоение иных надбавок и доплат, проверка достоверности и полноты сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых муниципальными служащими администрации, чьи должности включены в утвержденный перечень должностей, поощрение и награждение муниципальных служащих, применении к ним дисциплинарных взысканий, заключение трудовых договоров с гражданами при приеме их на работу, составление табеля учета рабочего времени, графика ежегодных оплачиваемых отпусков, оформления документов для выезда в служебные командировки, определение стажа муниципальнойслужбы, установления доплат к трудовым пенсиям муниципальнымслужащим, имеющим на это право, увольняемым из администрации, анализ уровня профессионального образования муниципальныхслужащих, его соответствия квалификационным требованиям, предъявляемым к замещаемым ими должностям муниципальнойслужбы, в целях проведения работы по планированию направления муниципальныхслужащих для прохождения дополнительного профессионального образования, подготовка материалов по представлению к награждению государственными наградами Российской Федерации, области и главы Бирофельдского сельского поселения, ведение учета лиц, награжденных наградами главы Бирофельдского сельского поселения. Кадровое делопроизводство на директора МКУ «Поселенческий Дом культуры с. Бирофельд»Участие в расследовании тяжелых, смертельных и групповых, с тяжелыми последствиями, расследование несчастных случаев на производстве в администрации Бирофельдского сельского поселения, МКУ «Поселенческий Дом культуры с. Бирофельд». Ведение банка данных по о прохождении обучения по охране труда, о проведении специальной оценки условий труда  | Конституция РФ, Устав Бирофельдского сельского поселения, ФЗ от 06.10.2003 N 131-ФЗ «Об общих принципах организации местного самоуправления в РФ», ФЗ от 02.05.2006 N 59-ФЗ «О порядке рассмотрения обращений граждан РФ», ФЗ от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»ФЗ от 04.12.2007 N 329-ФЗ «О физической культуре и спорте в РФ», ФЗ от 06.10.2003 N 131-ФЗ «Об общих принципах организации местного самоуправления в РФ»ФЗ от 12.06.2002 N 67-ФЗ «Об основных гарантиях прав и права на участие в референдуме граждан РФ», постановлениегубернатора ЕАО от 19.05.2011 N 179 «О мерах по реализации Положения о Государственной системе регистрации (учета) избирателей, участников референдума в Российской Федерации на территории ЕАО», постановлениеизбирательной комиссии ЕАО от 28.04.2011 N 77/326 «Об обеспечении функционирования Государственной системы регистрации (учета) избирателей, участников референдума на территории ЕАО»Конституция РФ, Трудовой кодекс РФ, Гражданский кодекс РФ, Налоговый кодекс РФ, Устав МО «Бирофельдское сельское поселение», ФЗ от 02.03.2007 N 25-ФЗ «О муниципальнойслужбе», ФЗ от 15.12.2001 N 167-ФЗ «Об обязательном пенсионном страховании в РФ», ФЗ от 16.07.1999 N 165-ФЗ «Об основах обязательного социального страхования», ФЗ от 29.11.2010 N 326-ФЗ «Об обязательном медицинском страховании в РФТрудовой кодекс РФ | Постоянно (предложения, письма творческого характера, заявления, жалобы содержащие сведения о серьезных недостатках и злоупотреблени-ях, коррупции.5 лет (личного характера)5 лет5 лет75 лет45 лет,до минования надобности |
| 2. | Ведущий специалист 2 разряда, главный бухгалтер  | Смешанный  | ФИО, дата рождения, профессия, доходы, копия паспорта, сведения о рождении детей, должность, стаж работы, сведения о повышении квалификации, сведения о поощрениях, сведения об отпусках, сведения о социальных гарантиях, сведения из страхового свидетельства обязательного пенсионного страхования, сведения из свидетельства о постановке на учет в налоговом органе, сведения из налоговых деклараций о доходах за расчетный период, сведения о размере пенсии, ИНН, реквизиты банковских счетовПаспортные данные, ИНН индивидуального предпринимателя, выписки из ЕГРИП, номер банковского счета, номер расчетного счета | Бухгалтерский и налоговый учет. Бухгалтерское обслуживание МКУ «Поселенческий Дом культуры с. Бирофельд», Собрание депутатов.Заключение договоров, расчеты с контрагентами.Заключение контрактов для муниципальныхнужд | Трудовой кодекс, Налоговый кодекс, ФЗ от 21.11.1996 N 129-ФЗ «О бухгалтерском учете», ФЗ от 06.10.2003 N 131-ФЗ «Об общих принципах организации местного самоуправления в РФ», ФЗ от 15.12.2001 N 167-ФЗ «Об обязательном пенсионном страховании в РФ»ФЗ от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ услуг для обеспечения государственных и муниципальныхнужд» | 75 лет5 лет 5 лет |
| 3.  | Ведущий специалист 2 разряда  | Смешанный  | ФИО, дата рождения, профессия, доходы, копия паспорта, сведения о рождении детей, должность, стаж работы, сведения о повышении квалификации, сведения о поощрениях, сведения об отпусках, сведения о социальных гарантиях, сведения из страхового свидетельства обязательного пенсионного страхования, сведения из свидетельства о постановке на учет в налоговом органе, сведения из налоговых деклараций о доходах за расчетный период, сведения о размере пенсии, ИНН, реквизиты банковских счетов Паспортные данные, ИНН индивидуального предпринимателя, копия выписки из ЕГРИП, номер банковского счета, номер расчетного счета | Бухгалтерский и налоговый учет. Бухгалтерское обслуживание МКУ «Поселенческий Дом культуры с. Бирофельд», Собрание депутатов.Заключение контрактов, расчеты с контрагентами.Заключение контрактов для муниципальныхнужд | Трудовой кодекс, Налоговый кодекс, ФЗ от 21.11.1996 N 129-ФЗ «О бухгалтерском учете», ФЗ от 06.10.2003 N 131-ФЗ «Об общих принципах организации местного самоуправления в РФ», ФЗ от 15.12.2001 N 167-ФЗ «Об обязательном пенсионном страховании в РФ»ФЗ от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ услуг для обеспечения государственных и муниципальныхнужд» | 75 лет,5 лет 5 лет |
| 4.  | Специалист-эксперт, юрист | Смешанный | ФИО, год рождения, дата рождения, паспортные данные, адрес, социальное положение, копии паспорта, анкетные и биографические данные трудовая деятельностьФИО, номер телефона, должность, домашний адрес | Осуществление методического руководства претензионной работой, анализ, предъявление и рассмотрение претензий и исков, судебная практика, договорная работаОсуществление правовой работы с учетом целей, задач и направлений, составление годовых и ежеквартальных отчетов по направлениям деятельности, обеспечение контроля за выполнением заданий, нормативно-правовых актов | Конституция РФ, кодексы РФ, Устав Бирофельдского сельского поселения, ФЗ от 06.10.2003 N 131-ФЗ «Об общих принципах организации местного самоуправления в РФ», Устав Бирофельдского сельского поселения, законодательство РФ по направлениям работыЗаконодательство РФ, в том числе нормативные правовые акты области, муниципального района, Бирофельдского сельского поселения | 5 летДо минования надобности |
| 5. | Инспектор ВУС | Смешанный | Паспортные данные, номер телефона, домашний адрес, дата рождения, семейное положение, социальное положение, образование, профессия, место работы или учебы, анкетные и биографические данные, сведения о рождении детей, пол, гражданство, сведения о регистрации по месту жительства и временной регистрации по месту пребывания, специальность, сведения о здоровье, воинские билеты | Сведения о воинском учете, сведения о призыве на военную службу, ведение отчетности | ФЗ от 28.03.1998 N 53-ФЗ «О воинской обязанности и воинской службе», | 75 лет |
| 6. | Специалист 1 разряда, землеустроитель | Смешанный | ФИО, номер телефона, домашний адрес, имущественное положение, выписки из Единого государственного реестра недвижимостиФИО, номер телефона, домашний адрес | Сделки с земельными участками, принадлежащими на праве собственности муниципальному образованию, третьим лицам, проведение торгов по землеОказание консультативной помощи по защите прав потребителей | Земельный кодекс РФ, ФЗ от 06.10.2003 N 131-ФЗ «Об общих принципах организации местного самоуправления в РФ», ФЗ от 13.07.2015 N 218-ФЗ «О государственной регистрации недвижимости», Устав Бирофельдского сельского поселенияЗакон РФ от 07.02.1992 N 200-1 «О защите прав потребителей» | 49 лет,5 летДо минования надобности |

ПРИЛОЖЕНИЕ № 6

к постановлению администрации

Бирофельдского сельского поселения

от 24.06.2019 № 67

**ПЕРЕЧЕНЬ**

**должностей муниципальных служащих администрации**

**Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным**

1. Доступ к персональным данным (далее по тексту настоящего Перечня – ПДн) служащих администрации Бирофельдского сельского поселения Биробиджанского муниципального района Еврейской автономной области (далее по тексту настоящего Перечня – Администрация) имеют:

- глава Администрации;

- заместитель главы Администрации;

- ведущий специалист-эксперт 2 разряда, главный бухгалтер Администрации в сфере исполнения возложенных должностных обязанностей;

- ведущий специалист-эксперт 2 разряда Администрации в сфере исполнения возложенных должностных обязанностей;

- инспектор военно-учетного стола Администрации в сфере исполнения возложенных должностных обязанностей.

2. Доступ к ПДн третьих лиц, обрабатываемых в Администрации, имеют:

- глава Администрации;

- заместитель главы Администрации;

- ведущий специалист-эксперт 2 разряда, главный бухгалтер Администрации;

- ведущий специалист-эксперт 2 разряда Администрации;

- специалист-эксперт, юрист;

- специалист 1 разряда, землеустроитель Администрации;

- инспектор военно-учетного стола Администрации.

ПРИЛОЖЕНИЕ № 7

к постановлению администрации

Бирофельдского сельского поселения

от 24.06.2019 № 67

**ПОЛОЖЕНИЕ**

**по обработке персональных данных без использования средств**

**автоматизации в администрации Бирофельдского сельского
поселения Биробиджанского муниципального района**

**Еврейской автономной области**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Трудовым Кодексом Российской Федерации, Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 02.03.2007 № 25-ФЗ «О муниципальнойслужбе в Российской Федерации», Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и определяет порядок обработки персональных данных (далее по тексту настоящего Положения – ПДн) служащих администрации [Бирофельдского](http://npa.eao.ru/law?doc&nd=517509855&nh=1&c=15.4.2016+N+344+344+%CF%CE%D1%D2%C0%CD%CE%C2%CB%C5%CD%C8%C5+%C1%C8%D0%CE%C1%C8%C4%C6%C0%CD%D1%CA%CE%C3%CE+%D0%C0%C9%CE%CD%C0+%CC%D3%CD%C8%D6%C8%CF%C0%CB%DC%CD%CE%C3%CE&spack=111barod%3Dx%5C122;y%5C18%26intelsearch%3D%EF%EE%F1%F2%E0%ED%EE%E2%EB%E5%ED%E8%E5+%E1%E8%F0%EE%E1%E8%E4%E6%E0%ED%F1%EA%EE%E3%EE+%EC%F3%ED%E8%F6%E8%EF%E0%EB%FC%ED%EE%E3%EE+%F0%E0%E9%EE%ED%E0+%EE%F2+15.04.2016+%B9+344%26listid%3D010000000100%26listpos%3D1%26lsz%3D6%26razdel%3D517500001%26w%3D5%26whereselect%3D5%26#C679) сельского поселения Биробиджанского муниципального района Еврейской автономной области (далее по тексту настоящего Положения – Администрация) и третьих лиц, в связи с представлением, получением, хранением, комбинированием, передачей или любым другим использованием ПДн, а также порядок защиты персональных данных служащих администрации и третьих лиц при их обработке без средств автоматизации.

1.2. Положение является внутренним нормативным документом, регламентирующим деятельность администрации в сфере защиты ПДн, обрабатываемых без использования средств автоматизации. Положение является обязательным для выполнения всеми служащими администрации.

1.3. Целью защиты ПДн, обрабатываемых без использования средств автоматизации, является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн.

1.4. Обработка ПДн считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПДн, как использование, уточнение, распространение, уничтожение в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека.

1.5. В Администрации приняты следующие возможные методы неавтоматизированной обработки персональных данных:

- обработка персональных данных исключительно на бумажных носителях информации;

- обработка персональных данных с использованием средств вычислительной техники с выводом документа на бумажный носитель.

1.6. Защита ПДн при их неавтоматизированной обработке достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее передачи и хранения.

1.7. Действие Положения не распространяется на устанавливаемый государственными органами режим защиты сведений, составляющих государственную тайну и иные виды тайн, защита которых определена отдельными законодательными и нормативно-методическими документами Российской Федерации.

2. ТРЕБОВАНИЯ К НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И МЕРОПРИЯТИЯ ПО ИХ ВЫПОЛНЕНИЮ

2.1. Служащие Администрации, осуществляющие обработку ПДн без использования средств автоматизации, в обязательном порядке должны быть ознакомлены с положениями настоящего положения.

2.2. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее - материальные носители), в специальных разделах или на полях форм (бланков).

2.3. Обработка, а также хранение документов, содержащих ПДн, осуществляется в специально отведенных местах. Служащие Администрации осуществляют обработку ПДн в соответствии со своими должностными обязанностями.

2.4. Служащие Администрации, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о целях обработки ПДн.

2.5. Документы, разрабатываемые в процессе неавтоматизированной обработки ПДн с использованием типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны печататься на фирменном бланке Администрации либо содержать необходимые реквизиты. При этом цель, сроки обработки ПДн должны содержаться в преамбуле документа.

2.6. При неавтоматизированной обработке ПДн осуществляется раздельное хранение документов, содержащих ПДн субъекта, обрабатываемые в разных целях.

2.7. 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 ПДн, принимаются следующие мероприятия по обеспечению безопасности ПДн:

2.7.1 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;

2.7.1 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;

2.7.3 уничтожение 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).

2.8. При необходимости изменения ПДн, зафиксированных на бумажном носителе, осуществляется исправление ПДн с использованием пишущей ручки или изготовлением нового документа.

2.9. Хранение ПДн на бумажных носителях должно осуществляться в установленных в помещении надежных хранилищах (металлических шкафах, пеналах, сейфах). При этом не допускается осуществлять совместное хранение ПДн и документов, не относящихся к ним.

3. ПРАВИЛА ПРИЕМА И РЕГИСТРАЦИИ ВХОДЯЩЕЙ КОРРЕСПОНДЕНЦИИ СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

3.1. Прием, первичную обработку и регистрацию входящей почтовой корреспонденции, содержащей ПДн, осуществляется служащий Администрации, в чьи должностные обязанности входит прием входящей корреспонденции, или служащий Администрации, уполномоченный на обработку и хранение соответствующих ПДн, при этом проверяется правильность ее доставки, целостность вложений и наличие приложений.

3.2. На полученных документах, в правом нижнем углу лицевой стороны документа проставляется регистрационный штамп Администрации, с указанием даты поступления документа и его регистрационного номера.

Состав документа фиксируется в «Журнале регистрации входящих документов».

3.3. Поступившие в Администрацию машинные носители информации, содержащие ПДн (в том числе сторонних организаций) учитываются как приложение к основному входящему документу в «Журнале регистрации входящих документов».

3.4. После регистрации входящие документы передаются на рассмотрение главе Администрации.

3.5. Рассмотренный документ в соответствии с наложенной резолюцией передается под роспись исполнителю для использования в работе.

3.6. В случае, когда документ должен быть передан двум и более исполнителям, изготавливается необходимое количество копий документов, которые передаются под роспись исполнителям. На подлиннике документа указывается дата, количество изготовленных копий, подпись, фамилия и инициалы лица их изготовивших.

3.7. Корреспонденция, содержащая ПДн, хранится у служащих Администрации, уполномоченных на обработку и хранение соответствующих ПДн, в сформированных номенклатурных делах в соответствии с пунктом 2.9 настоящего Положения.

3.8. При отсутствии необходимости хранения копий документов, содержащих ПДн, копии уничтожаются, при этом на оригинале документа проставляется соответствующая отметка.

3.9. При обнаружении во входящей корреспонденции содержащей ПДн повреждений или отсутствия указанных в корреспонденции вложенных документов, составляющих ПДн, составляется акт в двух экземплярах, один из которых направляется отправителю, второй – подшивается в дело.

3.10. При поступлении в Администрацию корреспонденции в электронном виде, содержащей сведения, отнесенные к, служащий, принявший корреспонденцию, обязан перенести документ на бумажный носитель и удалить входящее электронное письмо. Учет, первичная обработка и регистрация данного документа осуществляется в установленном настоящим разделом порядке.

3.11. Изготовление не учтенных (не зарегистрированных) копий документов, содержащих ПДн, запрещается.

4. ПРАВИЛА ПОДГОТОВКИ И ОТПРАВКИ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

4.1. Исходящие документы готовятся на фирменных бланках Администрации в соответствии с требованиями по делопроизводству, принятыми в Администрации.

4.2. Подписанный главой Администрации документ регистрируется служащим Администрации, в чьи должностные обязанности входит отправка исходящей корреспонденции или служащим Администрации, уполномоченным на обработку и хранение соответствующих ПДн, в «Журнале регистрации исходящих документов» и направляется адресату.

4.3. При получении служащим Администрации, в чьи должностные обязанности входит отправка исходящей корреспонденции, от исполнителей документов, предназначенных к отправке, он проверяет наличие всех экземпляров и листов документа, приложений к нему, правильность оформления и адресования; выясняет способ отправки документа (пакет может быть доставлен адресату ценным, заказным письмом либо лично исполнителем при наличии такой возможности).

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящее Положение доводится до служащих Администрации, в должностные обязанности которых входит обработка ПДн, под роспись при приеме на работу.

ПРИЛОЖЕНИЕ № 8

к постановлению администрации

Бирофельдского сельского поселения

от 24.06.2019 № 67

**ПОЛОЖЕНИЕ**

**об организации и обеспечении защиты персональных данных**

**при их обработке в информационных системах персональных**

**данных администрации Бирофельдского сельского поселения
Биробиджанского муниципального района**

**Еврейской автономной области**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных, на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПД», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей гостайну, содержащейся в государственных информационных системах», распорядительными и методическими документами ФСТЭК России и определяет порядок обработки персональных данных (далее по тексту настоящего Положения – ПДн) служащих администрации Бирофельдского сельского поселения Биробиджанского муниципального района(далее по тексту настоящего Положения – Администрация) и третьих лиц, в связи с представлением, получением, хранением, комбинированием, передачей или любым другим использованием ПДн, а также порядок защиты ПДн служащих Администрации и третьих лиц, в том числе при их обработке в информационных системах персональных данных (далее по тексту настоящего Положения – ИСПДн).

1.2. Положение является внутренним нормативным документом, регламентирующим деятельность Администрации в сфере защиты ПДн, обрабатываемых в ИСПДн Администрации. Положение является обязательным для выполнения всеми служащими Администрации.

1.3. Целью защиты ПДн является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн.

1.4. Защита ПДн в Администрации достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

1.5. Объектами защиты в Администрации являются ПДн, средства и системы информатизации (СВТ, АС различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети и системы и другие технические средства обработки информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки ПДн.

1.6. Действие Положения не распространяется на устанавливаемый государственными органами режим защиты сведений, составляющих государственную тайну и иные виды тайн, защита которых определена отдельными законодательными и нормативно-методическими документами Российской Федерации.

2. ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПОДЛЕЖАЩИЕ ЗАЩИТЕ

2.1. Информационные ресурсы, содержащие ПДн, определяются Перечнем информационных систем персональных данных в Администрации, утверждаемым настоящим Постановлением.

2.2. Информационные ресурсы, содержащие ПДн, расположены в ИСПДн Администрации, состоящих из автоматизированных рабочих мест (АРМ) пользователей на базе ПЭВМ, серверов и отчуждаемых носителей информации.

2.3. В целях информационного обеспечения Администрации могут создаваться общедоступные источники персональных данных (в том числе справочники, телефонные книги, адресные книги). Режим конфиденциальности для общедоступных источников персональных данных не устанавливается.

3. ОРГАНИЗАЦИОННАЯ СИСТЕМА

ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДН

3.1. Служащие Администрации несут персональную ответственность за обеспечение безопасности ПДн по направлениям своей работы, организуют выполнение установленных настоящим Положением требований по защите ПДн, принимают меры по максимальному ограничению возможности ознакомления с информацией служащих, которым по роду выполняемых ими должностных обязанностей она не требуется.

3.2. Общее руководство организацией защиты ПДн, координацию работ по защите ПДн, обеспечение безопасности ПДн при обработке в ИСПДн осуществляет глава Администрации.

3.3. Заместитель главы Администрации осуществляет подготовку предложений по совершенствованию и реализации мероприятий по обеспечению безопасности ПДн в ИСПДн Администрации, является администратором ИСПДн, ведет контроль деятельности служащих Администрации по выполнению ими установленных требований обеспечения безопасности ПДн в ИСПДн Администрации

3.4. Служащие Администрации при осуществлении своих функциональных обязанностей с использованием ИСПДн Администрации непосредственно реализуют требования безопасности информации, принятые для ИСПДн Администрации, исполняют установленные режимы защиты ПДн, обеспечивают строгое исполнение предписанных правил безопасности информации.

3.5. Глава Администрации:

- осуществляет взаимодействие с подразделениями, должностными лицами, органами государственной власти и местного самоуправления и юридическими лицами по вопросам предоставления сведений, содержащих персональные данные;

- организует порядок предоставления полномочий и допусков служащим подразделений к ПДн ИСПДн Администрации;

- проводит обучение персонала правилам работы с ПДн;

- организует учет и хранение отчуждаемых носителей ПДн;

- осуществляет поддержкц в актуальном состоянии эксплуатационной документации ИСПДн Администрации;

- участвует в работе экспертных комиссий при рассмотрении вопросов обеспечения информационной безопасности.

3.6. Заместитель (администратор безопасности):

- контролирует деятельность служащих Администрации по вопросам обеспечения безопасности информации;

- требует прекращения обработки защищаемой информации в Администрации при выявлении существенных нарушений в технологии обработки информации, при выходе из строя средств защиты информации и в других случаях выявления грубых нарушений требований по обеспечению информационной безопасности Администрации;

 вносит на рассмотрение главе Администрации предложения по привлечению к материальной и дисциплинарной ответственности виновных в утечке информации, составляющей конфиденциальную информацию;

- участвует в работе экспертных комиссий при рассмотрении вопросов обеспечения информационной безопасности;

- привлекает в установленном порядке служащих Администрации и сторонние организации для проведения исследований, разработки решений, проведения мероприятий и разработки нормативно-методических документов по вопросам обеспечения безопасности информации;

- определяет необходимость и участвует в разработке нормативных документов, касающихся вопросов обеспечения информационной безопасности, включая документы, регламентирующие деятельность служащих Администрации;

- участвует в разработке технических заданий и испытаниях программных, технических средств обеспечения безопасности информации в ИСПДн Администрации;

- получает информацию от служащих Администрации по вопросам используемых технологий обработки информации и эксплуатации ИСПДн.

3.7. Служащие Администрации осуществляющих обработку ПДн в пределах своих должностных обязанностей обеспечивают соблюдение технических требований по порядку и правилам при работе с ПДн.

3.8. Пользователи ИСПДн не имеют права использовать в неслужебных целях информационные ресурсы ИСПДн, обязаны хранить охраняемые законом ПДн и не разглашать ПДн, ставшие им известными в связи с исполнением должностных обязанностей.

3.9. Служащие Администрации, вовлеченные в защиту ПДн в Администрации, в пределах своих должностных обязанностей, обеспечивают соблюдение пользователями порядка и правил при работе с ПДн.

3.10. Методическое руководство деятельностью по организации и обеспечению безопасности информации осуществляется департаментом по защите информации аппарата губернатора и правительства ЕАО.

3.11. Классификация ИСПДн проводится в соответствии с постановлением правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3.12. Устанавливается четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий - четвертый, самый высокий - первый.

3.13. Классификация ИСПДн проводится на этапе создания ИСПДн или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн.

3.14. Класс защищенности определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

3.15. Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба может быть:

- высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

- средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

- низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

3.16. Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информации имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба. Информация имеет минимальный уровень значимости (УЗ 4), если обладателем информации (заказчиком) и (или) оператором степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) не может быть определена, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.

3.17. При обработке в информационной системе двух и более видов информации уровень значимости определяется отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

3.18. Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях. Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях. Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципальногообразования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

3.19. Класс защищенности информационной системы определяется в соответствии с таблицей:

|  |  |
| --- | --- |
| Уровень значимости информации | Масштаб информационной системы |
|  | Федеральный | Региональный | Объектовый |
| УЗ 1 | К1  | К1  | К1  |
| УЗ 2 | К1  | К2  | К2  |
| УЗ 3 | К2  | К3  | К3  |
| УЗ 4 | К3  | К3  | К4  |

3.20. По результатам классификации ИСПДн оформляется акт классификации, утверждаемый главой Администрации. Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации

3.21. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

3.22. При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

3.23. Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

3.24. Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 № 1085.

4. ТРЕБОВАНИЯ ПО ЗАЩИТЕ ПДн ПРИ ИХ ОБРАБОТКЕ В ИСПДн

4.1. Администрация должна соблюдать режим конфиденциальности при обработке ПДн, за исключением случаев, когда обеспечение конфиденциальности ПДн не требуется.

4.2. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защиту машинных носителей информации;

- регистрацию событий безопасности;

- антивирусную защиту;

- обнаружение (предотвращение) вторжений;

- контроль (анализ) защищенности информации;

- целостность информационной системы и информации;

 доступность информации;

- защиту среды виртуализации;

- защиту технических средств;

- защиту информационной системы, ее средств, систем связи и передачи данных.

4.3. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

4.4. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

4.5. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

4.6. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

4.7. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

4.8. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

4.9. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

4.10. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

4.11. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

4.12. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

4.13. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

4.14. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

4.15. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

4.16. Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

- определение базового набора мер защиты информации для установленного класса защищенности информационной системы в соответствии с базовыми наборами мер защиты информации;

- адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

- уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

- дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

4.17. Для выбора мер защиты информации для соответствующего класса защищенности информационной системы применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 № 1085.

5. ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО ЗАЩИТЕ

ПДн ПРИ ИХ ОБРАБОТКЕ В ИСПДн

Требования к оборудованию помещений

и рабочих мест пользователей ИСПДн

5.1. Все технические средства ИСПДн Администрации должны находиться в пределах контролируемых зон, исключающих неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

5.2. При размещении АРМ пользователей ИСПДн на нижних этажах зданий их рекомендуется располагать во внутренних помещениях, максимально удаленных от границ контролируемых зон.

5.3. Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обслуживанием оборудования.

5.4. Размещение устройств отображения и печати информации, используемых в составе АРМ пользователей ИСПДн Администрации, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами. Кроме того, должны приниматься дополнительные меры, исключающие подобный просмотр (шторы, жалюзи на окнах, непрозрачные экраны).

5.5. Неиспользуемые в процессе обработки ПДн устройства ввода/вывода АРМ пользователей ИСПДн (СОМ, LPT, НГМД, CD, USB) необходимо отключить либо опечатать (опломбировать) в случае, если данные функции нельзя реализовать с помощью СЗИ на программном уровне.

5.6. Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельном опломбированном помещении с прочной запираемой дверью. Перечень лиц, имеющих право доступа в указанные помещения, утверждается отдельным списком. Ключи от дверей данных помещений должны быть только у лиц, имеющих право доступа в них. Допускается устанавливать коммуникационное оборудование в отдельных запираемых и опечатываемых металлических шкафах, размещаемых в охраняемых помещениях.

Требования к процедуре получения доступа в ИСПДн

5.7. Предоставление доступа к ПДн, обрабатываемым в ИСПДн осуществляется на основании распоряжения Администрации. Администратором безопасности информации должна проводиться периодическая проверка прав пользователей ИСПДн следующим образом:

- проверка прав пользователей должна проводиться на периодической основе или после каждого изменения в системе. При этом проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться с меньшей периодичностью;

- должна быть предусмотрена регулярная проверка адекватности назначенных привилегий с целью исключения получения кем-либо из пользователей излишних прав.

6. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ

ПДн ПРИ ИХ ОБРАБОТКЕ В ИСПДн

6.1. Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности. В этом случае в информационных системах 1 и 2 класса защищенности применяются:

- средства вычислительной техники не ниже 5 класса;

- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

- межсетевые экраны не ниже 3 класса, в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена, и не ниже 4 класса, в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

6.2. В информационных системах 3 класса защищенности применяются:

- средства вычислительной техники не ниже 5 класса;

- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 5 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

- межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

6.3. В информационных системах 4 класса защищенности применяются:

- средства вычислительной техники не ниже 5 класса;

- системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса; межсетевые экраны не ниже 4 класса.

6.4. В информационных системах 1 и 2 классов защищенности применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Требования к резервированию

6.5. Для обеспечения возможности быстрого восстановления ПДн и средств их обработки в случае повреждения (утраты) рабочей копии в ИСПДн Администрации должны выполняться следующие требования:

- резервные копии информационных ресурсов, содержащих ПДн, и инструкции по их восстановлению должны храниться в специально выделенном месте, территориально отдаленном от места обработки самой информации;

- для обеспечения сохранности резервных копий должен быть применён комплекс организационных и технических мер защиты;

- носители, на которые осуществляется резервное копирование, должны регулярно проверяться на работоспособность;

- должны быть предусмотрены регулярные проверки процедур восстановления.

Обеспечение безопасности ПДн при передаче

6.6. При передаче ПДн субъекта должны соблюдаться следующие требования:

- не сообщать ПДн субъекта третьей стороне без его письменного согласия, за исключением случаев, предусмотренных действующим законодательством Российской Федерации;

- предупреждать лиц, получивших ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено; лица, получившие ПДн, обязаны соблюдать режим конфиденциальности;

- разрешать доступ к ПДн только специально уполномоченным на это служащим Администрации, при этом указанные служащие должны иметь право получать только те ПДн, которые необходимы для выполнения ими должностных обязанностей;

- передавать ПДн субъектов их представителям в порядке, установленном действующим законодательством Российской Федерации, и ограничивать эту информацию только теми ПДн, которые необходимы для выполнения указанными представителями их должностных функций;

- передача ПДн третьим лицам может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.7. Трансграничная передача ПДн на территорию иностранного государства допускается только с согласия субъекта или в случаях, определенных законодательством Российской Федерации.

Обеспечение безопасности при хранении ПДн

6.8. Круг лиц, допущенных к работе с документами, содержащими ПДн служащих Администрации, утверждается [настоящим](http://npa.eao.ru/law?doc&nd=517509855&nh=1&c=15.4.2016+N+344+344+%CF%CE%D1%D2%C0%CD%CE%C2%CB%C5%CD%C8%C5+%C1%C8%D0%CE%C1%C8%C4%C6%C0%CD%D1%CA%CE%C3%CE+%D0%C0%C9%CE%CD%C0+%CC%D3%CD%C8%D6%C8%CF%C0%CB%DC%CD%CE%C3%CE&spack=111barod%3Dx%5C122;y%5C18%26intelsearch%3D%EF%EE%F1%F2%E0%ED%EE%E2%EB%E5%ED%E8%E5+%E1%E8%F0%EE%E1%E8%E4%E6%E0%ED%F1%EA%EE%E3%EE+%EC%F3%ED%E8%F6%E8%EF%E0%EB%FC%ED%EE%E3%EE+%F0%E0%E9%EE%ED%E0+%EE%F2+15.04.2016+%B9+344%26listid%3D010000000100%26listpos%3D1%26lsz%3D6%26razdel%3D517500001%26w%3D5%26whereselect%3D5%26#C877) Постановлением.

6.9. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

6.10. ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, поэтому для каждой системы ПДн в обязательном порядке устанавливается срок хранения ПДн и осуществляется регулярное уничтожение, а также обезличивание ПДн при наличии такой возможности.

7. ПЛАНИРОВАНИЕ И КОНТРОЛЬ

ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДн

7.1. Планирование работ по защите информации проводится в целях выявления и устранения недостатков в системе защиты информации, разработки предложений по ее совершенствованию.

7.2. Планирование осуществляется заместителем главы Администрации по приведению информационных систем, обрабатывающих информацию ограниченного доступа, в соответствии с требованиями нормативных правовых документов Российской Федерации.

7.3. План мероприятий по защите информации ПДн разрабатывается ежегодно и включает следующие основные мероприятия:

- разработка (модернизация) систем защиты информации;

- контроль защищенности информации в ИСПДн;

- контроль организации защиты информации;

- устранение недостатков по результатам ранее проведенных проверок и контрольных мероприятий.

План также включает в себя перечень ответственных служащих Администрации за проведение работ, сроки выполнения мероприятий и состав отчетных документов, оформляемых по результатам их реализации.

7.4. С целью изучения, анализа и оценки фактического состояния безопасности ПДн, выявления недостатков и нарушений режима конфиденциальности в работе с ПДн, предпосылок к возникновению этих нарушений, установления их причин и выработки необходимых предложений для их устранения, а также для своевременного выявления и предотвращения утечки информации, содержащей ПДн, в ИСПДн должен проводиться периодический (не реже 1 раза в год) контроль состояния защиты ПДн, который заключается в оценке:

- соблюдения требований руководящих и нормативно-методических документов по защите ПДн;

- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

- знаний и выполнения персоналом своих функциональных обязанностей в части защиты ПДн.

7.5. Контроль осуществляется путем проведения плановых и внеплановых проверок. Плановые проверки пользователей ИСПДн, технических средств и систем проводятся комиссиями, назначаемыми распоряжением Администрации. Внеплановые проверки проводятся по усмотрению главы и заместителя главы Администрации.

7.6. Результаты проверок оформляются актом в произвольной форме. В акте указываются рекомендации по закрытию возможных каналов утечки информации.

7.7. Проверка технических средств и систем проводится не реже 1 раза в год, а также дополнительно при изменении состава технических средств и систем, условий обработки информации, содержащей ПДн.

7.8. Все работы по контролю должны проводиться при строгом соблюдении мер безопасности, исключающих разглашение сведений о проводимых работах, местах размещения технических средств и систем, используемых СЗИ и возможных каналах утечки информации, содержащей ПДн.

7.9. В случаях обнаружения нарушений при обработке ПДн в ИСПДн Администрации ответственный за обработку ПДн обязан:

- немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения, и принять меры к их устранению;

- организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

Возобновление работ разрешается только после устранения нарушений и проверки достаточности и эффективности принятых мер, соответствия их требованиям нормативных документов по защите ПДн.

8. ОТВЕТСТВЕННОСТЬ

Ответственность за обеспечение безопасности ПДн

8.1. Лица, виновные в нарушении нормативных правовых актов и внутренних актов Администрации, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8.2. Администрация, как владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения, реализующее полномочия владения, пользования, распоряжения конфиденциальной информацией в пределах, установленных законом, несет ответственность за использование персональных данных в целях причинения имущественного и морального вреда субъектов ПДн, затруднения реализации их прав и свобод. Ограничение прав субъектов ПДн на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено.

Ответственность за неразглашение информации, содержащей ПДн

8.3. Под разглашением информации, содержащей ПДн, понимается действие или бездействие должностных лиц, в результате которых информация, содержащая ПДн, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

8.4. Утрата документов, содержащих ПДн, - это выход (в том числе и временный) документов из владения ответственного за их сохранность служащего, которому они были доверены, вследствие чего эти документы, а равно содержащиеся в них сведения, стали, либо могли стать достоянием посторонних лиц.

8.5. Разглашение информации, содержащей ПДн, или утрата документов, содержащих таковую, относится к числу грубых нарушений служебного контракта.

8.6. За разглашение информации, содержащей ПДн, утрату документов, содержащих такие сведения, а также за иные нарушения режима защиты ПДн виновные лица несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

Ответственность за нарушение требований настоящего Положения

8.7. Служащие Администрации несут персональную ответственность за соблюдение настоящего Положения.

8.8. Служащие Администрации несут ответственность по действующему законодательству Российской Федерации за разглашение сведений, составляющих ПДн, ставших известными им случайно или по роду работы.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящее Положение доводится до служащих Администрации, в должностные обязанности которых входит обработка ПДн, под роспись при приеме на работу.