

Муниципальное образование

«ЗАНЕВСКОЕ ГОРОДСКОЕ ПОСЕЛЕНИЕ»

Всеволожского муниципального района Ленинградской области

**АДМИНИСТРАЦИЯ**

**ПОСТАНОВЛЕНИЕ**

20.06.2016 г. № 325

дер. Заневка

Об обеспечении безопасности персональных данных в администрации МО «Заневское городское поселение»

В соответствии с Федеральным законом 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», администрация муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области

**ПОСТАНОВЛЯЕТ:**

1. Утвердить Положение об обеспечении безопасности персональных данных в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области согласно приложению № 1.

2. Утвердить Положение о ролях и ответственности за обработку и защиту персональных данных в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области согласно приложению № 2.

3. Утвердить Порядок реагирования на инциденты информационной безопасности в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области согласно приложению № 3.

4. Утвердить Порядок учета, хранения и уничтожения носителей персональных данных в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области согласно приложению № 4.

5. Настоящее постановление подлежит опубликованию в официальных средствах массовой информации и размещению на официальном сайте администрации.

6. Настоящее постановление вступает в силу со дня его опубликования в официальных средствах массовой информации.

7. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации по общим и социальным вопросам Карвелиса М.А.

Глава администрации А.В.Гердий

Приложение № 1

к постановлению администрации

от «20» 06. 20 16 г.№ 325

Положение

об обеспечении безопасности персональных данных в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области

1. Используемые сокращения

В настоящем Положении использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

| № п/п | Сокращение | Описание |
| --- | --- | --- |
| 1. | ИСПДн | Информационная система персональных данных |
| 2. | НСД | Несанкционированный доступ |
| 3. | ПДн | Персональные данные |
| 4. | СКЗИ | Средство криптографической защиты информации |
| 5. | СЗПДн | Система защиты персональных данных |

1. Область применения

2.1. Настоящее Положение об обеспечении безопасности персональных данных в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области (далее – Положение) предназначено для применения при организации и проведении работ по обеспечению безопасности персональных данных в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области (далее – администрация).

2.2. Требования настоящего Положения распространяются на работников администрации, принимающих участие в обеспечении безопасности персональных данных.

1. Общие положения

3.1. Настоящее Положение определяет содержание и порядок осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПДн) администрации, представляющей собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных как с использованием средств автоматизации, так и без использования таких средств.

Безопасность персональных данных при их обработке в ИСПДн достигается путем снижения вероятности осуществления НСД к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

3.2. При обработке персональных данных в ИСПДн администрации должно быть обеспечено:

1) проведение мероприятий, направленных на предотвращение НСД к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

2) своевременное обнаружение фактов НСД к персональным данным;

3) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

4) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;

5) непрерывный контроль и анализ уровня защищенности персональных данных.

3.3. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные мероприятия и средства защиты информации (в том числе криптографические средства, средства предотвращения НСД, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПД информационные технологии.

Обеспечение безопасности персональных данных в администрации осуществляется на основе следующих принципов:

1) соответствие мер и средств защиты актуальным угрозам безопасности – построение и модернизация СЗПДн в администрации производится на основе анализа угроз безопасности персональных данных с учетом специфических особенностей ИСПДн;

2) соответствие мер и средств защиты требованиям нормативных документов Российской Федерации – в администрации используются меры и средства обеспечения безопасности персональных данных в строгом соответствии с действующими нормативным и правовыми актами Российской Федерации в области обработки и защиты персональных данных;

3) комплексность – с целью обеспечения безопасности персональных данных в администрации используется совокупность организационных мер и технических средств защиты;

4) патентная чистота – средства защиты информации, входящие в состав СЗПДн, отвечают требованиям по обеспечению патентной чистоты согласно действующим нормативным документам Российской Федерации. Используемое общесистемное, специальное и прикладное программное обеспечение имеет соответствующие лицензии производителей.

5) удобство пользователей – при построении и модернизации СЗПДн учитываются и по возможности сводятся к минимуму возможные трудности пользователей в работе со средствами защиты и с основными процедурами обеспечения безопасности персональных данных;

6) постоянное совершенствование – осуществляется регулярный внутренний контроль выполнения требований по обработке и обеспечению безопасности персональных данных, эффективности применяемых организационных мер и технических средств защиты и уровня защищенности персональных данных, а также регулярно пересматриваются состав угроз и уровень защищенности ПДн, на основании чего принимаются меры по устранению выявленных недостатков и модернизации/совершенствованию СЗПДн.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в ИСПДн оценивается при проведении государственного контроля и надзора.

3.4. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн администрации включают в себя:

1) определение уровня защищенности обрабатываемых ПДн, в том числе отслеживание изменений состояния ИСПДн, которые могут повлиять на классификационные признаки ИСПДн (уровень защищенности ПДн);

2) определение угроз безопасности персональных данных при их обработке в ИСПДн;

3) разработка на основании определенных угроз и поддержание в актуальном состоянии частной модели безопасности угроз безопасности персональных данных при обработке их в ИСПДн;

4) разработку на основе частной модели угроз системы защиты персональных данных (СЗПДн), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для установленного уровня защищенности ПДн;

5) установку и ввод в эксплуатацию СЗИ, входящих в состав СЗПДн, в соответствии с проектными решениями по созданию СЗПДн, эксплуатационной и технической документацией к данным СЗИ;

6) обучение лиц, использующих СЗИ, входящие в состав СЗПДн, правилам работы с ними;

7)учет применяемых СЗИ, входящих в состав СЗПДн, эксплуатационной и технической документации к ним;

8) учет носителей персональных данных;

9) учет лиц, допущенных к работе с персональными данными в ИСПДн;

10) контроль соблюдения условий использования СЗИ, входящих в состав СЗПДн, предусмотренных эксплуатационной и технической документацией к ним;

11) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования СЗИ, входящих в состав СЗПДн, которые могут привести к нарушению заданных характеристик безопасности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

12) описание состава и режима функционирования компонентов СЗПДн (описание СЗПДн).

3.5. Размещение компонентов ИСПДн, охрана помещений, в которых ведется работа с персональных данных, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и СЗИ, входящих в состав СЗПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Настоящее Положение должно быть доведено до всех работников администрации, участвующих в обеспечении безопасности персональных данных, под роспись.

4. Стадии создания СЗПДН

В администрации обеспечение безопасности персональных данных осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках следующих стадий создания и совершенствования СЗПДн:

1) предпроектная стадия;

2) стадия проектирования;

3) стадия приемки и ввода в действие;

4) модернизация СЗПДн.

СЗПДн включает организационные меры, технические средства защиты информации,   
а также используемые в ИСПДн информационные технологии, реализующие функции защиты информации.

Выполнение всех вышеуказанных стадий должно проходить по согласованию   
с должностным лицом, ответственным за организацию работ по обработке персональных данных.

Выполнение всех вышеуказанных стадий должно проходить под контролем должностного лица, ответственным за проведение работ по защите персональных данных.

## 

## 5. Описание требований к предпроектной стадии создания СЗПДн

5.1. Целью предпроектной стадии создания СЗПДн является:

1) определение категории субъектов персональных данных, чьи данные обрабатываются в администрации, состава и объема обрабатываемых персональных данных, а также цели и правовое основание обработки этих данных;

2) определение должностных лиц, участвующих в обработке персональных данных;

3) определение угроз безопасности персональных данных применительно к конкретным условиям функционирования ИСПДн;

4) определение уровня защищенности ПДн.

Для достижения указанных целей проводится анализ информационных систем администрации, содержащих персональные данные, и определяются все внутренние и внешние процессы обработки персональных данных, осуществляемые как с использованием средств автоматизации, так и без использования таковых.

По результатам предпроектной стадии определяется степень выполнения требований нормативно-правовых документов в области защиты персональных данных, а также разрабатывается план необходимых дальнейших организационных и технических мероприятий по реализации данных требований.

Должностное лицо, ответственное за проведение работ по защите персональных данных, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели предпроектной стадии.

5.21. Определение обрабатываемых персональных данных

В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в администрации определяются состав, цели, правовое основание обработки персональных данных и сроки хранения обрабатываемых персональных данных.

На основании полученных данных формируется документ «Перечень персональных данных, обрабатываемых в администрации».

5.3. Определение перечня должностных лиц, допущенных к работе с персональными данными

В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в администрации определяется перечень лиц, которым необходим доступ к персональных данных для выполнения трудовых обязанностей, а также перечень лиц, которые в рамках выполнения своих трудовых обязанностей имеют право доступа к ресурсам, содержащим персональные данные, без права ознакомления с персональными данными.

На основании полученных данных формируется перечень должностных лиц, допущенных в помещения и к работе со средствами вычислительной техники из состава ИСПДн администрации, который утверждается соответствующим распоряжением администрации.

5.4. Определение конфигурации и топологии ИСПДн

В ходе обследования информационных систем администрации определяются все базы данных (хранилища) и отчуждаемые носители информации и содержащиеся в них персональных данных. Кроме того, определяются конфигурация и топология ИСПДн в целом и ее отдельных компонентов, а именно перечень серверного оборудования, автоматизированных рабочих мест, общесистемных и прикладных программных средств, задействованных при обработке персональных данных, перечень применяемых средств защиты информации, а также сетевая инфраструктура и перечень сетевого оборудования.

На основании полученных данных формируются документы «Описания технологии обработки информации в администрации».

5.5. Определение угроз безопасности персональных данных

С целью определения необходимых мер и средств защиты, соответствующих актуальным угрозам безопасности персональных данных при их обработке в ИСПДн администрации, проводится анализ и оценка вероятности реализации и величины негативных последствий вследствие реализации угроз безопасности персональных данных при их обработке в ИСПДн.

В администрации составляется частная модель угроз безопасности персональных данных, которая разрабатывается на основании:

1) Базовой модели угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 15.02.2008 ФСТЭК России;

2) Методики определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 14.02.2008 ФСТЭК России;

3) Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации., утвержденных ФСБ России 21.02.2008 № 149/54-144.

5.6. Определение уровня защищенности ПДн

Определение уровня защищенности ПДн осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». При определении уровня защищенности ПДн используется модель угроз безопасности ПДн, в которой проведен анализ актуальных угроз безопасности ПДн.

## 6. Стадия проектирования СЗПДн

6.1. Цели проектирования СЗПДн:

1) определить требования по обеспечению безопасности персональных данных;

2) определить структуру и характеристики создаваемой СЗПДн, состав технических средств защиты информации, предполагаемых к использованию в СЗПДн, требования к настройке и эксплуатации этих средств, параметры их взаимодействия, а также план мероприятий по подготовке СЗПДн к вводу в действие;

3) определить требования и регламентировать деятельность работников администрации по организации легитимной обработки персональных данных и обеспечению безопасности персональных данных, обрабатываемых как с использованием средств автоматизации, так и без использования таковых.

Для достижения указанных целей в администрации разрабатывается комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных.

Должностное лицо, ответственное за проведение работ по защите персональных данных в администрации, определяет необходимость проведения мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии проектирования СЗПДн.

6.2. Определение требований по обеспечению безопасности персональных данных

По результатам предпроектной стадии, в зависимости от определенного уровня защищенности ПДн и определенного перечня актуальных угроз безопасности персональных данных, задаются конкретные требования по обеспечению безопасности ПДн при их обработке в ИСПДн администрации, выполнение которых обеспечивает минимизацию вероятности реализации предполагаемых угроз безопасности персональных данных.

6.3. Определение конфигурации СЗПДн

На основании требований, указанных выше, осуществляется проектирование СЗПДн, определяется состав и характеристики средств защиты информации, которые будут входить в состав создаваемой СЗПДн.

В администрации разрабатывается комплект организационно-распорядительной документации на СЗПДн, описывающей требования и процедуры по управлению и обеспечению безопасности персональных данных. За разработку и, при необходимости, пересмотр организационно-распорядительной документации на СЗПДн в администрации отвечает должностное лицо, ответственное за проведение работ по защите персональных данных в администрации.

7. Стадия ввода в действие СЗПДн

7.1. Цели стадии ввода в действие СЗПДн:

1) внедрить технические средства защиты информации;

2) проверить работоспособность средств защиты информации в составе ИСПДн;

3) принять организационные меры по обеспечению безопасности персональных данных;

4) ознакомить работников администрации с требованиями и обучить порядку обработки и обеспечения безопасности персональных данных.

7.2. Для достижения перечисленных целей выполняются следующие мероприятия:

1) осуществляется закупка, установка и настройка средств защиты информации;

2) проводятся опытная эксплуатация и приемо-сдаточные испытания средств защиты информации;

3) утверждается и вводится в действие комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных;

4) проводится обучение работников по направлению обеспечения безопасности персональных данных.

Должностное лицо, ответственное за проведение работ по защите персональных данных в администрации, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии ввода в действие СЗПДн.

7.3. Внедрение средств защиты информации

Согласно требованиям, определенным в документации, осуществляется закупка, установка и настройка программных и технических средств защиты информации с составлением соответствующих актов установки.

Установка и ввод в эксплуатацию средств защиты информации осуществляется строго в соответствии с эксплуатационной и технической документации к ним. Перед установкой средств защиты информации проверяется их готовность к использованию, и составляются заключения о возможности их эксплуатации.

В администрации необходимо применять средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия и имеющие соответствующие сертификаты ФСТЭК и ФСБ России.

7.4. Внедрение организационных мер по обеспечению безопасности персональных данных

В администрации утверждается и вводится в действие комплект организационно-распорядительной документации на СЗПДн.

Все должностные лица, допущенные к обработке персональных данных, и лица, ответственные за обеспечение безопасности персональных данных, в обязательном порядке изучают организационно-распорядительные документы на СЗПДн в части их касающейся и руководствуются ими в своей работе.

Общий контроль над исполнением требований организационно-распорядительной документации на СЗПДн в администрации возлагается на должностное лицо, ответственное за защиту ПДн.

7.5. Обучение работников по направлению обеспечения безопасности персональных данных

В администрации все работники, участвующие в обработке персональных данных, в обязательном порядке проходят обучение по следующим направлениям:

1) общие вопросы обеспечения информационной безопасности;

2) правила автоматизированной и неавтоматизированной обработки персональных данных и обеспечения безопасности персональных данных;

3) правила использования прикладных систем и технических средств обработки персональных данных;

4) правила использования средств защиты информации, входящих в состав СЗПДн;

5) ответственность за нарушение правил обработки и обеспечения безопасности персональных данных.

Ответственным за организацию и контроль проведения обучения работников администрации, участвующих в обработке и обеспечении безопасности персональных данных, является должностное лицо, ответственное за проведение работ по защите персональных данных в администрации.

Должностное лицо, ответственное за проведение работ по защите персональных данных в администрации, разрабатывает программу проведения обучения, которая согласовывается и утверждается должностным лицом, ответственным за организацию работ по обработке персональных данных.

Обучение может проводиться как самим должностным лицом, ответственным за проведение работ по защите персональных данных в администрации, так и с привлечением сторонних организаций.

Новые работники администрации, принимаемые на работу, в обязательном порядке проходят первичный инструктаж. Ответственным за направление работника на первичный инструктаж является должностное лицо, ответственное за организацию работ по обработке персональных данных в администрации.

Перед допуском работников администрации к работе с ПДн должностное лицо ответственное за проведение работ по защите ПДн проводит ознакомление с нормативной документацией, утвержденной в администрации, в области безопасности ПДн.

## 8. Модернизация СЗПДн

8.1. В случаях изменения состава или структуры ИСПДн администрации, состава угроз безопасности персональных данных или уровня защищенности ПДн, обработка которых осуществляется в ИСПДн администрации, проводится модернизация СЗПДн.

9. Мероприятия по организации и обеспечению

безопасности персональных данных

9.1. Под организацией обеспечения безопасности персональных данных при их обработке в ИСПДн администрации понимается формирование и реализация совокупности согласованных по целям, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

9.2. Организационные мероприятия по обеспечению безопасности персональных данных в администрации включает в себя:

1) мероприятия по обеспечению охраны и физической защиты помещений, в которых расположены технические средства ИСПДн, исключающие несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности;

2) обучение работников администрации правилам обработки и защиты персональных данных.

В целях осуществления технического обеспечения безопасности персональных данных при их обработке в ИСПДн администрации реализовываются мероприятия по защите от НСД к персональным данным.

Планирование мероприятий по обеспечению безопасности персональных данных осуществляется в соответствии с Разделом «Планирование работ по защите персональных данных».

## 10. Мероприятия по обеспечению управления доступом

10.1. Общие требования

Для организации системы допуска и учета должностных лиц, допущенных к работе с персональными данными в администрации, должен быть определен перечень должностных лиц и утвержден соответствующим распоряжением главы администрации.

В администрации должна быть реализована разрешительная система допуска пользователей и разграничение прав доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации с помощью функциональных возможностей операционной системы, прикладных систем обработки персональных данных либо специализированных средств защиты информации.

Работникам администрации предоставляется доступ к персональным данным и средствам их обработки в объеме, минимально необходимом для выполнения их трудовых обязанностей.

Для идентификации и аутентификации пользователей ИСПДн администрации должны применяться пароли условно-постоянного действия. Требования к формированию пароли и периодичности их смены определены в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности и Инструкция работника по правилам обработки ПДн).

10.2. Порядок проведения мероприятий

Своевременное предоставление работникам администрации прав доступа к персональным данным и средствам их обработки, а также изменение их полномочий обеспечивает должностное лицо, ответственное за проведение работ по защите персональных данных в администрации.

Порядок генерации, смены и прекращения действия паролей в ИСПДн администрации определен в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности).

11. Мероприятия по обеспечению регистрации и учета

11.1. Требования к учету и хранению носителей персональных данных

В администрации должен вестись учет как машинных, так и бумажных носителей персональных данных. Также должно быть организовано хранение и использование этих носителей, исключающее их хищение, подмену и уничтожение.

В администрации учету подлежат следующие типы машинных носителей персональных данных:

1) отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD, BD и прочее);

2) неотчуждаемые носители информации (жесткие магнитные диски).

11.2. Порядок проведения мероприятий

Порядок учета, хранения, использования носителей персональных данных (машинных и бумажных), а также порядок их уничтожения определены в документе «Порядок учета, хранения и уничтожения носителей персональных данных в администрации».

Ответственность за ведение учета машинных носителей персональных данных, организацию надлежащего хранения, а также уничтожение носителей персональных данных возлагается на должностное лицо, ответственное за защиту ПДн.

Контроль и ответственность за ведение учета бумажных носителей персональных данных, организацию надлежащего хранения, а также уничтожение носителей персональных данных возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

## 12. Мероприятия по обеспечению целостности

12.1. Требования к мероприятиям по обеспечению целостности

Сохранность и целостность программных средств ИСПДн и персональных данных являются обязательными и обеспечиваются в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн.

В администрации должен быть определен и документально зафиксирован состав и назначение ПО, используемого в ИСПДн. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, должен быть регламентирован.

Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован.

С целью недопущения изменения состава ПО ИСПДн, из него должны быть исключены программные средства, предназначенные для разработки и отладки ПО (либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения).

Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

В администрации должны быть реализованы механизмы восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним и/или возникновения форс-мажорных ситуаций или воздействия опасных факторов окружающей среды.

Требования к периодичности осуществления резервного копирования и требования к носителям, предназначенным для записи на них резервных копий, определены в документе «Порядок проведения резервного копирования персональных данных в администрации».

12.2. Порядок проведения мероприятий

Порядок организации резервного копирования и восстановления массивов информации в администрации определен в документе «Порядок проведения резервного копирования персональных данных в администрации».

Ответственность за организацию своевременного резервного копирования и восстановления информации, а также за надлежащее хранение резервных носителей, содержащих резервные копии данных, возлагается на должностное лицо ответственное за защиту ПДн.

## 13. Мероприятия по обеспечению антивирусной защиты

13.1. Требования к мероприятиям по обеспечению антивирусной защиты

Для предотвращения возможности внедрения в ИСПДн вредоносного программного обеспечения в администрации должны применяться антивирусные средства:

Требования к настройке антивирусных средств защиты определены в проектной документации на СЗПДн, процедуры по управлению антивирусными средствами определены в эксплуатационной документации СЗПДн (Руководство администратора информационной безопасности).

13.2. Порядок проведения мероприятий

Порядок использования антивирусных средств защиты определен в эксплуатационной документации СЗПДн (Руководство администратора информационной безопасности).

Администратор информационной безопасности осуществляет:

1) установку антивирусных средств защиты в соответствии с эксплуатационной и технической документацией к ним;

2) настройку параметров антивирусных средств защиты согласно требованиям по обеспечению безопасности, определенным в проектной документации на СЗПДн;

3) контроль эффективности работы антивирусных средств защиты;

Контроль соблюдения условий использования антивирусных средств защиты, предусмотренных эксплуатационной и технической документацией возлагается на должностное лицо ответственное за защиту ПДн.

## 14. Мероприятия по обеспечению криптографической защиты

14.1. Требования к мероприятиям по обеспечению криптографической защиты

В администрации должны применяться следующие типы средств криптографической защиты информации, сертифицированные ФСБ России:

1) СКЗИ для обеспечения безопасности персональных данных, передаваемых по каналам связи между Администрации и ИС сторонних организаций;

2) средства электронной подписи, т.е. шифровальные (криптографические) средства, используемые для подписания передаваемых документов и проверки электронной подписи получаемых документов.

СКЗИ, применяемые в администрации для защиты персональных данных, должны иметь класс, определенный в Частной модели угроз безопасности персональных данных при их обработке в ИСПДн администрации. Частная модель безопасности ПДн составляется на каждую ИСПДн.

Правила использования СКЗИ при обмене информацией со структурными подразделениями администрации должны быть определены в соответствующих регламентах, утвержденных администрацией.

Правила использования СКЗИ при обмене информацией со сторонними организациями СКЗИ должны быть определены условиями заключаемых договоров между администрации и данными организациями.

В администрации ведется учет всех применяемых СКЗИ, эксплуатационной и технической документации к ним, а также учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных.

14.2. На должностное лицо, ответственное за выполнение работ по защите персональных данных в администрации, возлагается ответственность за обеспечение функционирования и безопасности СКЗИ согласно требованиям руководящих документов ФСБ России.

## 15. Мероприятия по обеспечению физической защиты

15.1. Основные требования по обеспечению физической защиты:

В целях предотвращения несанкционированного входа (вскрытия) в помещения, а также исключения возможности неконтролируемого проникновения в эти помещения посторонних лиц, в администрации организуется и обеспечивается физическая охрана и техническая защита помещений администрации, с использованием охранной сигнализации, обеспечивающие сохранность технических средств обработки персональных данных, носителей персональных данных и средств защиты информации.

Защите подлежат следующие типы помещений:

1) помещения, в которых осуществляется непосредственно обработка персональных данных пользователями ИСПДн администрации;

2) серверные помещения, в которых установлено серверное, сетевое оборудование и технические средства защиты информации;

3) архивные помещения, в которых организовано хранение бумажных документов, содержащих персональных данных.

15.2. Перечень лиц, которые допускаются в указанные помещения, определяется распоряжением администрации.

15.3. В целях обеспечения физической защиты помещений применяться следующие средства защиты и контроля за несанкционированным вскрытием:

1) система охранной сигнализации;

2) двери помещений оборудуются замками для защиты от несанкционированного проникновения и местами для их опечатывания и сдачи под охрану;

3) устанавливаются металлические двери для защиты от несанкционированного проникновения в серверные и архивные помещения.

В целях организации противопожарной безопасности в администрации устанавливается система пожарной сигнализации

15.4. Порядок проведения мероприятий по обеспечению физической защиты:

Контроль обеспечения безопасности помещений, в которых расположены компоненты ИСПДн, возлагается на должностное лицо ответственное за защиту ПДн.

Доступ в защищаемые помещения осуществляется согласно перечню утвержденного распоряжением главы администрации.

Лица, не указанные в Перечне допущенных в защищаемые помещения, при наличии необходимости могут посещать помещения администрации только в сопровождении допущенных лиц.

Одиночное, бесконтрольное пребывание лиц, не допущенных к работе по обработке персональных данных, в помещениях администрации запрещено.

Пребывание посторонних лиц в серверных помещениях допускается в целях производственной необходимости, только в присутствии должностного лица, ответственного за защиту персональных данных или администратора информационной безопасности ИСПДн.

В случае утраты ключей (либо подозрении на утрату) к замкам в защищаемые помещения предпринимаются следующие меры:

1) оповещаются должностные лица, ответственные за организацию работ по обработке персональных данных за защиту ПДн служебной запиской;

2) производится немедленная замена запираемых замков;

3) назначается административная проверка всех режимных помещений с составлением акта и принятым мерам, виновные лица привлекаются к административной ответственности.

При возникновении форс-мажорных обстоятельств в защищаемых помещениях (возникновение пожара, затопление помещения, возгорание электропроводки и прочее) в отсутствии лиц, имеющих доступ в эти помещения, осуществляется вскрытие помещений с соблюдением следующих условий:

1) оповещается должностные лица ответственные за организацию работ по обработке и защите ПДн;

2) помещения вскрываются группой в составе не менее двух человек;

3) при вскрытии помещения составляется акт о вскрытии, в котором указываются должности и фамилии лиц, вскрывших помещение, дата, время и причины вскрытия.

16. Обязанности, права и ответственность должностных лиц

при обеспечении безопасности персональных данных

16.1. Обязанности, права и ответственность должностных лиц, участвующих в обеспечении безопасности персональных данных в администрации определены в документе «Положение о ролях и ответственности за обработку и защиту персональных данных в администрации».

17. Планирование работ по защите персональных данных

Планирование работ по защите информации, требования к содержанию плана, порядок разработки, согласования, утверждения и оформления плана, порядок отчетности и контроля над его выполнением определяются действующими нормативными документами Российской Федерации.

План определяет перечень основных проводимых организационно-технических мероприятий по защите информации (в том числе персональных данных) в администрации с указанием:

1) сроков выполнения мероприятий;

2) ответственных за выполнение соответствующих пунктов Плана работников.

В План включаются мероприятия по контролю состояния защищенности персональных данных;

План на очередной календарный год разрабатывается должностным лицом, ответственным за защиту ПДн, который осуществляет общий контроль над выполнением работ по защите информации.

Утвержденный план хранится у должностного лица ответственного за организацию работ по обработке ПДн.

Отчет о результатах выполнения запланированных мероприятий по обеспечению безопасности персональных данных за текущий год формируется должностным лицом, ответственным за защиту персональных данных, в рамках общего отчета работы за текущей год, утверждается главой администрации.

18. Контроль состояния защищенности персональных данных

Контроль состояния защищенности персональных данных в администрации осуществляется с целью своевременного выявления и предотвращения утечки конфиденциальной информации, отнесенной к категории персональных данных, вследствие НСД к ней, преднамеренных программно-технических воздействий на персональные данные и оценки защищенности персональных данных (далее - Контроль).

Контроль заключается в проверке выполнения требований действующих нормативных документов в области обработки и обеспечения безопасности персональных данных, в оценке обоснованности и эффективности принятых мер по защите персональных данных.

Контроль эффективности внедренных мер и СЗИ, входящих в состав СЗПДн, должен проводиться в соответствии с требованиями эксплуатационной документации на СЗПДн в целом на конкретные СЗИ, а также требованиями других нормативных документов не реже одного раза в год.

Обязательным является контроль СЗИ, входящих в состав СЗПДн, при вводе их в эксплуатацию после проведения ремонта таких средств, а также при изменении условий и расположения их эксплуатации.

Контроль обеспечения безопасности персональных данных в администрации организовывается должностным лицом, ответственным за проведение работ по защите персональных данных в администрации.

Контроль состояния и эффективности СЗПДн может осуществляться в соответствии с планом основных мероприятий по защите информации на текущий год или носить внеплановый характер.

Результаты периодического контроля оформляются отдельными протоколами или актами.

По всем выявленным нарушениям требований по защите персональных данных должностное лицо, ответственное за проведение работ по защите персональных данных в администрации, в пределах предоставленных ему прав и своих функциональных обязанностей обязано добиваться их немедленного устранения.

Должностное лицо, ответственное за организацию работ по обработке персональных данных в администрации, обязано принять все необходимые меры по немедленному устранению выявленных нарушений. При невозможности их немедленного устранения должна быть прекращена обработка персональных данных и организованы работы по устранению выявленных нарушений.

Работники администрации, осуществляющие обработку персональных данных в ИСПДн, обязаны выполнять требования должностного лица ответственного за защиту ПДн, по устранению допущенных ими нарушений норм и требований по обработке и/или обеспечении безопасности персональных данных. Также работники несут персональную ответственность за соблюдение требований по обеспечению безопасности персональных данных в ходе проведения работ.

Учет, хранение и выдача работникам паролей и ключей для системы защиты персональных данных от НСД, оперативный контроль действий работников, осуществляющих обработку персональных данных, осуществляет должностное лицо ответственное за защиту ПДн.

19. Управление инцидентами информационной безопасности

19.1. В администрации в целях своевременного устранения выявленных нарушений безопасности определен и задокументирован порядок действий при возникновении инцидентов информационной безопасности, связанных с нарушением требований по обработке и обеспечению безопасности персональных данных.

19.2. Требования к мероприятиям

К инцидентам информационной безопасности, связанным с нарушением требований по обработке и обеспечению безопасности персональных данных, относятся любые нарушения, приводящие к снижению уровня защищенности ИСПДн, в том числе несоблюдение условий хранения носителей персональных данных и использования средств защиты информации, которые могут привести к нарушению конфиденциальности, целостности или доступности ПДн.

В администрации в случаях возникновения подобных инцидентов информационной безопасности проводятся разбирательства, составляются заключения по фактам возникновения инцидентов, разрабатываются и принимаются меры по предотвращению возможных последствий инцидентов.

19.3. Порядок проведения мероприятий

Организация и контроль процесса реагирования на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности персональных данных, в администрации возлагается на должностное лицо ответственное за защиту ПДн.

Процедура управления инцидентами информационной безопасности, связанными с нарушением требований по обработке и обеспечению безопасности персональных данных, регламентирована в документе «Порядок реагирования на инциденты информационной безопасности в администрации». Данный документ определяет порядок проведения следующих мероприятий:

1) определение инцидента информационной безопасности;

2) оповещение ответственного лица о возникновении инцидента;

3) устранение последствий и причин инцидента;

4) расследование инцидента;

5) реализация необходимых корректирующих и превентивных мер.

Дополнительно порядок действий работников администрации в случаях возникновения инцидентов информационной безопасности определен в документе «Инструкция работника по правилам обработки персональных данных».

20. Модернизация системы защиты персональных данных

20.1. Для определения необходимости модернизации СЗПДн не реже одного раза в год должностным лицом ответственным за защиту ПДн проводится проверка состава и структуры СЗПДн, состава угроз и уровня защищенности ПДн, обработка которых осуществляется в ИСПДн администрации.

20.2. Модернизация СЗПДн в обязательном порядке проводится в случаях, если:

1) изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав обрабатываемых персональных данных, состав или структура программного обеспечения, технических средств обработки персональных данных, топологии ИСПДн и пр.);

2) изменился состав угроз безопасности персональных данных в ИСПДн;

3) изменился уровень защищенности ПДн.

Выбор мер и СЗИ, входящих в состав СЗПДн, проводится на основании проведенного анализа угроз и проведенной классификации ИСПДн (определения уровня защищенности ПДн).

20.3. Должностное лицо ответственное за защиту ПДн ежегодно разрабатывает план работ по обеспечению безопасности персональных данных в администрации, в котором определяется перечень необходимых мероприятий по обеспечению безопасности персональных данных с учетом уже выполненных мероприятий.

В план работ по обеспечению безопасности персональных данных включаются организационные и технические мероприятия, направленные на выполнение требований нормативно-правовых документов в области безопасности персональных данных и на совершенствование СЗПДн, а также контрольные мероприятия и мероприятия по проведению обучения работников администрации. В плане указываются дата, сроки проведения мероприятий, их периодичность (разовые или регулярные) и назначаются ответственные за их организацию и выполнение лица.

Работники, участвующие в обеспечении безопасности персональных данных   
в администрации вправе формировать предложения по совершенствованию СЗПДн и направлять их на рассмотрение должностному лицу ответственному за защиту ПДн, которое в свою очередь формирует сводный перечень предложений по совершенствованию СЗПДн.

Ежегодно должностное лицо ответственное за защиту ПДн формирует отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности персональных данных, обрабатываемых в администрации, и предоставляет его главе администрации совместно со сводным перечнем предложений по совершенствованию СЗПДн.

Ежегодный отчет по выполнению плана работ включает в себя:

1) результаты проведенной проверки состава и структуры, состава угроз и уровня защищенности ПДн;

2) результаты проведенных контрольных мероприятий по защите персональных данных;

3) результаты проверок регулирующими органами;

4) результаты анализа инцидентов информационной безопасности;

5) результаты плановых мероприятий по обеспечению безопасности персональных данных;

6) предложения по совершенствованию СЗПДн на основе полученных результатов.

На основании решения, принятого главой администрации, по результатам рассмотрения ежегодного отчета и предложений по совершенствованию СЗПДн должностное лицо ответственное за защиту ПДн составляет план работ по обеспечению безопасности персональных данных, обрабатываемых в администрации, на следующий год.

21. Привлечение сторонних организаций для проведения мероприятий по обеспечению безопасности персональных данных

21.1. В администрации могут привлекаться сторонние организации для проведения следующих мероприятий по обеспечению безопасности персональных данных:

1) разработка нормативно-методических материалов по вопросам обеспечения безопасности персональных данных;

2) поставка СЗИ и СКЗИ;

3) выполнение организационных и технических мероприятий в области защиты персональных данных, на проведение которых у администрации отсутствует соответствующее разрешение либо отсутствуют технические средства и подготовленные работники (специалисты);

4) выполнение организационных и технических мероприятий в области защиты персональных данных, выполнение которых силами администрации экономически нецелесообразно;

5) подтверждение соответствия мер по защите ИСПДн требованиям нормативно-правовой базы Российской Федерации в области безопасности персональных данных, путем проведения аттестационных испытаний ИСПДн администрации по требованиям безопасности информации;

6) контроль и аудит эффективности проводимых мероприятий по защите персональных данных.

21.2. Привлекаемые для оказания услуг в области защиты персональных данных сторонние организации должны иметь лицензии на соответствующие виды деятельности.

Перечень совместно выполняемых организационных и технических мероприятий в области защиты персональных данных определяется с учетом планируемых работ по созданию (реконструкции) ИСПДн и включается в План основных мероприятий по защите персональных данных.

В настоящем разделе определен порядок взаимодействия с вышеперечисленными сторонними организациями.

21.3. Привлечение сторонних организаций для проведения мероприятий по созданию и модернизации СЗПДн и/или проведению контрольных мероприятий

Привлекаемая сторонняя организация должна обладать соответствующими, проводимым работам, лицензиями и сертификатами.

Должностное лицо, ответственное за защиту ПДн, является ответственным за выбор организации, привлекаемой для проведения мероприятий по созданию или модернизации СЗПДн и проведению контрольных мероприятий. Должностное лицо, ответственное за защиту ПДн, осуществляет подбор подходящих организаций и формирует предложения для согласования с главой администрации.

Существенным условием договора является обязательство привлекаемой организации обеспечить конфиденциальность получаемой информации, ставшей известной в ходе выполнения работ по обеспечению безопасности персональных данных в администрации.

21.4. В случае привлечения сторонней организации для проведения мероприятий по созданию или модернизации СЗПДн в договоре прописываются обязательства привлекаемой организации по проведению необходимых организационно-технических мероприятий, включающих в себя:

1) организацию и проведение работ по созданию СЗПДн;

2) реализацию требований нормативно-правовых документов РФ в области обработки и защиты персональных данных;

3) своевременное совершенствование СЗПДн;

4) поддержание работоспособности и сопровождение СЗПДн.

21.5. В случае привлечения сторонней организации для проведения контрольных мероприятий (аудит обеспечения безопасности персональных данных) в договоре прописываются обязанности привлекаемой организации по выполнению необходимых работ, включающих   
в себя:

1) проверку выполнения требований нормативно-правовых документов РФ в области обработки и защиты персональных данных;

2) оценку обоснованности и эффективности принятых в администрации мер по обеспечению безопасности персональных данных.

Должностное лицо, ответственное за защиту ПДн, осуществляет контроль над выполнением привлекаемой организацией взятых на себя обязательств.

## 21.6. Привлечение сторонних организаций для проведения обучения работников

К организациям, привлекаемым для проведения обучения работников администрации по направлению обеспечения безопасности персональных данных, предъявляются следующие требования:

1) организация должна иметь лицензию на осуществление образовательной деятельности;

2) предлагаемые организацией программы и курсы обучения должны быть согласованы с регулирующими и надзорными органами;

3) по результатам проведенного обучения организация должна проводить итоговую аттестацию работников.

21.7. Привлечение сторонних организаций (подрядчиков) для ремонтно-восстановительных работ

Организацией обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн, в администрации занимается администратор информационной безопасности. В случае необходимости, ремонт технических средств может быть произведен с привлечением специалистов сторонних организаций на договорной основе с составлением актов выполненных работ.

Должностным лицом, ответственным за защиту ПДн, определяется порядок привлечения сторонних организаций (подрядчиков) для обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн.

Сопровождение и контроль сторонних организаций (подрядчиков) обеспечивается должностным лицом, ответственным за защиту ПДн.

Обязательным условием при передаче технических средств обработки персональных данных и машинных носителей ПДн для осуществления ремонтных работ сторонней организацией является удаление персональных данных с носителей, установленных на передаваемых устройствах, либо извлечение носителей персональных данных. Контроль исполнения данного требования возлагается на должностное лицо ответственное за защиту ПДн. В случае, когда выполнить данное требование не представляется возможным, должностным лицом, ответственным за защиту ПДн, составляется двусторонний протокол, в котором указано, что сторонняя организация осведомлена о том, какие именно персональные данные содержатся на носителе и обязана принять все необходимые меры по обеспечению их безопасности.

После проведения ремонта средств защиты или средств обработки персональных данных, при изменении условий их расположения или эксплуатации обязательно осуществляется проверка готовности этих средств к использованию с составлением заключений о возможности их эксплуатации.

22. Пересмотр и внесение изменение в настоящее Положение

22.1. Настоящее Положение должно пересматриваться в случаях:

1) изменения требований законодательства Российской Федерации в области обработки и обеспечения информационной безопасности персональных данных;

2) изменением организационной и технологической инфраструктуры, в рамках которой обрабатываются персональных данных;

3) выявления снижения общего уровня информационной безопасности администрации (по результатам регулярного мониторинга или аудита).

22.2. Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо, ответственное за защиту персональных данных в администрации.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Приложение № 2

к постановлению администрации

от «20» 06. 20 16 г.№ 325

Положение

о ролях и ответственности за обработку и защиту персональных данных в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области

# 1. Используемые сокращения

В настоящем Положении использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

|  |  |  |
| --- | --- | --- |
| № п/п | Сокращение | Описание |
| 1. | ИБ | Информационная безопасность |
| 2. | ИСПДн | Информационная система ПДн |
| 3. | ПДн | Персональные данные |
| 4. | СЗИ | Средства защиты информации |
| 5. | СЗПДн | Система защиты ПДн |

# 2. Область применения

2.1. Настоящее Положение о ролях и ответственности за обработку и защиту персональных данных (далее – Положение) предназначено для определения основных ролей сотрудников администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области (далее ‑ администрация) при обеспечении безопасности персональных данных, обрабатываемых в администрации, в соответствии с требованиями нормативных документов РФ, в области обработки и защиты ПДн.

2.2. Настоящее Положение доводится до сведения всех сотрудников администрации, участвующих в обработке и обеспечении безопасности персональных данных.

2.3. Общее руководство и контроль над выполнением положений данного документа возложены на должностное лицо ответственное за организацию работ по обработке ПДн.

# 3. Роли и ответственность

3.1. В целях разграничения обязанностей и функций работников в области обработки и обеспечения безопасности ПДн в администрации вводятся следующие роли:

1) должностное лицо ответственное за организацию работ по обработке ПДн;

2) должностное лицо ответственное за защиту ПДн;

3) администратор информационной безопасности (ИБ);

4) сотрудники администрации (пользователи ИСПДн).

3.2. Должностное лицо, ответственно за организацию работ по обработке персональных данных назначается распоряжением администрации.

Должностное лицо, ответственное за защиту ПДн и администратор информационной безопасности назначаются распоряжением администрации.

3.3. Все работники, назначенные на соответствующую роль, в своей работе руководствуются требованиями организационно-распорядительных документов, регламентирующих требования по обеспечению безопасности ПДн.

## 4. Права, обязанности и ответственность должностного лица,

## ответственного за организацию работ по обработке ПДн

4.1. Должностное лицо, ответственное за организацию работ по обработке ПДн обязано:

1) взаимодействовать с регулирующими органами по вопросам обработки и обеспечения безопасности персональных данных;

2) давать ответственному за защиту ПДн поручения по взаимодействию с регулирующими органами в рамках его компетенции;

3) контролировать договора с третьими лицами на предмет их соответствия требованиям организационно-распорядительных документов администрации по обработке и обеспечению безопасности ПДн;

4) предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении контрольных мероприятий по обеспечению безопасности ПДн;

5) обеспечивать выполнение требований по обработке и обеспечению безопасности ПДн в соответствии с Правилами о порядке обработки персональных данных в администрации и иными нормативными документами в области обработки и защиты ПДн;

6) осуществлять непрерывный контроль действий подчиненных при обработке ПДн, разъяснять и требовать от подчиненных выполнения требований нормативных документов в области обработки и защиты ПДн;

7) участвовать в процессе разработки организационно-распорядительных документов, регламентирующих требования по обеспечению информационной безопасности ПДн, обрабатываемых в администрации;

8) определять необходимость и направлять на обучение сотрудников администрации (пользователей ИСПДн);

9) предоставлять консультации сотрудникам администрации (пользователям ИСПДн) по вопросам автоматизированной и неавтоматизированной обработки ПДн   
в рамках своих компетенций;

10) организовывать и контролировать своевременное предоставление сотрудникам администрации доступа к ПДн и средствам их обработки в объеме, необходимом для выполнения ими своих трудовых обязанностей;

11) определять права доступа к ПДн и автоматизированным средствам обработки ПДн в рамках своих компетенций;

12) сообщать о выявленных нарушениях требований Положения о порядке обработки персональных данных в администрации и должностному лицу ответственному за защиту ПДн.

4.2. Должностное лицо, ответственное за организацию работ по обработке ПДн имеет право:

1) формировать предложения по совершенствованию системы защиты персональных данных для должностного лица ответственного за защиту ПДн;

2) формировать предложения о необходимости проведения контрольных мероприятий по обеспечению безопасности персональных данных для должностного лица ответственного за защиту ПДн;

3) формировать предложения по внесению изменений в организационно-распорядительные документы, регламентирующие требования по обеспечению информационной безопасности ПДн, обрабатываемых в администрации;

4) запрашивать у сотрудников администрации, участвующих в обработке и обеспечении безопасности персональных данных, информации и документов, необходимых для выполнения своих функциональных обязанностей.

4.3. Должностное лицо, ответственное за организацию работ по обработке ПДн несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Положением.

## 5. Права, обязанности и ответственность должностного лица,

## ответственного за защиту ПДн

5.1. Должностное лицо, ответственное за защиту персональных данных обязано:

1) проводить мониторинг изменений в законодательных и нормативных актах Российской Федерации, касающихся обработки и обеспечения безопасности ПДн;

2) организовывать контроль состояния СЗПДн администрации и соблюдения сотрудниками установленных норм и требований по обеспечению безопасности ПДн;

3) организовывать разработку и поддержание в актуальном состоянии организационно-распорядительных документов, определяющих требования и порядок обработки и обеспечения безопасности ПДн в администрации;

4) утверждать параметры конфигурации компонентов СЗПДн;

5) согласовывать права доступа работников к ПДн и средствам их обработки;

6) утверждать решения о привлечении сторонних организаций (подрядчиков) для обслуживания, настройки и ремонта СЗИ, входящих в состав СЗПДн;

7) оформлять допуск сотрудников администрации к средствам криптографической защиты информации (СКЗИ);

8) контролировать выдачу СКЗИ сотрудникам администрации и ведение журнала учета выдачи СКЗИ;

9) проводить обучение сотрудников администрации правилам работы с СКЗИ   
и выдавать работникам СКЗИ;

10) инициировать процесс получения ключевой информации для СКЗИ;

11) организовывать и контролировать процесс реагирования на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности ПДн;

12) проводить анализ произошедших инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн, и организовывать мероприятия, нацеленные на их предотвращение и недопущение их повторения;

13) взаимодействовать с регулирующими органами по вопросам защиты ПДн при проведении плановых и внеплановых проверок регулирующими органами (по указанию должностного лица, ответственного за организацию работ по обработке ПДн);

14) организовывать сбор и предоставление необходимой информации при проведении проверок регулирующими органами и при проведении внутренних контрольных мероприятий по обеспечению безопасности ПДн;

15) информировать должностное лицо, ответственное за организацию работ по обработке о состоянии СЗПДн, о планируемых мероприятиях, нацеленных на обеспечение безопасности ПДн, а также о результатах проведенных мероприятий;

16) организовывать расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;

17) обеспечивать непрерывное функционирование СЗПДн в целом и ее программных и технических компонентов в отдельности;

18) организовывать разработку инструкции Пользователям ПДн по работе со СЗИ;

19) контролировать учет носителей ПДн и обеспечивать их безопасное уничтожение;

20) контролировать обслуживание, настройку и ремонт средств обработки ПДн и СЗИ, входящих в состав СЗПДн;

21) сопровождать и контролировать сторонние организации (подрядчиков), в случае привлечения их для обслуживания, настройки и ремонта средств обработки ПДн и СЗИ, входящих в состав СЗПДн;

22) осуществлять контроль за взаимодействием с субъектами ПДн.

5.2. Должностное лицо, ответственное за защиту персональных данных имеет право:

1) формировать предложения по внесению изменений в организационно-распорядительные документы на СЗПДн администрации;

2) запрашивать у лиц, участвующих в обработке и обеспечении безопасности ПДн, информацию и документы, необходимые для выполнения указанных выше обязанностей.

3) формировать предложения для должностного лица ответственного   
за организацию работ по обработке ПДн о необходимости проведения контрольных проверок сотрудников администрации (пользователей ИСПДн) по выполнению требований по обеспечению безопасности ПДн.

5.3. Должностное лицо, ответственное за защиту персональных данных несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Положением.

## 

## 6. Права, обязанности и ответственность

## администратор информационной безопасности

6.1. Администратор информационной безопасности обязан:

1) проводить мониторинг изменений в законодательных и нормативных актах Российской Федерации, касающихся обработки и обеспечения безопасности ПДн;

2) осуществлять проведение контрольных проверок Пользователей ПДн по выполнению требований по обеспечению безопасности ПДн;

3) по поручению должностного лица ответственного за защиту ПДн разрабатывать и поддерживать в актуальном состоянии организационно-распорядительные документы, определяющие требования и порядок обработки и обеспечения безопасности ПДн   
в администрации;

4) проводить обучение сотрудников администрации правилам работы с СКЗИ   
и выдавать работникам СКЗИ;

5) вести журнал учета выданных СКЗИ;

6) согласовывать права доступа работников к ПДн и средствам их обработки;

7) совместно с должностным лицом, ответственным за защиту ПДн проводить анализ произошедших инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн, и выполнять мероприятия, нацеленные на их предотвращение и недопущение их повторения;

8) в рамках своей компетенции взаимодействовать с регулирующими органами по вопросам защиты ПДн при проведении плановых и внеплановых проверок регулирующими органами (по указанию должностных лиц ответственных за организацию работ по обработке и защите ПДн);

9) по указанию должностного лица, ответственного за защиту ПДн собирать и предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении внутренних контрольных мероприятий по обеспечению безопасности ПДн;

10) принимать участие в расследовании инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;

11) обеспечивать непрерывное функционирование СЗПДн в целом и ее программных и технических компонентов в отдельности;

12) разрабатывать инструкции Пользователям ПДн по работе со СЗИ;

13) предоставлять экспертные консультации и рекомендации по вопросам использования СЗИ работникам, участвующим в обработке и обеспечении безопасности ПДн;

14) вести учет носителей ПДн и обеспечивать их безопасное уничтожение;

15) проводить обслуживание, настройку и ремонт средств обработки ПДн и СЗИ, входящих в состав СЗПДн;

16) определять параметры конфигурации компонентов ИСПДн (параметры конфигурации автоматизированных систем обработки ПДн, параметры конфигурации средств обработки и СЗИ, входящих в состав СЗПДн);

17) вести журналы учета СЗИ;

18) хранить эталонные версии программного обеспечения СЗИ;

19) настраивать параметры конфигурации СЗИ, входящих в состав СЗПДн;

20) назначать права доступа сотрудников администрации (пользователей ИСПДн) к ПДн и средствам их обработки в ИСПДн, согласно требованиям по обеспечению информационной безопасности ПДн;

6.2. Администратор информационной безопасности имеет право:

1) формировать предложения по внесению изменений в организационно-распорядительные документы на СЗПДн администрации;

2) запрашивать у лиц, участвующих в обработке и обеспечении безопасности ПДн, информацию и документы, необходимые для выполнения указанных выше обязанностей.

3) формировать предложения для должностных лиц ответственных за организацию работ по обработке и защите ПДн о необходимости проведения контрольных проверок сотрудников администрации (пользователей ИСПДн) по выполнению требований   
по обеспечению безопасности ПДн.

6.3. Администратор информационной безопасности несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Положением.

## 

## 7. Сотрудники администрации (пользователи ИСПДн)

7.1. Сотрудники администрации (пользователи ИСПДн) обязаны:

1) соблюдать требования организационно-распорядительных документов, регламентирующих требования по обеспечению информационной безопасности ПДн, обрабатываемых в администрации;

2) проходить обучения и инструктажи по вопросам обработки и обеспечения безопасности ПДн;

3) предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении внутренних контрольных мероприятий по защите ПДн;

4) сообщать о выявленных нарушениях требований Положения о порядке обработки персональных данных в администрации должностному лицу, ответственному за организацию работ по обработке ПДн и ответственному за защиту ПДн.

7.2. Сотрудники администрации (пользователи ИСПДн) имеют право:

1) получать доступ к ПДн в рамках выполнения своих трудовых обязанностей;

2) получать консультации и рекомендации, по вопросам обработки и обеспечения безопасности ПДн от должностных лиц, ответственных за организацию обработки и обеспечение безопасности ПДн в администрации.

7.3. Сотрудники администрации (пользователи ИСПДн) несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Положением.

# 8. Пересмотр и внесение изменений в настоящее Положение

8.1. Настоящее Положение должно пересматриваться в случаях:

1) изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;

2) изменением организационной и технологической инфраструктуры, в рамках которых обрабатываются ПДн;

3) выявления снижения общего уровня ИБ в администрации (по результатам регулярного мониторинга или аудита).

8.2. Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо, ответственное за защиту персональных данных в администрации.

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

Приложение № 3

к постановлению администрации

от «20» 06. 20 16 г.№ 325

Порядок

реагирования на инциденты информационной безопасности в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области

# Используемые сокращения

В настоящем Порядке использованы следующие сокращения, приведенные   
в Таблице 1:

Таблица 1. Сокращения

|  |  |  |
| --- | --- | --- |
| № п/п | Сокращение | Описание |
| 1. | ИБ | Информационная безопасность |
| 2. | ИСПДн | Информационная система ПДн |
| 3. | НСД | Несанкционированный доступ |
| 4. | ПДн | ПДн |

# Область применения

2.1. Настоящий Порядок реагирования на инциденты информационной безопасности (далее – Порядок) предназначен для определения единого порядка реагирования на возникшие инциденты информационной безопасности, проведения служебных расследований, а так же проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области (далее ‑ администрация).

2.2. Требования настоящего Порядка распространяются на должностных лиц администрации, отвечающие за обеспечение безопасности ПДн.

# Общие положения

3.1. Настоящий Порядок разработан в соответствии с Правилами о порядке обработки персональных данных в администрации.

3.2. В соответствии с настоящим Порядком к инцидентам ИБ в администрации относятся:

1) нарушение конфиденциальности, целостности или доступности ПДн;

2) отказ оборудования, сервисов, средств обработки и (или), входящих в состав ИСПДн;

3) несоблюдение требований внутренних организационно-распорядительных документов и действующих нормативных документов РФ в области обработки и защиты ПДн (нарушение правил обработки ПДн);

4) заражение программных компонентов ИСПДн вредоносным программным обеспечением.

3.3. К инцидентам ИБ в ИСПДн также относятся попытки и факты получения НСД к ИСПДн:

1) сеансы работы в ИСПДн незарегистрированных пользователей;

2) сеансы работы Пользователей ИСПДн, срок действия полномочий которых истек, либо в состав полномочий которых не входят выявленные действия с ПДн;

3) действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой выгоды, методом подбора пароля или иными методами (случайного разглашения пароля и т.п.) без ведома владельца учетной записи;

4) совершение попыток несанкционированного доступа к рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);

5) несанкционированное внесение изменений в параметры конфигурации

программных или аппаратных средств обработки или защиты, входящих в состав ИСПДн.

3.4. Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для возникновения описанных выше инцидентов.

# Оповещение об инциденте информационной безопасности

4.1. В случае выявления инцидента ИБ устанавливается следующая последовательность действий сотрудников администрации:

1. прекратить работу с ресурсом, в котором выявлен инцидент ИБ;

2) оповестить своего непосредственного руководителя о факте выявления инцидента ИБ;

3) руководитель должен оповестить должностное лицо ответственное за защиту ПДн;

4) после извещения указанных должностных лиц по их требованию предоставить всю необходимую информацию.

4.2. Должностное лицо ответственное за защиту ПДн проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его возникновению, и составляет краткую справку, в которой описывается произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ. Справка направляется главе администрации для принятия решения о проведении расследования инцидента ИБ.

# 5. Мероприятия при возникновении инцидента информационной безопасности, ставшего причиной возникновения негативных последствий для субъекта ПДн

5.1. В случае если инцидент ИБ может стать (или уже стал) причиной возникновения негативных последствий для субъектов ПДн, необходимо немедленно блокировать ПДн этих субъектов до устранения причин повлекших за собой возникновение инцидента ИБ.

5.2. Решение о блокировании ПДн принимает должностное лицо ответственное за защиту ПДн.

5.3. ПДн остаются заблокированными до устранения причин, повлекших за собой возникновение инцидента ИБ.

# 6. Проведение расследования инцидента информационной безопасности

6.1. Внутреннее расследование и составление заключений должно в обязательном порядке проводиться в случае выявления:

1) нарушения конфиденциальности, целостности или доступности ПДн;

2) халатности и несоблюдения требований по обеспечению безопасности ПДн;

3) несоблюдения условий хранения носителей ПДн;

4) использования СЗИ, которые могут привести к нарушению заданных характеристик безопасности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

6.2. Задачами внутреннего расследования являются:

1) установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

2) установление лиц, непосредственно виновных в данном нарушении;

3) выявление причин и условий, способствовавших нарушению.

6.3. Проведение внутреннего расследования проводится по решению главы администрации. С целью проведения расследования в обязательном порядке формируется Комиссия, в состав которой входят должностное лицо ответственное за защиту персональных данных и администратор ИБ, юрист и иные должностные лица администрации, участие которых может потребоваться

Комиссия должна приступить к работе по расследованию не позднее следующего рабочего дня после даты выявления инцидента ИБ.

Общая продолжительность внутреннего расследования не должна превышать тридцати календарных дней.

В рамках проведения расследования инцидента ИБ Комиссия уполномочена:

1) проводить опрос сотрудников администрации, по вине которых предположительно произошел инцидент ИБ, а также должностных лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента ИБ;

2) проводить осмотр объектов и предметов, которые могут иметь отношение к инциденту ИБ.

По решению главы администрации на Комиссию могут быть возложены дополнительные обязанности и права.

6.4. Работник, в отношении которого проводится расследование, должен быть ознакомлен с распоряжением о проведении расследования.

6.5. Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (акты, протоколы, справки и т.п.).

6.6. Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами Комиссии в виде протокола.

6.7. В целях исключения возможности какого-либо воздействия на процесс расследования члены Комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения главой администрации.

6.8. Для оперативного проведения внутреннего расследования должностное лицо ответственного за защиту ПДн составляет План проведения расследования.

6.9. Одновременно с проведением внутреннего расследования, глава администрации может поручить Комиссии определить ущерб для администрации и (или) для субъекта ПДн от произошедшего инцидента ИБ. В отдельных случаях такая оценка может быть осуществлена с привлечением специализированной организации.

6.10. По окончании внутреннего расследования Комиссия представляет главе администрации отчет по результатам расследования, в котором излагаются:

1) основания и время проведения расследования;

2) проделанная работа (кратко);

3) время, место и обстоятельства факта нарушения;

4) причины и условия совершения нарушения;

5) виновные лица и степень их вины;

6) наличие умысла в действиях виновных лиц;

7) предложения по возмещению ущерба;

8) предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;

9) рекомендации по исключению подобных нарушений;

10) другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т. д.).

К отчету прилагаются:

1) письменные объяснения лиц, которых опрашивали члены Комиссии;

2) акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т. д.;

3) другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба.

Отчет должен быть подписан всеми членами Комиссии. При несогласии с выводами или содержанием отдельных положений член Комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

Отчет подлежит утверждению главой администрации.

6.11. Работник, в отношении которого проводится расследование, или его уполномоченный представитель имеют право ознакомления с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с отчетом по результатам расследования.

6.12. Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется распоряжением администрации.

6.13. При наличии в действиях работника признаков административного правонарушения или уголовного преступления глава администрации обязан обратиться в правоохранительные органы для привлечения виновного к ответственности, в соответствии с положениями нормативных документов РФ.

6.14. В соответствии с Трудовым кодексом РФ, возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нанесение ущерба.

6.15. Первый экземпляр отчета с резолюцией главы администрации, копия распоряжения (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дела о внутренних расследованиях хранятся у главы администрации.

# 7. Превентивные меры по недопущению повторного

# возникновения инцидентов информационной безопасности

7.1. Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение, в зависимости от произошедшего инцидента ИБ, включают в себя:

1) мониторинг событий в информационной системе ПДн;

2) своевременное удаление неиспользуемых учетных записей;

3) контроль и мониторинг действий пользователей в информационной системе ПДн;

4) контроль действий системных администраторов;

5) проведение обучения (повторного обучения) пользователей правилам обработки и обеспечения безопасности ПДн;

6) ознакомление пользователей с мерами ответственности, установленными

нормативными документами РФ, за нарушение норм и правил обработки ПДн, а также за разглашение полученных данных.

# 8. Пересмотр и внесение изменений в настоящий Порядок

8.1. Настоящий Порядок должен пересматриваться в случаях:

1) изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;

2) по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;

3) по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн.

8.2. Ответственным за пересмотр настоящего Порядка и составление рекомендаций по изменению является должностное лицо, ответственное за защиту персональных данных в администрации.

**\_\_\_\_\_\_\_\_\_\_\_\_**

Приложение № 4 к постановлению администрации

от «20» 06. 20 16 г.№ 325

Порядок

учета, хранения и уничтожения носителей персональных данных в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области

# Используемые сокращения

В настоящем Порядке использованы следующие сокращения, приведенные   
в Таблице 1:

Таблица 1. Сокращения

|  |  |  |
| --- | --- | --- |
| № п/п | Сокращение | Описание |
| 1. | ИСПДн | Информационная система персональных данных |
| 2. | ОС | Операционная система |
| 3. | ПДн | Персональные данные |
| 4. | СВТ | Средство вычислительной техники |
| 5. | СЗПДн | Система защиты персональных данных |

# 

# Область применения

2.1. Настоящий Порядок учета, хранения и уничтожения носителей персональных данных (далее – Порядок) предназначен для определения единого порядка обращения с машинными (электронными) и бумажными носителями персональных данных в администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области (далее ‑ администрация).

# Общие положения

3.1. Настоящий Порядок устанавливает порядок учета, хранения, использования и уничтожения носителей ПДн в процессах обработки ПДн.

3.2. Настоящий Порядок разработан в соответствии с Положением об обеспечении безопасности персональных данных в администрации.

# Порядок работы с бумажными носителями

## 

## 4.1. Порядок учета бумажных носителей, содержащих ПДн

Любой документ, содержащий ПДн, является конфиденциальным и подлежит обязательному учету. Учет документов, содержащих ПДн, осуществляется в соответствии с положениями настоящего Порядка.

Ответственность за организацию ведения учета документов возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

## 4.2. Порядок хранения бумажных носителей, содержащих ПДн

С целью обеспечения физической сохранности документов, содержащих ПДн, предотвращения хищения документов, а также с целью недопущения разглашения содержащихся в них сведений документы должны храниться в местах, исключающих доступ к ним посторонних лиц.

Хранение открытых документов вместе с конфиденциальными документами разрешено только в случаях, когда они являются приложениями к конфиденциальным документам.

Рабочее место работника администрация должно быть организовано таким образом, чтобы исключить возможность просмотра документов с ПДн лицами, которые не допущены к ПДн.

Во время работы на столе должны находиться только те документы, непосредственно с которыми ведется работа, все остальные должны быть убраны в места, предназначенные для хранения.

## 4.3. Порядок уничтожения бумажных носителей, содержащих ПДн

Основанием для уничтожения документов, содержащих ПДн, является достижение целей обработки.

Локальные документы, содержащие ПДн, уничтожаются по мере необходимости.

Ответственность за своевременное уничтожение документов возлагается на должностное лицо, ответственное за организацию работ по обработке ПДн.

Уничтожение документов производится с помощью специальных бумагорезательных технических средств (шредеров) или сжиганием.

4.4. Уничтожение массивов документов

Массивы документов (архивы, библиотеки и т.п.) уничтожаются под контролем должностного лица, ответственного за защиту ПДн.

Экспертиза документа проводится раз в год. Экспертиза охватывает все документы, содержащие ПДн, за соответствующий период времени.

Экспертиза проводится путем изучения содержания документов. Цель проведения экспертизы – определить возможность уничтожения документов либо дальнейшие сроки их хранения.

После проведения экспертизы составляется Акт о выделении дел и документов, подлежащих уничтожению (Приложение А). В Акт включаются отобранные дела для уничтожения, отдельные документы из дел и документы выделенного хранения.

Уничтожение массивов документов производится с помощью бумагорезательных технических средств или сжиганием.

Если уничтожение массивов документов производит третья сторона, с которой заключен соответствующий договор, то документы, выделенные для уничтожения, помещаются в короба, после чего короба запечатываются и передаются третьей стороне.

После уничтожения массива документов должностными лицами ответственными   
за организацию работ по обработке ПД и за защиту ПДн, а также работниками производившими уничтожение документов подписывается Акт об уничтожении документов, содержащих ПДн (Приложение Б).

# Порядок работы с машинными носителями

5.1. Учету подлежат следующие типы машинных носителей ПДн:

1) отчуждаемые носители информации (внешние жесткие магнитные диски,

гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD и прочее);

2) неотчуждаемые носители информации (жесткие магнитные диски).

5.2. Порядок учета машинных носителей, содержащих ПДн

Все отчуждаемые машинные носители данных, используемые при работе со средствами вычислительной техники (далее ‑ СВТ) для обработки и хранения ПДн, обязательно регистрируются и учитываются в Журнале учета выдачи машинных носителей ПДн (Приложение В).

Неотчуждаемые носители информации подлежат учету в составе системных блоков СВТ, которые в свою очередь учитываются в Техническом паспорте ИСПДн.

5.3. Ответственность за ведение Журнала учеты выдачи машинных носителей ПДн и контроль учета носителей ПДн возлагается на администратора информационной безопасности.

5.4. Каждому машинному носителю, содержащему ПДн, присваивается учетный номер согласно Журналу.

В качестве учетного номера допускается использование серийного (заводского) номера носителя. В случае отсутствия серийного номера, учетный номер наносится на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.

5.5. Порядок использования машинных носителей ПДн

Машинные носители ПДн выдаются пользователям или другим лицам, участвующим в обработке ПДн, для работы под подпись в Журнале. По завершении работы машинные носители ПДн сдаются обратно.

В случае повреждения машинных носителей ПДн, работник, за которым закреплен носитель, сообщает о случившемся должностному лицу, ответственному за защиту ПДн.

Передача носителя, содержащего ПДн, третьим сторонам производится в соответствии с требованиями договора между администрацией и третьим лицом.

Машинные носители ПДн пересылаются в том же порядке, что и документы.

При фиксации ПДн на машинных носителях не допускается фиксация на одном машинном носителе ПДн, цели обработки которых заведомо не совместимы.

Вынос машинных носителей, содержащих ПДн, за пределы контролируемой зоны администрация запрещается без соответствующего разрешения должностного лица ответственного за защиту ПДн.

## 5.6. Порядок хранения машинных носителей ПДн

Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможность хищения, нарушения целостности или уничтожения содержащейся на них информации.

Отчуждаемые съемные носители после окончания работы с ними должны убираться в сейфы или металлические шкафы, запираемые на ключ.

Не допускается оставлять без присмотра на рабочем столе или в СВТ машинные носители, содержащие ПДн.

Персональную ответственность за сохранность полученных машинных носителей и предотвращение несанкционированного доступа к записанным на них ПДн несет работник, за которым закреплен носитель.

## 5.7. Порядок уничтожения машинных носителей ПДн

Основанием для уничтожения машинных носителей ПДн, является повреждение машинного носителя, исключающее его дальнейшее использование, или потеря практической ценности носителя. Решение об уничтожении машинного носителя принимает должностное лицо ответственное за защиту ПДн.

Списанные машинные носители, подлежащие уничтожению, хранятся в сейфе должностного лица ответственного за защиту ПДн. Уничтожение таких носителей производится раз в год.

Уничтожение носителей производится путем их физического разрушения с предварительным затиранием (форматированием, уничтожением) содержащихся на них ПДн, если это позволяют физические принципы работы носителя.

Уничтожение машинных носителей производится Комиссией в составе не менее 3 человек. В состав Комиссии должно обязательно входить должностное лицо, ответственное за защиту ПДн. После уничтожения всех машинных носителей составляется Акт об уничтожении персональных данных (Приложение Г).

При уничтожении, машинные носители снимаются с учета. Отметка об уничтожении носителей проставляется в Журнале.

## 5.8. Порядок уничтожения (стирания) ПДн с машинного носителя

Основанием для уничтожения (стирания) записей или части записей с электронного носителя являются следующие случаи:

1) возврат носителя сотрудником;

2) передача носителя в ремонт;

3) списание носителя.

Хранящаяся на электронных носителях и потерявшая актуальность информация, содержащая ПДн, своевременно стирается (уничтожается). Работник, совместно с администратором информационной безопасности, принимает окончательное решение о необходимости уничтожения (стирания) с него записей.

Работник осуществляет уничтожение информации с носителя самостоятельно, с использованием встроенных средств ОС.

При невозможности самостоятельного уничтожения информации с носителя, работник передает электронный носитель должностному лицу ответственному за защиту ПДн. Совместно с носителем передается служебная записка, в которой указывается причины передачи (возврата) и основание для уничтожения содержащейся на нем информации.

Должностное лицо, ответственное за защиту ПДн, ответственное за уничтожение (стирание) информации с электронных носителей, при получении носителя должно обеспечить уничтожение (стирание) информации с носителя, способом, исключающим ее дальнейшее восстановление и подготовить Акт об уничтожении персональных данных (Приложение Г).

В Акт заносится дата, учетный номер носителя и способ уничтожения (стирания) информации, а также используемые для этого программные средства.

Носители, пригодные к повторной эксплуатации, после уничтожения записанной на них информации могут быть использованы для повторной записи информации.

# Пересмотр и внесение изменений

6.1. Пересмотр положений настоящего документа проводится в следующих случаях:

1) при появлении новых требований к обработке и обеспечению безопасности

ПДн со стороны законодательства РФ и контролирующих органов исполнительной власти Российской Федерации;

2) по результатам внутреннего контроля (аудита) системы защиты ПДн, в

случае выявления существенных нарушений;

3) по результатам расследования инцидентов информационной безопасности,

связанных с обработкой и обеспечением безопасности ПДн.

6.2. Ответственным за пересмотр настоящего Порядка и составление рекомендаций по изменению является должностное лицо, ответственное за защиту ПДн.

**\_\_\_\_\_\_\_\_\_\_\_\_**

# Приложение А

А К Т № \_\_\_\_\_\_

о выделении дел и документов, подлежащих уничтожению

от «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_201\_ г.

Комиссия в составе:

<Фамилия И.О. – должность;>

<Фамилия И.О. – должность.>

<Фамилия И.О. – должность.>

составила настоящий акт о том, что на основании проведенной экспертизы, отобрала к уничтожению, следующие документы и дела, утратившие практическую ценность:

|  |  |  |
| --- | --- | --- |
| **№ п\п** | **Заголовок документа\дела** | **Основание для уничтожения** |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Члены комиссии: |  |  |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# Приложение Б

А К Т № \_\_\_\_\_\_

уничтожения бумажных носителей, содержащих

персональные данные

от «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

Комиссия в составе:

<Фамилия И.О. – должность;>

<Фамилия И.О. – должность.>

<Фамилия И.О. – должность.>

составила настоящий акт о том, что произведено плановое уничтожение бумажных носителей, содержащих персональные данные, с истекшим сроком использования и/или утративших практическое значение.

* «тип носителя, учётный номер носителя»
* «тип носителя, учётный номер носителя»
* …

Бумажные носители уничтожены путём сжигания/шредирования/химической обработки и т.п. *(нужное отметить)*.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Члены комиссии |  |  |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# Приложение В

Журнал учета носителей информации, содержащих персональные данные

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Учетный № носителя | Дата | Тип носителя | Содержимое носителя | Ф.И.О.  отв. лица | Подпись отв. лица | Отметка о возврате (с указанием причины) | Ф.И.О. отв. лица | Подпись отв. лица | Дата уничтожения носителя | Ф.И.О. отв. за уничтожение |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

# Приложение Г

|  |
| --- |
| УТВЕРЖДАЮ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (руководитель органа местного самоуправления)  \_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись)  «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г. |

# Акт об уничтожении персональных данных

Комиссия в составе:

Председатель – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Дата | Тип носителя | Регистрационный номер  носителя ПДн | Примечание |
|  |  |  |  |  |
|  |  |  |  |  |

Всего съемных носителей \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем

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

(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем

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

(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_/

Члены комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_/

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_/