18-ОД

КОМИТЕТ ГОРОДСКОГО ХОЗЯЙСТВА
администрации города Ставрополя

ПРИКАЗ

«13» 04 2020 г. г. Ставрополь № 50

Об утверждении положения по организации работы с персональными данными комитета городского хозяйства администрации города Ставрополя и положения по организации и проведению работы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии с постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативно правовыми актами, операторами, являющимися государственными или муниципальными органами»

ПРИКАЗЫВАЮ:

1. Утвердить положение по организации работы с персональными данными в комитете городского хозяйства администрации города Ставрополя согласно приложению.
2. Утвердить положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных согласно приложению.
3. Настоящий приказ вступает в силу с момента его подписания.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Заместитель главы администрации
города Ставрополя, руководитель
комитета городского хозяйства
администрации города Ставрополя И.А. Скорняков

Приложение 1
к приказу комитета городского
хозяйства администрации города
Ставрополя
от «13» 04 2020 г. № 50

ПОЛОЖЕНИЕ
по организации работы с персональными данными в комитете городского хозяйства администрации города Ставрополя

Содержание

1. Общие положения.

Настоящим положением по организации работы с персональными данными в комитете городского хозяйства администрации города Ставрополя (далее – Положение) определяется порядок организации работы, связанной с получением, учетом, обработкой, накоплением и хранением информации, относящейся к персональным данным, содержащимся в информационных системах персональных данных (далее – ИСПДн) комитета городского хозяйства администрации города Ставрополя (далее – Комитет).

Настоящее Положение разработано в соответствии со следующими нормативными актами:

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2. Цели Положения.

Настоящее Положение направлено на достижение следующих целей:

- выполнение требований нормативных документов Российской Федерации, связанных с персональными данными;
- защита прав и свобод граждан Российской Федерации при обработке их персональных данных в информационных системах Комитета;
- защита персональных данных, обрабатываемых в Комитете от несанкционированного доступа и от других несанкционированных действий.

3. Ответственность и области применения.

Настоящее Положение обязаны знать и использовать в работе все сотрудники Комитета и сотрудники, участвующие в обработке персональных данных в ИСПДн Комитета.

4. Основные понятия и сокращения.

В настоящем Положении используются следующие основные понятия и сокращения:

ИСПДн – информационная система персональных данных.

ПДн – персональные данные.

Персональные данные – любая информация, касающаяся конкретного лица (в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация).

Обработка персональных данных, осуществляемая без использования средств автоматизации – обработка ПДн (а именно – использование, уточнение, распространение и уничтожение) содержащихся в информационной системе ПДн либо извлеченных из такой системы, осуществляемая при непосредственном участии человека.

Обработка персональных данных – действия (операции) с ПДн, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Структурное подразделение – официально выделенная в организационной структуре Комитета группа работников, выполняющая определенные функции и задачи в соответствии с положением об отделе.

Ответственный за применение нормативного документ – должностное лицо, ответственное за внедрение и применение нормативного документа. Термин применим к нормативным документам, кроме регламента процесса, для регламента процесса используется термин «Владелец процесса». Ответственный за применение нормативного документа и ответственный за разработку нормативного документа могут совпадать.

Ответственный за разработку нормативного документа – должностное лицо или структурное подразделение, ответственное за создание и поддержание нормативного документа в актуальном состоянии. Ответственный за разработку нормативного документа отвечает за плановый пересмотр документа.

5. Мероприятия по организации работы сотрудников с ПДн.

5.1. Принципы и требования по организации работы с ПДн распространяются на:

1) все возможные носители информации, такие как:

- бумажные носители;
- электронные носители;
- электрические сигналы в проводнике;
- акустические колебания и т.п.;

2) на все возможные форматы представления ПДн, такие как:

- документы;
- голос;
- файлы;
- почтовые сообщения;
- базы данных;

- записи базы данных;
- другие информационные массивы.

5.2. ПДн являются сведениями, отнесенными к информации ограниченного доступа Комитета, в соответствии с «Положением по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн» Комитета.

5.3. Настоящее Положение представляет правила обращения с ПДн при их обработке в ИСПДн. При этом рассматриваются такие операции, как:

- сбор;
- уточнение;
- использование;
- распространение;
- уничтожение.

5.4. При работе с ПДн, во всех случаях, не урегулированных нормативными документами Комитета, необходимо руководствоваться действующим законодательством Российской Федерации.

5.5. В Комитете должен быть определен перечень сотрудников, участвующих в обработке ПДн.

5.6. Все операции по обработке данной информации должны выполняться только сотрудниками, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях и допущенными к работе с ПДн приказом.

5.7. Основания и порядок допуска сотрудников Комитета и иных лиц к сведениям ограниченного доступа определен в «Положении по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн» Комитета.

5.8. Обязанности и ответственность сотрудников Комитета, участвующих в обработке ПДн определен в «Положении по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн» Комитета.

5.9. Необходимо проводить регулярное обучение сотрудников по вопросам, связанным с обеспечением безопасности процессов обработки ПДн.

5.10. При необходимости разрабатываются инструкции или регламенты процессов, описывающие особенности обработки ПДн в каждой ИСПДн.

5.11. Мероприятия и требования по обеспечению безопасности ПДн при их обработке определены в «Положении по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн» Комитета.

6. Характеристики ПДн.

6.1. Определяются основные характеристики ПДн, обрабатываемых в Комитете:

- цели обработки ПДн;
- круг субъектов, ПДн которых подлежат обработке для достижения целей;
- источники получения ПДн;
- состав ПДн необходимый для достижения целей;
- сроки хранения ПДн в Комитете;
- способы обработки ПДн;
- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой исключительно автоматизированная обработка его ПДн;

6.2. Обработка ПДн осуществляется в Комитете только с согласия субъектов ПДн.

6.3. Цели обработки ПДн должны соответствовать целям, заявленным при сборе ПДн.

6.4. Объем, состав и способы обработки ПДн должны соответствовать целям обработки ПДн.

6.5. Не допускается обработка ПДн, избыточных по отношению к целям обработки ПДн.

6.6. Не допускается объединение информационных массивов, созданных для несовместимых между собой целей обработки ПДн.

6.7. ПДн подлежат уничтожению по достижении целей их обработки.

6.8. В ИСПДн Комитета не допускается обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни без наличия согласия субъекта ПДн на обработку подобных ПДн.

7. Права субъектов ПДн.

7.1. Субъект ПДн имеет право:

7.1.1. На получение информации о наличии его ПДн в Комитете, и основных характеристик этих ПДн.

7.1.2. На свободный бесплатный доступ к своим ПДн, за исключением случаев, предусмотренных законодательством Российской Федерации.

7.1.3. Требовать об исключении или исправлении неверных или неполных ПДн, а также данных, не являющихся необходимыми для заявленной цели обработки ПДн.

7.1.4. Подавать возражение против решения, основанного исключительно на автоматизированной обработке его ПДн.

7.2. Субъектам ПДн запрещено отказываться от своих прав на сохранение и защиту тайны.

8. Предоставление ПДн.

8.1. При получении запроса от субъекта ПДн на получение информации о наличии и основных характеристиках его ПДн в Комитете, на ознакомление со своими ПДн, ответное уведомление или доступ к ПДн должен быть предоставлен в течении десяти рабочих дней со дня получения запроса.

8.2. При получении запроса от уполномоченного органа по защите прав субъектов ПДн на информацию, необходимую для осуществления деятельности указанного органа, Комитет обязан предоставить эту информацию в течение семи рабочих дней с даты получения такого запроса.

8.3. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке Комитета и в том объеме, который позволяет не разглашать ПДн о субъектах ПДн.

8.4. Запрос субъекта ПДн оформляется в письменном виде.

8.5. Уведомление субъекта ПДн, о наличии и основных характеристиках его ПДн в Комитете, оформляется в письменном виде.

9. Уточнение или уничтожение ПДн.

9.1. Уничтожение ПДн субъектов оператор обязан осуществлять в следующих случаях:

- выявление неправомерной обработки ПДн, в том числе по обращению субъекта ПДн или его представителя либо запросу уполномоченного органа по защите прав субъектов ПДн, если обеспечить правомерность обработки ПДн невозможно;
- требование субъекта ПДн, если его ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отзыв субъектом ПДн согласия на обработку его ПДн, если сохранение ПДн более не требуется для целей обработки ПДн;
- достижение цели обработки ПДн или утрата необходимости в достижении этих целей;
- истечения сроков хранения ПДн, установленных нормативно - правовыми актами Российской Федерации;

- признание недостоверности ПДн или получения их незаконным путем по требованию уполномоченного органа по защите прав субъектов ПДн;
- в иных, установленных законодательством случаях.

9.2. При получении запроса от субъекта ПДн на уточнение или уничтожение его ПДн, оператор уведомляет субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя, либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган об уничтожении ПДн.

9.3. Сотрудники Комитета, уполномоченные на получение, обработку, хранение, передачу и любое другое использование ПДн осуществляют:

- контроль наступления случаев, указанных в пункте 9.1 настоящего Положения;
- подготовку и представление экспертной комиссии по проведению мероприятий по защите ПДн, а также по контролю за соблюдением порядка обращения с документами, содержащими ПДн, в Комитете (далее - комиссия) пакета документов, содержащего ПДн, подлежащие уничтожению, с описью, на утилизацию.

9.4. Руководитель отдела Комитета, чьи документы, содержащие ПДн, подлежат уничтожению, осуществляет контроль обоснованности их уничтожения.

9.5. Решение об уничтожении ПДн принимается комиссией, утвержденной приказом Комитета «О создании комиссии по уничтожению ПДн».

9.6. В зависимости от типа носителя информации (бумажный или электронный) выделяются два способа уничтожения ПДн:

- физическое уничтожение носителя (уничтожение через шредерование, сжигание);
- уничтожение информации с носителя (многократная перезапись в секторах магнитного диска).

9.7. Уничтожение части ПДн, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

9.8. Уничтожение ПДн производится в срок, не превышающий трех рабочих дней с момента наступления случаев, указанных в пункте 9.1 настоящего Положения.

9.9. После уничтожения ПДн составляется Акт об уничтожении материальных носителей, содержащих ПДн (далее - Акт), по форме, утвержденной приказом Комитета.

9.10. Акт подписывается членами комиссии.

9.11. После подписания Акта в журнал учета уничтожения носителей ПДн (далее - журнал) вносится запись об их уничтожении. Форма журнала утверждается приказом Комитета.

10. Обработка ПДн.

10.1 В Комитете проводиться обработка персональных данных с использованием средств автоматизации и без использования средств автоматизации.

10.2 Особенности обработки ПДн, осуществляемой без использования средств автоматизации.

10.3. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, а также если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе ПДн и информации, не являющейся ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

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

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

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

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

10.6. При составлении типовых форм необходимо, чтобы каждый субъект ПДн, чьи ПДн указаны в документе, имел возможность ознакомиться со

своими персональными данными, содержащими в документе, не нарушая прав и законных интересов иных граждан.

Приложение 2
к приказу комитета городского
хозяйства администрации города
Ставрополя

от «13» 04 2020 г. № 50

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных комитета городского хозяйства города Ставрополя

Содержание

1. Условные обозначения и сокращения.

АРМ – Автоматизированное рабочее место.

ИБ – Информационная безопасность.

ИС – Информационная система.

ИСПДн – Информационная система персональных данных

ПДн – Персональные данные.

СЗПДн – Система защиты персональных данных.

СОИБ – Система обеспечения ИБ.

НСД – Несанкционированный доступ (действия).

2. Термины.

В настоящем Положении по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных комитета городского хозяйства города Ставрополя (далее – Положение) используются следующие термины:

Безопасность информации (данных) - состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Блокирование ПДн - временное прекращение сбора, систематизации, накопления, использования, распространения, ПДн, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления НСД и (или) воздействии на ПДн или ресурсы ИСПДн.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения ПДн, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки ПДн или в помещениях, в которых установлены ИСПДн.

Доступ к информации - возможность получения информации и ее использования.

Защита информации (далее – ЗИ) - деятельность, направленная на

предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИСПДн – ИС, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Конфиденциальность ПДн - обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в ИСПДн и (или) выходящей из ИС.

Модель угроз (безопасности информации) - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

НСД - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн.

Носитель защищаемой информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое

отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка ПДн - действия (операции) с ПДН, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку ПДн, а также определяющие цели и содержание обработки ПДн.

Технические средства ИСПДн - средства вычислительной техники, информационно - вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства ЗИ.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

ПДн - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение ИСПДн и(или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной ИС, осуществляемое с использованием вредоносных программ.

Ресурс ИС - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности ПДн - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных НД при их обработке в ИСПДн.

Уничтожение ПДн - действия, в результате которых невозможно восстановить содержание ПДн в ИСПДн или в результате которых уничтожаются материальные носители ПДн.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уполномоченное оператором лицо - лицо, которому на основании договора оператор поручает обработку ПДн.

Целостность информации - способность средства вычислительной техники или ИС обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Цель ЗИ - заранее намеченный результат ЗИ.

Результатом ЗИ является предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

3. Общие положения.

Настоящее Положение определяет порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн комитета городского хозяйства администрации города Ставрополя (далее - Комитет) и содержит общие принципы защиты ПДн.

Настоящее Положение разработано в соответствии со следующими

нормативными актами:

– Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

– Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Постановлением Правительства Российской Федерации от 15 сентября 2008 г № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– нормативными документами Федеральной службы безопасности России, Федеральной службы по техническому и экспортному контролю России (далее – ФСТЭК), Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Настоящее Положение направлено на достижение следующих целей:

– выполнение требований законодательства Российской Федерации, связанных с ПДн;

– защита прав и свобод граждан Российской Федерации при обработке их ПДн в ИСПДн Комитета;

– защита ПДн, обрабатываемых в Комитете, от НСД и от других НСД;

– снижение уровня регуляторных рисков в отношении Комитета.

Требования настоящего Положения распространяются на все отделы Комитета, которые участвуют в обработке ПДн, либо в организации обработки ПДн.

Настоящее Положение обязаны знать и использовать в работе все сотрудники Комитета.

Настоящее положение устанавливает требования по защите ПДн, принципы обработки ПДн в ИСПДн, направленные на защиту интересов Комитета в области его компетенции в соответствии с Положением о комитете городского хозяйства администрации города Ставрополя, утвержденного постановлением администрации города Ставрополя, от 11.05.2017 № 795. ПДн являются сведениями, отнесенными к информации ограниченного доступа Комитета.

Настоящее Положение является методологической основой для:

– формирования и проведения единой политики в области обеспечения безопасности ПДн;

– принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса

согласованных мер нормативно-правового, технического и организационно-технического характера, направленных на выявление, отражение и уменьшение угроз безопасности ПДн;

– координации деятельности отделов Комитета при проведении работ по созданию, развитию и эксплуатации ИСПДн с соблюдением требований по обеспечению безопасности ПДн;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн.

Принципы и требования по обеспечению безопасности ПДн распространяются:

1) на все возможные формы существования информации, такие как:

– физические поля (электрические, акустические, электромагнитные, оптические и т.п.);

– носители на бумажной, магнитной, оптической и иной основе.

2) на все возможные форматы представления ПДн, такие как:

– документы;

– голос;

– изображения;

– файлы;

– почтовые сообщения;

– базы данных;

– записи базы данных;

– другие информационные массивы.

Предотвращение несанкционированного и нелегитимного доступа к ИС, технологиям и информационным ресурсам результатом которого может стать уничтожение, модификация, искажение, копирование, распространение, блокирование ПДн требует применения комплекса правовых, организационных, организационно-технических мер защиты с использованием сертифицированных средств ЗИ.

Настоящее Положение определяет:

– роли, полномочия, ответственность за обеспечение безопасности ПДн отделов Комитета;

– порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн;

– мероприятия по обеспечению безопасности ПДн;

– требования по управлению процессом обеспечения безопасности ПДн;

– требования к составу и содержанию документов Комитета, регламентирующих защиту и работу с ПДн.

При работе с ПДн, во всех случаях, не урегулированных нормативными документами Комитета, необходимо руководствоваться действующим законодательством Российской Федерации.

4. Цели и задачи защиты ПДн.

Целью создания СЗПДн является исключение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий.

В общем случае можно выделить следующие основные цели защиты ПДн, это обеспечение:

– конфиденциальности ПДн;

– целостности ПДн;

– доступности ПДн;

– неотказуемости;

– учетности;

– аутентичности;

– адекватности.

Конкретный состав целей защиты ПДн зависит от конкретной ИСПДн и определяется по результатам разработки (актуализации) модели угроз и нарушителя безопасности ПДн.

К основным задачам в области обеспечения безопасности ПДн относится:

– определение новых ИСПДн;

– инвентаризация и управление изменениями в составе и структуре ИСПДн;

– сбор согласий на обработку ПДн с субъектов ПДн;

– разработка и актуализация перечня персональных данных, обрабатываемых в Комитете;

– контроль целей обработки ПДн, состава обрабатываемых ПДн целям обработки;

– уничтожение ПДн;

– оптимизация информационных и бизнес процессов обработки ПДн;

– управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;

– взаимодействие с субъектами ПДн по вопросам обработки их ПДн;

– классификация ИСПДн;

– разработка (актуализация) документации на СЗПДн;

– выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;

– сертификация применяемых средств ЗИ;

– эксплуатация системы защиты ПДн в соответствии с документацией на нее;

– контроль уровня защищенности ПДн;

– обучение персонала по вопросам защиты ПДн;

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

– учет лиц, допущенных к обработке ПДн;

– взаимодействие с регуляторными органами по вопросам защиты ПДн;

– актуализация и подача уведомлений в уполномоченный орган по защите прав субъектов ПДн;

– реагирование на нештатные ситуации, расследование нештатных ситуаций, возникающих при обработке ПДн.

5. Принципы обработки ПДн.

В соответствии с Федеральным законом № 152-ФЗ обработка ПДн осуществляется в соответствии со следующими принципами:

– законности целей и способов обработки ПДн и добросовестности;

– соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям оператора;

– соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

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

– недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн.

В Комитете проводится регулярный анализ соответствия процессов обработки ПДн указанным принципам. Данный анализ проводится в случае:

– создания новых ИСПДн;

– внесения изменений в технологические процессы существующие в ИСПДн;

– изменения нормативной базы затрагивающей принципы и (или) процессы обработки ПДн в ИСПДн Комитета;

– проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

6. Порядок отнесения сведений к персональным данным.

В соответствии с Федеральным законом № 152-ФЗ операторами и третьими лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных.

Отнесение сведений Комитета к соответствующим категориям информации представляет собой процесс обоснованного установления (документального оформления и утверждения руководителем Комитета) критериев их выделения из всей совокупности сведений, находящихся в обращении.

В качестве таких критериев в отношении ПДн в Комитете разработан и утвержден приказом комитета городского хозяйства администрации города Ставрополя от 17.10.2017 № 347, «Перечень персональных данных, обрабатываемых в комитете городского хозяйства города Ставрополя».

7. Организационная структура СЗПДн.

СЗПДн является частью общей системы обеспечения информационной безопасности Комитета.

Основу организационной структуры СЗПДн в Комитете составляют:

– руководство;

– отдел правого и кадрового обеспечения;

– общий отдел;

– ответственное лицо за защиту ПДн;

– администратор ИСПДн;

– отделы, участвующие в процессах обработки ПДн;

– сотрудники Комитета.

Руководитель Комитета осуществляет следующие основные функции в

области обеспечения безопасности ПДн:

– обеспечивает общую организацию работы по защите ПДн;

– издает приказы по вопросам организации СЗПДн;

– утверждает перечень ПДн, обрабатываемых в Комитете;

– назначает ответственное лицо за обеспечение безопасности ПДн;

– рассматривает и утверждает нормативные документы Комитета по защите ПДн;

– заслушивает при необходимости ответственных лиц за защиту ПДн и других должностных лиц о состоянии работ по защите ПДн.

Отдел правого и кадрового обеспечения осуществляет следующие основные функции:

– дает юридическую оценку возможности создания (модернизации) ИСПДн;

– проводит ознакомление сотрудников с нормативными документами в области защиты ПДн.

Ответственное лицо за защиту ПДн осуществляет следующие основные функции:

– разрабатывает перечень ПДн, обрабатываемых в Комитете (далее - Перечень ПДн);

– проводит классификацию ИСПДн (разрабатывает и утверждает акт классификации ИСПДн);

– распределяет ответственность по вопросам обработки и защиты ПДн;

– определяет допустимые сроки хранения ПДн по каждой категории ПДн;

– организует подачу уведомлений в уполномоченный орган по защите прав субъектов ПДн;

– заслушивает руководителей отделов Комитета о принимаемых мерах по состоянию и совершенствованию СЗПДн;

– организует работы по разработке, изменению и уточнению политик, регламентов, стандартов в части защиты ПДн;

– осуществляет организацию плановых и внеплановых проверочных мероприятий;

– организует выполнение требований по защите ПДн в Комитете;

– проводит разработку и актуализацию нормативных документов, регламентирующих защиту ПДн;

– разрабатывает и актуализирует Модели угроз безопасности ПДн;

– подготавливает проекты решений по изменению Перечня ПДн, обрабатываемых в Комитете, классификации ИСПДн, уведомления об обработке ПДн и других решений по обработке и обеспечению безопасности ПДн в Комитете;

– определяет необходимость обучения сотрудников по вопросам обеспечения безопасности ПДн, а также определяют формы и программы обучения сотрудников Комитета в области защиты ПДн;

– организует работы по сбору сведений об изменениях в составе и структуре ИСПДн;

– осуществляет контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов Российской Федерации по защите ПДн, а также внутренних организационно-распорядительных документов Комитета;

– контролирует исполнение требований по уничтожению ПДн;

– разрабатывает рекомендации по оптимизации существующих и новых информационных и бизнес-процессов обработки ПДн по критериям соответствия требованиям по защите ПДн и минимизации затрат на создание и эксплуатацию СЗПДн;

– контролирует исполнение требований нормативных документов Комитета в области обеспечения безопасности ПДн, отделами и сотрудниками Комитета;

– организует и осуществляет взаимодействие с регуляторами по вопросам защиты ПДн;

– осуществляет контроль лояльности администратора ИБ ИСПДн;

– проводит работы по классификации ИСПДн;

– управляет проектами по внедрению систем и средств защиты ПДн;

– контролирует ввод в действие, эксплуатацию СЗПДн;

– проводит расследования инцидентов, связанных с нарушением безопасности ПДн, правил обработки ПДн, принимают меры по недопущению повторения нештатных ситуаций.

Администратор ИБ ИСПДн осуществляют следующие основные функции:

– осуществляет сопровождение средств и СЗПДн;

– проводит оперативный контроль функционирования средств и СЗПДн;

– проводит резервирование ПДн;

– осуществляет выявление и регистрацию попыток НСД к компонентам ИСПДн, информационным ресурсам;

– контролирует соответствие технических, программных и программно-аппаратных средств ИСПДн требованиям, предъявляемым к ним средствами и СЗПДн;

– проводит оценку эффективности принятых мер и применяемых средств защиты ПДн;

– проводит занятия с сотрудниками по изучению организационно-распорядительных документов по всему комплексу вопросов защиты ПДн;

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

– контролирует выполнение сотрудниками Комитета требований по защите ПДн;

– участвует в расследованиях причин возникновения нештатных ситуаций;

– готовят предложения по совершенствованию СЗПДн;

– выполняют комплекс мероприятий по ЗИ при проведении ремонтных и регламентных работ;

– обеспечивают защиту ПДн при выводе из эксплуатации компонентов ИСПДн.

Отделы Комитета, участвующие в процессах обработки ПДн выполняют следующие основные функции:

– осуществляют взаимодействие с субъектами ПДн по вопросам обработки их ПДн;

– принимают меры по реализации перечня необходимых защитных мероприятий в процессе обработки ПДн субъектов.

Сотрудники Комитета выполняют следующие основные функции:

– соблюдают требования нормативных документов по защите ПДн;

– осуществляют обработку ПДн в соответствии с заданием и предоставленными полномочиями.

Для координации процесса обеспечения безопасности ПДн и решения задач требующих скоординированных действий разных отделов Комитета могут создаваться рабочие группы, в состав которых должны входить руководители всех заинтересованных отделов Комитета.

8. Порядок организации и проведения работ по обеспечению безопасности ПДн.

Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ выполняемых в рамках жизненного цикла ИСПДн.

Работы по обеспечению безопасности ПДн привязаны к жизненному циклу ИСПДн, а именно к следующим этапам:

1) Инициация проекта ИСПДн;

2) Планирование проекта ИСПДн;

3) Реализация проекта ИСПДн, в составе:

- выбор технического решения – концепция реализации;
- проектирование ИСПДн;
- производство ИСПДн;
- приемка ИСПДн;
- внедрение ИСПДн;
- передача системы в опытно-промышленную эксплуатацию;
- опытная эксплуатация;
- передача в промышленную эксплуатацию;
- завершение проекта;
- документирование проекта.

4) Эксплуатация ИСПДн;

5) Модернизация ИСПДн;

6) Вывод из эксплуатации.

Работы по защите ПДн с привязкой к этапам жизненного цикла ИСПДн приведены в таблице 1.

Таблица 1. Распределение работ по защите ПДн на стадии существования ИСПДн.

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
1.	Инициация проекта ИСПДн		
1.1.	определение ИСПДн	При создании ИС или существенном изменении существующей ИС определяется необходимость обработки ПДн. Если такая необходимость имеется, то система объявляется - ИСПДн	С автоматизированной обработкой С неавтоматизированной обработкой
1.2.	определение существенной информации об ИСПДн	На данном этапе производится: ▪ определение перечня ПДн, которые будут обрабатываться в ИСПДн; ▪ определение целей обработки ПДн,	С автоматизированной обработкой С неавтоматизированной обработкой

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
		действий выполняемых с ПДн, допустимых сроков хранения ПДн; • определение перечня типов технических средств, предполагаемые к использованию в ИСПДн, перечня системных и прикладных программных средств; • определение степени участия персонала в обработке ПДн, характер взаимодействия персонала между собой и с системой.	
1.3.	определение предварительной категории ПДн	Детализация проводимых работ приведена в разделе 9 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
1.4.	определение предварительного класса ИСПДн	Детализация проводимых работ приведена в разделе 9 Положения	С автоматизированной обработкой
1.5.	оценивается возможность оптимизации ИСПДн	Детализация проводимых работ приведена в разделе 10 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
1.6.	юридическая оценка возможности создания ИСПДн	На данном этапе производится юридическая оценка: • целей обработки ПДн; • операций, которые будут выполняться с ПДн; • наличия (возможности сбора) согласий на обработку ПДн, необходимости сбора согласий на обработку ПДн; • степени участия контрагентов Организации в обработке ПДн и необходимые юридические основания для такой обработки; • соответствия предполагаемых процессов обработки ПДн принципам их обработки в соответствии с разделом 5 Положения.	С автоматизированной обработкой С неавтоматизированной обработкой
1.7.	проведение оценки возможных затрат на создание СЗПДн по срокам и стоимости	Оцениваются возможные затраты на создание СЗПДн, которые должны учитываться при защите проекта и планировании проекта	С автоматизированной обработкой С неавтоматизированной обработкой
2.	Реализация проекта ИСПДн – концепция реализации ИСПДн/СЗПДн		
2.1.	определяется необходимость		С автоматизированной обработкой

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
	корректировки «Перечня ПДн», при необходимости проводится его корректировка		С неавтоматизированной обработкой
2.2.	построение модели информационных потоков персональных данных	Разработка модели информационных потоков должно производиться на основании соответствующего стандарта	С автоматизированной обработкой С неавтоматизированной обработкой
2.3.	определение перечня актуальных угроз безопасности ПДн в конкретных условиях функционирования (разработка модели угроз и нарушителя безопасности ПДн)	Детализация проводимых работ приведена в разделе 11 Положения	С автоматизированной обработкой
2.4.	определение категорий ПДн и класса ИСПДн	Детализация проводимых работ приведена в разделе 9 Положения	С автоматизированной обработкой
2.5.	определение необходимости создания СЗПДн	На данном этапе на основе класса ИСПДн определяется необходимость создания СЗПДн[1]	С автоматизированной обработкой
2.6.	разработка технического (специального технического) задания на разработку СЗПДн	На данном этапе определяются требования к техническим, программным, программно-аппаратным и организационным средствам и мерам обеспечения безопасности ПДн.	С автоматизированной обработкой
3.	Реализация проекта ИСПДн – проектирование ИСПДн		
3.1.	разработка эскизного проекта на СЗПДн	На данном этапе разрабатывается: • пояснительная записка; • схема структурная комплекса технических средств.	С автоматизированной обработкой
3.2.	проработка форм документов предполагающих включение в них ПДн	На данном этапе производится: • определение форм документов, в которых будут содержаться ПДн; • оценка соответствия форм требованиям, предъявляемым к ним нормативными документами РФ в области защиты ПДн; • производится корректировка форм.	С неавтоматизированной обработкой
3.3.	разработка эксплуатационной документации на ИСПДн	Производится разработка положений, регламентов, инструкций, определяющих частный порядок защиты ПДн в данной ИСПДн	С автоматизированной обработкой С неавтоматизированной обработкой

[1] Для ИСПДн 4 класса создание СЗПДн не обязательно (по решению руководства Комитета)

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
4.	Реализация проекта ИСПДн – производство ИСПДн		
4.1.	внедрение комплекса средств и мер защиты ПДн	Производятся монтажные, пуско-наладочные работы средств ЗИ. Производится реализация комплекса организационно-технических мероприятий по защите ПДн.	С автоматизированной обработкой
4.2.	реализация требований по физической защите компонентов ИСПДн и носителей ПДн	Производятся монтажные работы средств физической защиты (замков, шкафов, сейфов и т.п.)	С автоматизированной обработкой С неавтоматизированной обработкой
4.3.	заключаются договора с контрагентами, которые будут осуществлять обработку ПДн Организации, с учетом требований по защите ПДн (при необходимости)	На данном этапе определяются договора, в которые должны быть внесены изменения. В данные договора вносятся требования по обеспечению конфиденциальности ПДн контрагентами, которые будут иметь к ним доступ.	С автоматизированной обработкой С неавтоматизированной обработкой
4.4.	определение подразделений и назначение лиц, ответственных за эксплуатацию средств ЗИ		С автоматизированной обработкой С неавтоматизированной обработкой
5.	Реализация проекта ИСПДн – передача системы в опытно-промышленную эксплуатацию		
5.1.	проводится обучение сотрудников по направлению обеспечения безопасности ПДн	Детализация проводимых работ приведена в разделе 12 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
5.2.	проводится ознакомление сотрудников с нормативными документами в области защиты ПДн		С автоматизированной обработкой С неавтоматизированной обработкой
6.	Реализация проекта ИСПДн – опытная эксплуатация ИСПДн		
6.1.	начинает производиться сбор согласий на обработку ПДн с субъектов ПДн (в случае необходимости их сбора определенной в п. 1.6)		С автоматизированной обработкой С неавтоматизированной обработкой
6.2.	оценивается необходимость	На данном этапе производится: • определение необходимости	С автоматизированной обработкой

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
	изменения Уведомления об обработке ПДн	изменения Уведомления об обработке ПДн; • производится подготовка, согласование и отправка нового Уведомления об обработке ПДн в Уполномоченный орган по защите прав субъектов ПДн. Форма, состав Уведомления определяется в соответствии с нормативными документами Уполномоченного органа по защите прав субъектов ПДн	С неавтоматизированной обработкой
6.3.	проводится опытная эксплуатация средств ЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн		С автоматизированной обработкой
6.4.	разрабатывается программа и методика приемочных испытаний		С автоматизированной обработкой
6.5.	проводятся приемочные испытания СЗПДн	Приемочные испытания СЗПДн проводятся в соответствии с программой и методикой приемочных испытаний	С автоматизированной обработкой
7.	Реализация проекта ИСПДн – передача в промышленную эксплуатацию		
7.1.	проводится оценка соответствия ИСПДн требованиям по безопасности ПДн	В зависимости от класса ИСПДн проводится: • аттестация по требованиям безопасности информации для ИСПДн 1 и 2 классов; • декларирование соответствия для ИСПДн 3 класса.	С автоматизированной обработкой
8.	Эксплуатация ИСПДн		
8.1.	допуск персонала к обработке ПДн	Детализация проводимых работ приведена в разделе 13 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
8.2.	производится уничтожение ПДн	Детализация проводимых работ приведена в разделе 14 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
8.3.	производится работа с носителями ПДн	Детализация проводимых работ приведена в разделе 15 Положения	С автоматизированной обработкой

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
			С неавтоматизированной обработкой
8.4.	производится учет средств ЗИ, эксплуатационной документации к ним	Учет средств ЗИ, эксплуатационной документации производится администраторами ИСПДн, порядок учета должен быть регламентирован в соответствующем РП	С автоматизированной обработкой
8.5.	осуществляется контроль изменений в составе и структуре ИСПДн	Детализация проводимых работ приведена в разделе 15 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
8.6.	обеспечивается защита от несанкционированного физического доступа к элементам ИСПДн	Детализация проводимых работ приведена в разделе 16 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
8.7.	осуществляется резервирование ПДн	Детализация проводимых работ приведена в разделе 17 Положения	С автоматизированной обработкой
8.8.	осуществляется эксплуатация СЗПДн в соответствии с документацией на нее	Эксплуатация системы защиты осуществляется в соответствии с проектом, регламентами и стандартами. Состав СЗПДн и мероприятий по защите ПДн определяется дифференцированно для различных ИСПДн, в зависимости от результатов разработки Модели угроз и ТЗ (СТЗ) на СЗПДн	С автоматизированной обработкой
8.9.	осуществляется контроль за обеспечением необходимого уровня защищенности ПДн	Детализация проводимых работ приведена в разделе 18 Положения	С автоматизированной обработкой
8.10.	производится реагирование на нештатные ситуации	Детализация проводимых работ приведена в разделе 19 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
8.11.	производится контроль лояльности персонала	Детализация проводимых работ приведена в разделе 20 Положения	
8.12.	проводится обучение персонала правилам обеспечения безопасности ПДн	Детализация проводимых работ приведена в разделе 12 Положения	С автоматизированной обработкой
8.13.	осуществляется взаимодействие с субъектами ПДн по вопросам обработки их	Взаимодействие с субъектами ПДн производится в порядке, определенном законодательством РФ	С автоматизированной обработкой С неавтоматизированной обработкой

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
	ПДн		
8.14.	отслеживается необходимость получения лицензий ФСТЭК и ФСБ России	В рамках данного процесса производится отслеживание сроков действия имеющихся лицензий ФСТЭК и ФСБ России касающихся защиты ПДн. При необходимости производится инициация работ по повторному получению данных лицензий.	С автоматизированной обработкой С неавтоматизированной обработкой
8.15.	осуществляется взаимодействие с регуляторными органами по вопросам защиты ПДн		С автоматизированной обработкой С неавтоматизированной обработкой
9.	Модернизация ИСПДн		
9.1.	осуществляется управление изменениями в ИСПДн	Детализация проводимых работ приведена в разделе 15 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
9.2.	производится оценка существенности предполагаемой модернизации ИСПДн	Проводится анализ: ▪ Возможности изменения класса ИСПДн, актуальных угроз, требований к СЗПДн ▪ Необходимости корректировки документации на СЗПДн ▪ Необходимости проведения дополнительных мероприятий по защите ПДн	С автоматизированной обработкой С неавтоматизированной обработкой
9.3.	на основе оценки существенности модернизации, проводится необходимый объем мероприятий указанный в пунктах 1-7 данной таблицы		С автоматизированной обработкой С неавтоматизированной обработкой
10.	Вывод из эксплуатации ИСПДн		
10.1.	производится уничтожение ПДн	Детализация проводимых работ приведена в разделе 14 Положения	С автоматизированной обработкой С неавтоматизированной обработкой
10.2.	производится уведомление субъектов ПДн (а при необходимости и Уполномоченный орган по защите прав субъектов ПДн) об	Взаимодействие с субъектами ПДн производится в порядке, определенном законодательством Российской Федерации	С автоматизированной обработкой С неавтоматизированной обработкой

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
	уничтожении ПДн		

9. Категорирование ПДн и классификация ИСПДн.

Категорирование ПДн и классификация ИСПДн должны проводиться для ИСПДн с автоматизированной обработкой персональных данных.

Процесс категорирования ПДн и классификации ИСПДн является основой для определения требований к уровню защиты ПДн.

Все ИСПДн Комитета с автоматизированной обработкой относятся к категории специальных ИСПДн (ИСПДн для которых требуется обеспечить не только конфиденциальность ПДн).

Классификация ИСПДн и категорирование ПДн проводятся путем:

– приведения исходных характеристик, влияющих на класс и категорию ПДн;

– указания предположений, влияющих на категорию ПДн и классификацию ИСПДн;

– логического обоснования предполагаемого класса ИСПДн и категорий ПДн.

Исходные характеристики, предположения и обоснования, а также выводы о классе ИСПДн и категории ПДн приводятся в Модели угроз безопасности ПДн.

Модель угроз безопасности ПДн может быть разработана на несколько ИСПДн сразу или на какую-либо конкретную ИСПДн.

Оценка необходимости пересмотра класса ИСПДн должна осуществляться каждый раз, когда изменились характеристики, учитываемые при классификации ИСПДн.

Результатом классификации ИСПДн является акт классификации. Форма акта приведена в Приложении № 1 к настоящему Положению.

10. Оценка возможности оптимизации ИСПДн.

Оценка возможности оптимизации ИСПДн имеет своей целью такую реструктуризацию ИСПДн, выполнение требований по защите ПДн в которой может быть обеспечено с минимальным уровнем затрат на создание и эксплуатацию СЗПДн.

При проведении оптимизации ИСПДн должна оцениваться возможность:

– снижения категории обрабатываемых ПДн;

– обезличивания ПДн;

– придания ПДн статуса общедоступных;

– изменения структуры и состава технических и программных средств ИСПДн, технологических процессов обработки ПДн.

Снижение категории ПДн, в общем случае, позволяет снизить класс ИСПДн и, соответственно, уровень требований к ИСПДн.

Обезличивание и отнесение ПДн к общедоступным – это эффективный способ обеспечения их безопасности, так как для обезличенных и общедоступных ПДн не требуется обеспечение их конфиденциальности.

Отсутствие необходимости защиты конфиденциальности ПДн не снимает необходимости защиты других характеристик безопасности (целостности, доступности и т.п.).

Необходимость защиты других характеристик безопасности определяется посредством оценки возможности ущерба для субъектов ПДн при нарушении этих характеристик безопасности. При наличии такого ущерба, в отношении таких ИСПДн, должен применяться комплекс мероприятий по их защите в полном объеме, в соответствии с разделом 8 настоящего Положения.

Среди мероприятий по обезличиванию ПДн, можно выделить следующие:

– разделение ПДн, позволяющее идентифицировать субъекта ПДн и остальной информации по разным ИСПДн, базам или массивам данных;

– удаление ПДн, позволяющих идентифицировать субъекта ПДн, в технологических процессах, в которых не требуется однозначного определения физического лица.

Придание ПДн статуса общедоступных возможно в следующих случаях:

– при принятии соответствующего федерального закона, определяющего, что этот состав ПДн является общедоступным;

– при наличии возможности сбора согласий на общедоступность их ПДн с субъектов ПДн.

Изменение структуры и состава технических и программных средств ИСПДн, технологических процессов обработки ПДн может проводиться, в том числе, с целью:

– уменьшения количества компонентов ИСПДн, на которые потребуется установка средств защиты;

– изменения возможности, степени опасности угроз для ИСПДн и, соответственно, уменьшения перечня актуальных угроз;

– изменения требований к характеристикам средств ЗИ, в результате

которого возможно использование более оптимальных по стоимости средств.

11. Модель угроз и нарушителя безопасности ПДн.

СЗПДн внедряется для нейтрализации актуальных угроз безопасности ПДн.

Оценка актуальности угроз производится посредством разработки модели угроз безопасности ПДн (далее - Модель угроз) и модели нарушителя.

Методической базой для разработки Модели угроз и нарушителя безопасности ПДн является:

– базовая модель угроз безопасности ПДн при их обработке в ИСПДн. Утверждена ФСТЭК России 15 февраля 2008 года;

– методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн. Утверждена ФСТЭК России 14 февраля 2008 года;

– методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации, ФСБ России 31 марта 2015 г., № 149/7/2/6-432.

Результатом разработки Модели угроз и нарушителя безопасности ПДн должен являться:

– перечень актуальных угроз;

– вывод о классе ИСПДн;

– вывод о типе нарушителя, существующем в ИСПДн и требуемом классе средств криптографической ЗИ.

Модель угроз и нарушителя безопасности ПДн должна содержать:

– описание структуры и состава ИСПДн (состав обрабатываемых ПДн, состав технических средств и программного обеспечения, существующие процессы обработки ПДн, схему организации связи и т.п.);

– обоснование характеристик безопасности ПДн (конфиденциальность, целостность, доступность и т.п.), нарушение которых ведет к ущербу для субъектов ПДн;

– модель угроз (перечень угроз, оценку вероятностей угроз, показатели опасности угроз для ИСПДн, оценки возможностей реализации угроз, выводы об актуальности угроз);

– модель нарушителя (объекты атак, возможные типы нарушителей, предположения о возможностях нарушителей, предположения об ограничениях на эти возможности, предположения о каналах атак и средствах атак, выводы о типе нарушителя);

– модель угроз и нарушителя безопасности ПДн пересматривается каждый

раз, когда изменяются характеристики, влияющие на актуальность угроз, класс ИСПДн, тип нарушителя.

12. Обучение сотрудников комитета, участвующих в обработке ПДн.

Должно проводиться регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн.

В общем случае, для различных категорий сотрудников форматы обучения должны отличаться.

Определены следующие форматы обучения:

- полные курсы (длительностью 5 дней и более);
- кратковременные курсы (длительностью от 1 до 3 дней);
- внешние и внутренние семинары;
- конференции;
- инструктажи;
- учения.

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

- ответственного лица за защиту ПДн;
- администратора ИСПДн.

Для обучения сотрудников отделов Комитета, участвующих в процессах обработки ПДн, должны проводиться:

- внутренние семинары;
- инструктажи.

Внутренние семинары проводятся ответственным лицом за защиту ПДн, приглашенными специалистами, а также другими подготовленными лицами.

Обучение каждой категории сотрудников должно проводиться не реже одного раза в год.

Инструктажи проводятся в отношении отдельных лиц, по мере необходимости Администратором ИСПДн, ответственным лицом за защиту ПДн.

При необходимости должны разрабатываться инструкции, описывающие особенности обработки ПДн в каждой ИСПДн, для отдельных категорий сотрудников.

13. Допуск сотрудников комитета к обработке ПДн.

При допуске сотрудников, допущенных к обработке ПДн в ИСПДн Комитета необходимо руководствоваться приказом Комитета от 02.03.2020 № 26 «О внесении изменений в приказ комитета городского хозяйства администрации города Ставрополя от 29.09.2015 № 297 «О допуске сотрудников комитета городского хозяйства администрации города Ставрополя к обработке персональных данных».

Список сотрудников Комитета, допущенных к обработке ПДн в ИСПДн составляется и ведётся Администратором ИСПДн совместно с сотрудниками отдела правового и кадрового обеспечения Комитета.

14. Уничтожение ПДн.

В соответствии с законодательством Российской Федерации ПДн должны быть уничтожены:

– по требованию субъекта ПДн, в определенных законом случаях;

– при истечении срока хранения;

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

– в случае достижения цели обработки ПДн;

– в случае утраты необходимости достижения цели обработки.

Контроль сроков хранения, целей обработки ПДн производится на основании допустимых сроков хранения и допустимых целей, указанных для конкретных категорий ПДн в «Перечне персональных данных, обрабатываемых в комитете городского хозяйства администрации города Ставрополя в связи с реализацией служебных и трудовых отношений, а также в связи с предоставлением муниципальных услуг и осуществлением муниципальных функций».

Уничтожение ПДн осуществляется в Комитете в соответствии с пунктом 9 «Положения по организации работы с персональными данными в комитете городского хозяйства администрации города Ставрополя».

15. Контроль изменений в составе и структуре ИСПДн.

Все изменения в составе и структуре ИСПДн контролируются лицом, ответственным за защиту ПДн в Комитете.

Контролю подлежат следующие изменения:

– внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);

– изменение мест включения существующих компонент ИСПДн;

– удаление устройства из состава ИСПДн;

– изменение мест установки устройства из состава ИСПДн;

– прокладка новых кабельных линий связи СКС и внешних линий связи или удаление старых кабельных линий связи;

– существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке ПДн;

– создание новых и изменение существующих технологических процессов, связанных с обработкой ПДн.

Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн отслеживается и анализируется на предмет соответствия требованиям по защите ИСПДн. При необходимости должна производиться модернизация СЗПДн.

16. Защита от несанкционированного физического доступа к элементам ИСПДн.

Мероприятия по физическому контролю доступа включают:

– мероприятия по контролю доступа в помещения с оборудованием ИСПДн;

– мероприятия по контролю доступа к техническим средствам ИС;

– мероприятия по контролю перемещений физических компонентов ИСПДн.

Мероприятия по контролю доступа на территорию Комитета должны обеспечить контролируемое нахождение посетителей на территории Комитета.

Двери помещений, в которых размещаются сервера и АРМ пользователей ИСПДн, должны быть оборудованы замками, либо в этих помещениях должны обеспечиваться мероприятия по контролю действий находящихся в них посторонних лиц.

Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн, должно производиться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

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

При выносе устройств, хранящих ПДн, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное удаление информации хранимой на этих устройствах с предварительным копированием её на другие носители.

17. Резервирование ПДн.

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

В регламенте процесса резервирования должны быть учтены следующие вопросы:

- порядок резервирования;
- ответственные лица за резервирование;
- порядок восстановления информации после аварий;
- порядок хранения резервных копий.

Резервированию должна подвергаться информация на серверах ИСПДн.

Доступ к резервным копиям предоставлен Администратору ИСПДн или лицу временно его замещающему.

Резервирование должно осуществляться в соответствии с «Регламентом резервного копирования».

18. Контроль за обеспечением необходимого уровня защищенности ПДн.

Для обеспечения эффективности процесса обеспечения безопасности ПДн проводится:

- контроль за соблюдением требований по обработке и защите ПДн;
- контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
- контроль эффективности средств защиты ПДн.

Контрольные мероприятия могут быть:

- текущими;
- внезапными;
- плановыми внешними;
- плановыми внутренними.

Ответственность за текущий контроль эффективности обеспечения безопасности ПДн возлагается на Администраторов ИСПДн.

При проведении контроля эффективности в общем случае должно проверяться:

- наличие установленных средств ЗИ;
- корректность настроек средств ЗИ;

– выполнение пользователями и администратором требований инструктивных материалов по защите ПДн;

– исполнение требований к процедурам обработки ПДн (уничтожению ПДн, сбору согласий, допуску персонала к ПДн и т.п.);

– соответствие СЗПДн реальному положению дел в Комитете и т.п.

19. Реагирование на нештатные ситуации.

Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн, в Комитете регламентированы следующие вопросы:

– порядок определения нештатной ситуации;

– порядок оповещения сотрудников при возникновении различных нештатных ситуаций;

– порядок действий по нейтрализации нештатных ситуаций, сведения их негативных последствий к минимуму.

В Комитете проводятся расследования инцидентов, связанных с НСД доступом и другими несанкционированными действиями.

В рамках данного процесса решаются следующие задачи:

– расследование инцидентов, связанных с безопасностью ПДн;

– ликвидация последствий инцидентов связанных с безопасностью ПДн;

– принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

Реагирование на нештатные ситуации производится в соответствии с «Инструкцией по действиям персонала в нештатных ситуациях».

20. Контроль лояльности сотрудников.

В Комитете проводится комплекс мероприятий, направленных на исключение присутствия злоумышленников среди сотрудников Комитета.

Комплекс мероприятий включает, в том числе:

– проверки работников при приеме в Комитет;

– периодический мониторинг действий персонала.

Мероприятия по обеспечению безопасности персонала должны обеспечить невозможность злоумышленного сговора двух или более сотрудников Комитета.

При приеме на работу должны проводиться проверки идентичности личности, точности и полноты биографических фактов и заявляемой квалификации.

Приложение № 1 – Форма акта
классификации информационных систем
персональных данных

УТВЕРЖДАЮ

Заместитель главы администрации
города Ставрополя, руководитель
комитета городского хозяйства
администрации города Ставрополя

«____»_____20___ г.

АКТ
классификации информационных систем персональных данных
комитета городского хозяйства администрации города Ставрополя

В соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к обработке персональных данных при их обработке в информационных системах персональных данных» и приказом руководителя комитета городского хозяйства администрации города Ставрополя от «___»_____20__г. № ___ комиссия в составе:

председатель комиссии: _____

члены комиссии:_____

произвела сбор данных об информационной системе персональных данных и установила нижеследующее:

1) в информационной системе персональных данных (далее - ИСПДн) обрабатываются персональные данные (*категория персональных данных*);
2) в ИСПДн одновременно обрабатываются персональные данные менее чем _____ субъектов персональных данных (*объём обрабатываемых персональных данных*);
3) по структуре ИСПДн относится к локальной информационной системе состоящей из_____(*структура информационной системы*);
4) *наличие подключения к сетям и системам общего пользования, к сети Интернет;*
5) по режиму обработки персональных данных в информационной системе ИСПДн относится к _____(*однопользовательская или многопользовательская*);
6) в зависимости от местонахождения технических средств ИСПДн относится к системам, технические средства которых размещены в Российской Федерации (*адрес, № кабинета*);
7) речевая обработка сведений составляющих ПДн в информационной системе (*осуществляется или нет*);

8) условие обработки персональных – для информационной системы актуальны угрозы ____типа и информационная система обрабатывает (категория персональных данных) _____ (количество) субъектов.

В соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к обработке персональных данных при их обработке в информационных системах персональных данных», на основании анализа исходных данных информационной системе персональных данных _____ (*название ИСПДн*) присвоить уровень защищенности ____ (___).

Председатель: _____
Члены комиссии:

_____
_____