

Содержание

[1. Условные обозначения и сокращения 3](#_Toc270948443)

[2. Термины 3](#_Toc270948444)

[3. Общие положения 7](#_Toc270948445)

[4. Цели и задачи защиты ПДн 9](#_Toc270948446)

[5. Принципы обработки ПДн 9](#_Toc270948447)

[6. Порядок отнесения сведений к персональным данным 10](#_Toc270948448)

[7. Организационная структура сз ПДн 11](#_Toc270948449)

[10. Обучение персонала, участвующего в обработке ПДн 13](#_Toc270948454)

[11. Допуск персонала к обработке ПДн 14](#_Toc270948455)

[12. Уничтожение ПДн 14](#_Toc270948456)

[13. Организация работы с носителями ПДн 14](#_Toc270948457)

[14. Контроль изменений в составе и структуре ИСПДн 15](#_Toc270948458)

[15. Защита от несанкционированного физического доступа к элементам ИСПДн……………. 16](#_Toc270948459)

[16. Резервирование ПДн 16](#_Toc270948460)

[17. Контроль за обеспечением необходимого уровня защищенности ПДн 17](#_Toc270948461)

[18. Реагирование на нештатные ситуации 18](#_Toc270948462)

[20. История версий документа 19](#_Toc270948467)

[Приложение № 1 Форма акта классификации ИСПДн ….20](#_Toc270948468)

Приложение № 2 Исходные данные классификации ИСПДн

# 1.Условные обозначения и сокращения

|  |  |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| ИБ | Информационная безопасность |
| ИС | Информационная система |
| ИСПДн | Информационная система персональных данных |
| ЛВС | Локальная вычислительная сеть |
| ПДн | Персональные данные |
| СЗПДн | Система защиты персональных данных |
| СКС | Структурированная кабельная система |
| СОИБ | Система обеспечения информационной безопасности |
| СТЗ | Специальное техническое задание |
| ТЗ | Техническое задание |
| НСД | Несанкционированный доступ |

1. Термины

1.1. В настоящем Положении используются следующие термины:

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

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

1.1.3. 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.

1.1.4. Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействии на персональные данные или ресурсы информационной системы персональных данных.

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

1.1.6. Доступ к информации - возможность получения информации и ее использования.

1.1.7. Защита информации (далее – ЗИ) - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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

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

1.1.10. Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

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

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

1.1.13. Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

1.1.15. Не декларированные 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.

1.1.16. Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

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

1.1.19. Технические средства информационной системы персональных данных - 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 защиты информации.

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

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

1.1.22. 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.

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

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

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

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

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

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

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

1.1.30. Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

1.1.31. Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

1.1.33. Уполномоченное оператором лицо - лицо, которому на основании договора оператор поручает обработку персональных данных.

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

1.1.35. Автоматизированная обработка ИСПДн – обработка персональных данных с помощью средств вычислительной техники.

1.1.36. Неавтоматизированная обработка ИСПДн – обработка персональных данных на бумажных носителях.

1.1.37. Цель защиты информации - заранее намеченный результат защиты информации.

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

2. Общие положения

2.1. Настоящее Положение определяет порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) комитета муниципального заказа и торговли администрации города Ставрополя (далее - комитет) и содержит общие принципы защиты персональных данных (ПДн).

2.2. Настоящее Положение разработано в соответствии со следующими нормативными актами:

2.2.1. Федеральным законом Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

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

2.2.3. Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

2.2.4. Совместным приказом от 13 февраля 2008 года ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи России № 20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;

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

2.2.6. Нормативными документами ФСБ России, ФСТЭК России, Роскомнадзора.

2.3. Настоящее Положение направлено на достижение следующих целей:

2.3.1. Выполнение требований законодательства Российской Федерации, связанных с персональными данными;

2.3.2. Защита прав и свобод граждан Российской Федерации при обработке их персональных данных в информационных системах персональных данных комитета;

2.3.3. Защита персональных данных, обрабатываемых в комитете, от несанкционированного доступа и от других несанкционированных действий;

2.3.4. Снижение уровня регуляторных рисков в отношении комитета;

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

2.5. Настоящее Положение обязаны знать и использовать в работе все сотрудники комитета.

2.6. Настоящее положение устанавливает требования по защите персональных данных, принципы обработки персональных данных в информационных системах персональных данных.

2.8. Персональные данные являются сведениями, отнесенными к информации ограниченного доступа комитета.

2.9. Настоящее Положение является методологической основой для:

2.9.1. Формирования и проведения единой политики в области обеспечения безопасности персональных данных;

2.9.2. Принятия управленческих решений и разработки практических мер по воплощению политики безопасности персональных данных и выработки комплекса согласованных мер нормативно-правового, технического и организационно-технического характера, направленных на выявление, отражение и уменьшение угроз безопасности ПДн.

2.10. Принципы и требования по обеспечению безопасности персональных данных распространяются на:

2.10.1. Носители на бумажной, магнитной, оптической и иной основе.

2.10.2 . На все возможные форматы представления персональных данных, такие как:

2.10.2.1. документы;

2.10.2.2. файлы;

2.10.2.3. почтовые сообщения;

2.10.2.4. базы данных;

2.10.2.5. записи базы данных;

2.11. Предотвращение несанкционированного и нелегитимного доступа к информационным системам, 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 защиты информации.

2.12. Настоящее Положение определяет:

2.12.1. Роли, полномочия, ответственность за обеспечение безопасности ПДн комитета;

2.12.2. Порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн;

2.12.3. Мероприятия по обеспечению безопасности ПДн;

2.12.4. Требования по управлению процессом обеспечения безопасности ПДн;

2.12.5. Требования к составу и содержанию документов Комитета, регламентирующих защиту и работу с ПДн.

2.13. При работе с персональными данными, во всех случаях, не урегулированных нормативными правовыми актами комитета, необходимо руководствоваться действующим законодательством Российской Федерации.

3. Цели и задачи защиты ПДн

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

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

3.2.1. Конфиденциальности ПДн;

3.2.2. Целостности ПДн;

3.2.3. Доступности ПДн;

3.2.4. Учетности;

3.2.5. Аутентичности;

3.2.6. Адекватности.

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

3.4. К основным задачам в области обеспечения безопасности ПДн относится:

3.4.1. Определение новых ИСПДн;

3.4.2. Инвентаризация и управление изменениями в составе и структуре ИСПДн;

3.4.3. Сбор согласий на обработку ПДн с субъектов ПДн;

3.4.4. Контроль целей обработки ПДн, состава обрабатываемых ПДн целям обработки;

3.4.5. Уничтожение ПДн;

3.4.6. Взаимодействие с субъектами ПДн по вопросам обработки их ПДн;

3.4.7. Классификация ИСПДн;

3.4.8. Эксплуатация системы защиты ПДн в соответствии с документацией на нее;

3.4.9. Контроль уровня защищенности ПДн;

3.4.10. Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

3.4.11. Учет лиц, допущенных к обработке ПДн;

4. Принципы обработки ПДн

4.1. В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» обработка ПДн должна осуществляться в соответствии со следующими принципами:

4.1.1. Законности целей и способов обработки персональных данных и добросовестности;

4.1.2. Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

4.1.3. Соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4.1.4. Достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

4.1.5. Недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

4.2. В комитете должен проводиться регулярный анализ соответствия процессов обработки ПДн указанным принципам. Данный анализ проводится в случае:

4.2.1. Создания новых ИСПДн;

4.2.2. Внесения изменений в технологические процессы существующие в ИСПДн;

4.2.3. Изменения нормативной базы затрагивающей принципы и(или) процессы обработки ПДн в ИСПДн комитете;

4.2.4. Проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

5. Порядок отнесения сведений к персональным данным

5.1. В соответствии с Федеральным законом от 27 июля 2006 г № 152-ФЗ «О персональных данных» операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

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

5.3. В качестве таких критериев в отношении персональных данных в комитете разрабатывается и утверждается «Перечень персональных данных, обрабатываемых в комитете муниципального заказа и торговли администрации города Ставрополя.

5.4. Перечень персональных данных, обрабатываемых в комитете муниципального заказа и торговли администрации города Ставрополя» утверждается руководителем комитета муниципального заказа и торговли администрации города Ставрополя.

6. Организационная структура сз ПДн

6.1. Система защиты ПДн является частью общей Системы обеспечения информационной безопасности комитета.

6.2. Основу организационной структуры СЗПДн составляют следующие организационные структуры комитета:

6.2.1 Руководство;

6.2.2. Юридический отдел;

6.2.3. Общий отдел;

6.2.4. Отдел бухгалтерского учета и отчетности;

6.2.5. Ответственное лицо за защиту ПДн;

6.2.6. Администратор ИСПДн;

6.2.7. Сотрудники комитета.

6.3. Руководство комитета осуществляет следующие основные функции в области обеспечения безопасности ПДн:

6.3.1. Обеспечивает общую организацию работы по защите ПДн;

издает приказы по вопросам организации СЗПДн;

6.3.2. Утверждает «Перечень персональных данных, обрабатываемых в комитете муниципального заказа и торговли администрации города Ставрополя»;

6.3.3. Назначает ответственное лицо за обеспечение безопасности ПДн;

6.3.4. Утверждает Декларацию о соответствии ИСПДн требованиям по защите ПДн;

6.4.5. Рассматривает и утверждает нормативные документы комитета по защите ПДн;

6.5. Юридический отдел осуществляет следующие основные функции:

6.5.1. Дает юридическую оценку нормативным документам в области защиты ПДн;

6.6. Общий отдел осуществляет следующие основные функции:

6.6.1. Проводит ознакомление сотрудников с нормативными документами в области защиты ПДн.

6.7. Администратор ПДн осуществляют следующие основные функции:

6.7.1. Разрабатывает «Перечень ПДн, обрабатываемых в комитете муниципального заказа и торговли администрации города Ставрополя» (далее Перечень ПДн);

6.7.2. Распределяет ответственность по вопросам обработки и защиты ПДн;

6.7.3. Определяет допустимые сроки хранения ПДн по каждой категории ПДн;

6.7.4. Осуществляет организацию плановых и внеплановых проверочных мероприятий;

6.7.5. Организует выполнение требований по защите ПДн в комитете;

6.7.6. Определяет необходимость обучения сотрудников по вопросам обеспечения безопасности ПДн, а также определяют формы и программы обучения сотрудников комитете в области защиты ПДн;

6.7.7. Организовывает работы по сбору сведений об изменениях в составе и структуре ИСПДн;

6.7.8. Осуществляет контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов Российской Федерации по защите ПДн, а также внутренних организационно-распорядительных документов комитета;

6.7.9. Контролирует исполнение требований по уничтожению ПДн;

6.7.10. Контролирует исполнение требований нормативных документов комитета в области обеспечения безопасности ПДн сотрудниками комитета;

6.7.11. Контролирует ввод в действие, эксплуатацию СЗПДн;

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

6.8. Администратор ИБ ИСПДн осуществляют следующие основные функции:

6.8.1. Осуществляет сопровождение средств и систем защиты ПДн;

6.8.2. Проводит оперативный контроль функционирования средств и систем защиты ПДн;

6.8.3. Проводит резервирование ПДн;

6.8.4. Контролирует выполнение сотрудниками подразделения требований по защите ПДн;

6.8.5. Участвует в расследованиях причин возникновения критических (нештатных) ситуаций;

6.8.6. Выполняет комплекс мероприятий по защите информации при проведении ремонтных и регламентных работ;

6.8.7. Обеспечивает защиту ПДн при выводе из эксплуатации компонентов ИСПДн.

6.9. Конкретное распределение функций Администратора ИБ ИСПДн должно быть приведено в эксплуатационной документации информационных систем.

6.10. Владельцы ИСПДн осуществляют следующие основные функции:

6.10.1 . Осуществляют контроль и учет проведения изменений в ИСПДн, согласуют проводимые изменения с ответственным лицом за защиту ПДн;

6.10.2. Организуют и проводят уничтожение ПДн;

6.10.3. Составляют и актуализируют списки должностных лиц, имеющих доступ к ПДн;

6.10.4. Обеспечивают выполнение требований по защите ПДн, обрабатываемых неавтоматизированным способом;

6.10.5. Проводят согласование форм договоров, анкет, журналов и других документов, предназначенных для включения в них ПДн, с ответственным лицом за защиту ПДн;

6.10.6. Осуществляют взаимодействие с субъектами ПДн, данные которых обрабатываются в их зоне ответственности, по вопросам обработки их ПДн;

7. Обучение персонала, участвующего в обработке ПДн

7.1. Проводится Администратором ИСПДн при участии сотрудников комитета информационных технологий бесплатное регулярное обучение сотрудников по вопросам, связанным с обеспечением безопасности ПДн.

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

7.3. Определены следующие форматы обучения:

7.3.1. Полные курсы (длительностью 5 дней и более);

7.3.2. Кратковременные курсы (длительностью от 1 до 3 дней);

внешние и внутренние семинары;

7.3.3. Конференции;

7.3.4. Инструктажи;

7.3.5. Учения.

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

7.4.1. Администраторов ИСПДн.

7.5. Для руководителей отделов, участвующих в процессах обработки ПДн, могут проводиться кратковременные курсы во внешних специализированных организациях.

7.6. Для обучения остальных категорий персонала, участвующих в процессах обработки ПДн, должны проводиться:

7.6.1. Внутренние семинары;

7.6.2. Инструктажи.

7.7. Внутренние семинары проводятся ответственными лицами за защиту ПДн, приглашенными специалистами, а также другими подготовленными лицами. На всех семинарах следует использовать презентации.

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

7.9. Инструктажи проводятся в отношении отдельных лиц, по мере необходимости Администратором ИСПДн. Учения проводятся для закрепления практических навыков реагирования на возникающие угрозы и могут проводиться как для отдельных отделов, так и для комитета в целом.

7.10. Учения проводятся не реже одного раза в год.

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

7.12. Для проведения семинаров создаются учебные группы по комитету. Состав группы не должен превышать 20-25 человек.

7.13. Инструкторы учебных групп должны в первый год, а в дальнейшем не реже 1 раза в 3 года проходить подготовку в специализированных учебно-методических центрах по вопросам защиты ПДн.

8. Допуск персонала к обработке ПДн

8.1 При допуске к ПДн необходимо руководствоваться приказом руководителя комитета муниципального заказа администрации города Ставрополя от 26.06.2013 № 69 «О допуске сотрудников к обработке персональных данных в комитете муниципального заказа и торговли администрации города Ставрополя».

8.2. Форма «Перечня должностных лиц, имеющих доступ к персональным данным» представлена в Приложении.

8.3. Перечни должностных лиц составляются и ведутся владельцами ИСПДн и процессов обработки ПДн, на основании данных о должностных лицах, допущенных к ПДн, подаваемых руководителями отделов комитета.

9. Уничтожение ПДн

9.1. В соответствии с законодательством РФ ПДн должны быть уничтожены:

9.1.1. При истечении срока хранения;

9.1.2. В случае выявления неправомерных действий с персональными данными и невозможности устранения допущенных нарушений;

9.1.3. В случае достижения цели обработки ПДн;

9.1.4. В случае утраты необходимости достижения цели обработки.

9.2. 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 муниципального заказа и торговли администрации города Ставрополя».

9.3. Решение об уничтожении ПДн, организацию и проведение уничтожения принимает и осуществляет Администратор ИСПДн..

9.4. Порядок уничтожения ПДн должен быть регламентирован в «Положении о работе с ПДн».

10. Организация работы с носителями ПДн

10.1. Порядок организации документооборота связанного с ПДн в комитете соответствует единому порядку организации конфиденциального делопроизводства.

10.2. Для этого должны быть упорядочены и регламентированы следующие работы, связанные с ПДн:

10.2.1.Оформление носителей, содержащих персональные данные;

10.2.2. Учет носителей, содержащих персональные данные;

10.2.3. Обращение с носителями, содержащими персональные данные;

10.2.4. Систематизация носителей, содержащих персональные данные;

10.2.5. Хранение носителей, содержащих персональные данные;

подготовка носителей, содержащих персональные данные для передачи их в архив;

10.2.6. Подготовка носителей, содержащих персональные данные для их уничтожения;

10.2.7. Проверка наличия носителей, содержащих персональные данные;

10.2.8. Распечатка ПДн.

10.3. Работы с ПДн регламентируются в виде документов на следующих носителях:

10.3.1. Бумажных носителях;

10.3.2. Электронных съемных носителях;

10.3.3. Электронных несъемных носителях, используемых в технических средствах ИСПДн.

11. Контроль изменений в составе и структуре ИСПДн

11.1. Все изменения в составе и структуре ИСПДн должны контролироваться и регламентироваться лицом ответственным за защиту ПДн в комитете.

11.2. Контролю подлежат следующие изменения:

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

11.2.2. Изменение мест включения существующих компонент ИСПДн;

11.2.3. Удаление устройства из состава ИСПДн;

11.2.4. Изменение мест установки устройства из состава ИСПДн;

11.2.5. Прокладка новых кабельных линий связи СКС и внешних линий связи или удаление старых кабельных линий связи;

11.2.6. Существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке ПДн;

11.2.7.Создание новых и изменение существующих технологических процессов, связанных с обработкой ПДн.

11.3. Все запросы на изменения стандартизированы и выполняются в соответствии с разработанными формальными процедурами. Результаты всех изменений должны оцениваться и документироваться.

11.4. Применяются процедуры гарантирующие, что все потенциальные изменения оцениваются с точки зрения возможных негативных последствий на эксплуатацию системы и ее функциональность.

11.5. Устанавливаются процедуры, определяющие необходимость проведения экстренных изменений и процедуры контроля этих изменений.

11.6. 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.

12. Защита от несанкционированного физического доступа к элементам ИСПДн

12.1. Мероприятия по физическому контролю доступа включают:

мероприятия по контролю доступа на территорию комитета;

12.1.1.Мероприятия по контролю доступа в помещения с оборудованием ИСПДн;

12.1.2.Мероприятия по контролю доступа к техническим средствам ИС;

12.1.3.Мероприятия по контролю перемещений физических компонентов ИСПДн.

12.1.4.Мероприятия по контролю доступа на территорию комитета обеспечивают контролируемое нахождение посетителей на территории комитета.

12.2. Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн, а также помещения в которых размещаются АРМ пользователей оборудованы замками.

12.3. Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие сотрудники), производится только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

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

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

13. Резервирование ПДн

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

13.2. В регламенте процесса резервирования учитываются следующие вопросы:

13.2.1. Порядок резервирования;

13.2.2. Ответственные лица за резервирование;

13.2.3. Порядок восстановления информации после аварий;

13.2.4. Порядок хранения резервных копий.

13.3. Резервированию подвергается информация на серверах ИСПДн.

13.4. Резервирование осуществляется на магнитные ленты или другие носители информации с соответствующим уровнем надежности и долговечности.

13.5. Хранение резервных копий осуществляется в надежных сейфах (металлических шкафах). Хранение (по возможности) осуществляется в месте, территориально удаленном от основного хранилища информации.

13.6. Доступ к резервным копиям строго регламентирован.

14. Контроль за обеспечением необходимого уровня защищенности ПДн

14.1. Для обеспечения эффективности процесса обеспечения безопасности ПДн проводится:

14.1.1. Контроль за соблюдением требований по обработке и защите ПДн;

14.1.2. Контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;

14.1.3. Контроль эффективности средств защиты ПДн.

14.2. Контрольные мероприятия могут быть:

14.2.1. Текущими;

14.2.2. Внеплановыми;

14.2.3. Плановыми внешними;

14.2.4. Плановыми внутренними.

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

14.4. Ответственность за плановый контроль эффективности обеспечения безопасности ПДн возлагается на ответственного за защиту ПДн.

14.5. Данные проверки должны включаться в план аудитов информационной безопасности на год.

14.6. Для планового контроля эффективности СЗПДн должны использоваться средства выявления уязвимостей информационной безопасности.

14.7. Внезапные проверки эффективности при необходимости могут проводиться специальными группами по решению ответственных лиц за защиту ПДн.

14.8. При проведении контроля эффективности в общем случае должно проверяться:

14.8.1. Наличие установленных средств защиты информации;

14.8.2. Корректность настроек средств защиты информации;

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

14.8.4. Правильность организации работы с носителями ПДн;

правильность обращения ключевой информации;

14.8.5. Соответствие системы защиты ПДн реальному положению дел в комитете и т.п.

15. Реагирование на нештатные ситуации

15.1. Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн, в комитете регламентируются следующие вопросы:

15.1.1. Порядок определения нештатной ситуации;

15.1.2. Порядок оповещения сотрудников при возникновении различных нештатных ситуаций;

15.1.3. Порядок действий по нейтрализации нештатных ситуаций, сведения их негативных последствий к минимуму.

15.2. Разработанные порядки действий в нештатных ситуациях регулярно (не реже 1-2 раз в год) проверяются посредством проведения учений с корректировкой порядков по результатам проведенных проверок.

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

15.4. В рамках данного процесса должны решаться следующие задачи:

15.4.1. Расследование инцидентов, связанных с безопасностью ПДн;

15.4.2. Ликвидация последствий инцидентов связанных с безопасностью ПДн;

принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

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

# История версий документа

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Дата создания версии | Должность ответственного за разработку | ФИО ответственного лица за разработку | Краткое описание изменений документа |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Приложение № 1 Форма акта классификации ИСПДн

|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДАЮ |
|  |  | Руководитель комитета муниципального заказа и торговли администрации города Ставрополя |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Ломанов |
|  |  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г. |

АКТ

классификации информационных систем персональных данных комитета муниципального заказа и торговли администрации города Ставрополя

Комиссия в составе:

Председатель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии:

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

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

рассмотрев исходные данные на следующие информационные системы персональных данных:

* Наименование ИСПДн 1,
* Наименование ИСПДн 2,

условия их эксплуатации, с учетом характера обрабатываемой информации (Приложение № 1), в соответствии с требованиями совместного приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»,

РЕШИЛА:

установить следующие классы информационным системам персональных данных администрации города Ставрополя:

|  |  |
| --- | --- |
| Наименование ИСПДн | Установленный класс |
|  |  |
|  |  |

Председатель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии:

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

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

Приложение № 2 к Акту классификации ИСПДн комитета муниципального заказа и торговли администрации города Ставрополя

|  |
| --- |
| УТВЕРЖДАЮ |
|  |
| Руководитель комитета муниципального заказа и торговли администрации города Ставрополя |
| \_\_\_\_\_\_\_\_\_\_\_\_ А.А.Ломанов |

Исходные данные классификации

информационных систем персональных данных

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Наименование информационной системы персональных данных | Исходные данные классификации информационной системы | | | | | | | Примечание |
| Категория персональных данных | Объем обрабатываемых персональных данных (количество субъектов персональных данных) | Структура информационной системы персональных данных | Наличие подключений к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) | Режим обработки персональных данных | Разграничение доступа пользователей | Нахождение информационной системы (ее составных частей) за пределами России |
|  |  |  |  |  |  |  |  |  |