АДМИНИСТРАЦИЯ ГОРОДА КУРСКА
Курской области

П О С Т А Н О В Л Е Н И Е

«13» февраля 2018 г. г. Курск № 292

Об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации города Курска

В целях исполнения Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», ПОСТАНОВЛЯЮ:

1. Утвердить положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации города Курска согласно приложению 1.
2. Утвердить план мероприятий по защите персональных данных в Администрации города Курска согласно приложению 2.
3. Утвердить план внутренних проверок режима обработки и защиты персональных данных согласно приложению 3.
4. Утвердить форму отчета о результатах проведения внутренней проверки режима обработки и защиты персональных данных в Администрации города Курска согласно приложению 4.
5. Управлению информации и печати Администрации города Курска (Комкова Т.В.) обеспечить опубликование настоящего постановления в газете «Городские Известия» и размещение на официальном сайте Администрации города Курска в информационно-телекоммуникационной сети «Интернет».
6. Постановление вступает в силу со дня его официального опубликования.

Глава города Курска Н.И. Овчаров

ПРИЛОЖЕНИЕ 1
УТВЕРЖДЕНО
постановлением
Администрации города Курска
от «13» февраля 2018 года
№ 292

ПОЛОЖЕНИЕ
об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации города Курска

1. Общие положения

1.1. Настоящее Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации города Курска (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 16 апреля 2012 года № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием

шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 30 августа 2012 года № 440 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

1.2. Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) Администрации города Курска (далее – Оператор) на протяжении всего жизненного цикла ИСПДн.

2. Термины и определения

2.1. В настоящем Положении используются следующие термины и их определения:

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

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, если иное не предусмотрено федеральным законом.

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.

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

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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).

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Ресурс информационной системы – 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.

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.

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

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

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

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

3. Порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации города Курска

3.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн Администрации города Курска понимается формирование и реализация совокупности согласованных по целям, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (далее – СЗПДн).

3.2. СЗПДн включает в себя организационные и (или) технические мероприятия, определенные с учетом актуальных угроз безопасности ПДн, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах.

3.3. Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор или лицо, осуществляющее обработку ПДн по поручению оператора на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПДн при их обработке в информационной системе.

3.4. Выбор средств защиты информации для СЗПДн осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее – ФСБ

России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) во исполнение Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

3.5. Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности ПДн при их обработке в ИСПДн.

3.6. Проводится предпроектное обследование и разработка технического задания на создание СЗПДн.

3.6.1. Назначается ответственный за организацию обработки ПДн Администрацией города Курска.

3.6.2. Определяются цели обработки ПДн.

3.6.3. Определяется перечень ИСПДн Администрации города Курска и состава ПДн, обрабатываемых в ИСПДн.

3.6.4. Определяется перечень обрабатываемых Администрацией города Курска ПДн.

3.6.5. Определяются сроки обработки и хранения ПДн, исходя из требования, что ПДн не должны храниться дольше, чем этого требуют цели обработки этих ПДн, по достижению которых ПДн подлежат уничтожению.

3.6.6. Определяется перечень используемых в ИСПДн (предлагаемых к использованию в ИСПДн) общесистемных и прикладных программных средств.

3.6.7. Определяется режим обработки ПДн в ИСПДн в целом и в отдельных компонентах.

3.6.8. Назначается ответственный за обеспечение безопасности ПДн в ИСПДн (далее – Ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн.

3.6.9. Назначается ответственный пользователь криптосредств, обеспечивающий функционирование и безопасность криптосредств, предназначенных для обеспечения безопасности ПДн. Утверждается перечень лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности ПДн в ИСПДн (пользователей криптосредств).

3.6.10. Определяется перечень помещений, в которых размещены ИСПДн и материальные носители ПДн.

3.6.11. Определяется конфигурация и топология ИСПДн в целом и их отдельных компонентов, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения.

3.6.12. Определяются технические средства и системы, используемые в ИСПДн, включая условия их расположения.

3.6.13. Формируются технические паспорта ИСПДн.

3.6.14. Разрабатываются организационно-распорядительные документы (далее – ОРД), регламентирующие процесс обработки и защиты ПДн.

3.6.15. Получается при необходимости согласие на обработку ПДн

субъектом ПДн, подписываются обязательства о соблюдении конфиденциальности ПДн сотрудником Администрации города Курска.

3.6.16. Определяется уровень защищенности ПДн при их обработке в ИСПДн в соответствии с «Требованиями к защите ПДн при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 (подготовка и утверждение акта определения уровня защищенности ПДн при их обработке в ИСПДн).

3.6.17. Определяются типы угроз безопасности ПДн, актуальных для информационной системы, с учетом оценки возможного вреда в соответствии с нормативными правовыми актами, принятыми во исполнение Федерального закона «О персональных данных». Определяются угрозы безопасности ПДн в конкретных условиях функционирования ИСПДн (разработка моделей угроз безопасности ПДн при их обработке в ИСПДн).

3.6.18. Формируется техническое задание на разработку СЗПДн по результатам предпроектного обследования на основе нормативно-методических документов ФСТЭК России и ФСБ России с учетом установленного уровня защищенности ПДн при их обработке в ИСПДн.

3.7. Организуется проектирование СЗПДн, закупка, установка, настройка и опытная эксплуатация необходимых средств защиты информации.

3.7.1. Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиям к обеспечению безопасности ПДн для соответствующего уровня защищенности ПДн при их обработке в ИСПДн и/или не нейтрализуют всех угроз безопасности ПДн для данной ИСПДн.

3.7.2. Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Администрации города Курска.

3.7.3. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.7.4. На стадии проектирования и создания СЗПДн для ИСПДн Администрации города Курска проводятся следующие мероприятия:

разработка технического проекта СЗПДн;

приобретение (при необходимости), установка и настройка серийно выпускаемых технических средств обработки, передачи и хранения информации;

разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

приобретение, установка и настройка сертифицированных технических, программных и программно-технических средств защиты информации, в том числе (при необходимости) средств криптографической защиты информации;

реализация разрешительной системы доступа пользователей ИСПДн к обрабатываемой в ИСПДн информации;

подготовка эксплуатационной документации на используемые средства защиты информации;

корректировка (дополнение) организационно-распорядительной документации в части защиты информации.

3.8. ИСПДн с СЗПДн вводится в эксплуатацию.

3.8.1. На стадии ввода в ИСПДн (СЗПДн) осуществляются:

опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн (при необходимости);

приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации (при необходимости);

контроль выполнения требований (возможно проведение данного контроля в виде аттестации по требованиям безопасности ПДн).

3.8.2. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

4. Проведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации города Курска

4.1. Работы по обеспечению безопасности ПДн проводятся в соответствии с Планом мероприятий по защите персональных данных в Администрации города Курска (приложение 2). Внутренние проверки режима обработки и защиты ПДн Администрацией города Курска проводятся в соответствии с Планом внутренних проверок режима обработки и защиты персональных данных (приложение 3). По результатам проведения внутренней проверки составляется Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в Администрации города Курска.

4.2. Контроль за проведением работ по обеспечению безопасности ПДн осуществляет ответственный за организацию обработки ПДн в виде методического руководства, участия в разработке требований по защите ПДн, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи,

технических и программных средств защиты, участия в оценке соответствия ИСПДн Администрации города Курска требованиям безопасности ПДн.

4.3. При необходимости к проведению работ по обеспечению безопасности ПДн могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

4.4. В соответствии с Постановлением Правительства Российской Федерации от 16 апреля 2012 года N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», приказом ФСБ России от 30 августа 2012 года № 440 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности ПДн Администрации города Курска необходимо привлекать специализированные организации, имеющие лицензии ФСБ России на осуществление работ по распространению шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну, на осуществление технического

обслуживания шифровальных (криптографических) средств, на осуществление работ по оказанию услуг в области шифрования информации, не содержащих сведений, составляющих государственную тайну.

5. Решение вопросов обеспечения безопасности персональных данных в динамике изменения обстановки и контроля эффективности защиты

5.1. Модернизация СЗПДн для функционирующих ИСПДн Администрации города Курска должна осуществляться в случае:

изменения состава или структуры ИСПДн или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

изменения состава угроз безопасности ПДн в ИСПДн;

изменения уровня защищенности ПДн при их обработке в ИСПДн;

прочих случаях, по решению оператора.

5.2. В целях определения необходимости доработки (модернизации) СЗПДн ответственным за организацию обработки ПДн должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и уровня защищенности ПДн при их обработке в ИСПДн, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. По результатам проведения внутренней проверки составляется отчет проверки, который утверждается ответственным за организацию обработки ПДн в Администрации города Курска.

5.3. Анализ инцидентов безопасности ПДн и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

несоблюдение условий хранения носителей ПДн;

использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;

нарушение заданного уровня безопасности ПДн (конфиденциальность/ целостность/доступность).

ПРИЛОЖЕНИЕ 2
УТВЕРЖДЕН
постановлением
Администрации города Курска
от «13» февраля 2018 года
№ 292

ПЛАН
мероприятий по защите персональных данных в Администрации города Курска

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с ПДн	При необходимости	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
2.	Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»
3.	Ограничение доступа сотрудников к ПДн	При необходимости (при создании ИСПДн)	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона необходимо разграничить доступ сотрудников Оператора к ПДн
4.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи персональных данных, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц
5.	Ведение журналов учета отчуждаемых электронных носителей персональных данных,	Постоянно	

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
	средств защиты информации		
6.	Повышение квалификации сотрудников в области защиты ПДн	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за обеспечение безопасности ПДн в ИСПДн)
7.	Инвентаризация информационных ресурсов	Раз в год	Проводится с целью выявления в информационных ресурсах присутствия ПДн
8.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для ПДн Оператором устанавливаются сроки обработки ПДн.
9.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн.
10.	Определение уровня защищенности ПДн при их обработке в ИСПДн	При необходимости	Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется при создании ИСПДн, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
11.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИСПДн
12.	Аттестация ИСПДн на соответствие требованиям по обеспечению безопасности ПДн	При необходимости	Проводится совместно с лицензиатами ФСТЭК
13.	Понижение требований по защите ПДн путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер	При необходимости	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона

ПРИЛОЖЕНИЕ 3
УТВЕРЖДЕН
постановлением
Администрации города Курска
от «13» февраля 2018 года
№ 292

ПЛАН
внутренних проверок режима обработки и защиты персональных данных в Администрации города Курска

№	Мероприятие	Периодич-ность	Дата, подпись исполни-теля
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Ежегодно	
2.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Раз в полгода	
3.	Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта	Ежегодно	
4.	Проверка ведения журналов по учету обращений субъектов ПДн и учету передачи ПДн субъектов третьим лицам	Ежегодно	
5.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
6.	Проверка соблюдения условий хранения материальных носителей ПДн	Раз в полгода	
7.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику Администрации города Курска в отношении обработки ПДн	Ежегодно	
8.	Проверка применения для обеспечения безопасности ПДн средств защиты информации, прошедших в установленном порядке процедуру соответствия	Ежегодно	
9.	Контроль учета машинных носителей ПДн	Ежегодно	
10.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПДн	Ежегодно	
11.	Контроль внесения изменений в структурно-функциональные характеристики ИСПДн	Раз в полгода	

№	Мероприятие	Периодич-ность	Дата, подпись исполни-теля
12.	Контроль корректности настроек средств защиты информации	Раз в полгода	
13.	Контроль за обеспечением резервного копирования	Ежегодно	
14.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты ПДн	Ежегодно	

ПРИЛОЖЕНИЕ 4
УТВЕРЖДЕН
постановлением
Администрации города Курска
от «13» февраля 2018 года
№ 292

ОТЧЕТ
о результатах проведения внутренней проверки режима обработки и защиты персональных данных в Администрации города Курска

1.1 Внутренняя проверка произведена на основании постановления Администрации города Курска «Об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации города Курска» №_____ от «____»_____ 20__ г.

1.2 Проверка проводилась «___»_____20__ г. по адресу:
_____
_____

1.3 В ходе проверки были проведены следующие мероприятия:
1) _____
2) _____
3) _____
4) _____
5) _____

1.4 Результаты проведения проверки:
1) _____
2) _____
3) _____
4) _____
5) _____

1.5 Необходимые мероприятия.
На основании проведения внутренней проверки режима обработки и защиты ПДн рекомендуется осуществить следующие мероприятия:
1) _____
2) _____

3) _____

4) _____

5) _____

Подписи ответственных лиц, проводивших внутреннюю проверку режима обработки и защиты ПДн:

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)
_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)
_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)