Администрация города Кирсанова
Тамбовской области

РАСПОРЯЖЕНИЕ

«17» апреля 2013 г. **г. Кирсанов** **№104-р**

Об утверждении документов по организации работ по защите персональных данных в администрации города

В соответствии с постановлением 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» утвердить:

1.Инструкцию ответственного за организацию обработки персональных данных в администрации города согласно приложению 1.

2.Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города согласно приложению 2.

3. Разместить (опубликовать) настоящее постановление на портале http://www.top68.ru.

4. Разместить настоящее распоряжение на официальном сайте администрации города http://g37.tambov.gov.ru.

5. Контроль за исполнением настоящего распоряжения возложить на управляющего делами Г.М.Волкову.

Глава администрации города Д.В.Терещенко

ПРИЛОЖЕНИЕ 1

УТВЕРЖДЕНА

распоряжением администрации города

от « 17 » апреля 2013 г.№104-р

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в администрации города

1. Основные понятия

Применяемые в настоящей Инструкции термины и понятия означают:

Администратор безопасности - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место (АРМ) - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Защита информации от разглашения - защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа (ЗИ от НСД) - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Информационная система персональных данных (ИСПДн) - 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.

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.

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.

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Лицо ответственное за организацию обработки персональных данных (далее - Ответственный) – лицо, назначенное нормативным правовым актом администрации города, ответственное за регламентацию процесса обработки и защиты персональных данных.

Персональные данные (ПДн) - 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.

Распространение персональных данных - действия, направленные на передачу ПДн определенному кругу лиц (передача ПДн) или на ознакомление с ПДн неограниченного круга лиц, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом.

Средство защиты информации (СЗИ) - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

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

2. Общие положения

1. Настоящая инструкция разработана на основании следующих нормативных правовых документов:

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ;

Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ;

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

специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Государственная техническая комиссия при президенте Российской Федерации, 2002 г.;

2.2. Инструкция определяет основные задачи, функции, обязанности и права Ответственного за организацию обработку ПДн ИСПДн.

2.3. В своей деятельности Ответственный руководствуется требованиями действующих федеральных законов, общегосударственных нормативных правовых документов, (указанных в п. 2.1.), а также нормативно правовых актов администрации города по вопросам защиты ПДн и обеспечивает их выполнение.

2.4. Ответственный за организацию обработки персональных данных, получает указания непосредственно от главы администрации города и подотчетно ему.

3. Задачи и функции Ответственного

3.1. Основными задачами Ответственного являются:

разработка нормативной правовой документации, регламентирующей порядок обработки и защиты ПДн;

организация доведения до сведения сотрудников, допущенных к ПДн, положений законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

осуществление внутреннего контроля соблюдения требований законодательства РФ и инструкций при обработке ПДн, в том числе требований к защите ПДн;

организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;

заполнение и отправка уведомления об обработке (о намерении осуществлять обработку) ПДн;

организация контроля эффективности защиты ПДн.

3.2. Для выполнения поставленных задач на Ответственного возлагаются следующие функции:

организация допуска пользователей (разработчиков, эксплуатационного персонала) к техническим, программным средствам и информационным ресурсам ИСПДн в соответствии с матрицей доступа пользователей к защищаемым ПДн ИСПДн на всех стадиях жизненного цикла ИСПДн.

участие на стадии проектирования (внедрения) ИСПДн, в разработке технологии обработки ПДн по вопросам:

организации порядка учета, хранения и обращения с документами и носителями информации;

подготовка новых инструкций и внесение изменений и дополнений в настоящую Инструкцию, определяющих задачи, функции, ответственность, права и обязанности администраторов и пользователей ИСПДн по вопросам защиты ПДн;

организация контроля выполнения требований действующих нормативных документов по вопросам защиты информации при обработке ПДн в ИСПДн

оперативный контроль хода технологического процесса обработки ПДн;

методическое руководство работой пользователей ИСПДн в вопросах обеспечения информационной безопасности.

4. Обязанности Ответственного

4.1. Для реализации поставленных задач и возложенных функций Ответственный обязан:

Осуществлять учет и периодический контроль состава и полномочий пользователей различных ПЭВМ, на которых ведется обработка ПДн.

Своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ от НСД, установленных на ПЭВМ.

Контролировать обеспечение защиты ПДн при взаимодействии пользователей с информационными сетями общего пользования.

Требовать прекращения обработки ПДн, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

Организовывать контроль эффективности защиты ПДн:

по выявлению возможности вмешательства в процесс функционирования ПЭВМ и осуществления НСД к информации и техническим средствам ПЭВМ;

проводить занятия с администраторами и пользователями ИСПДн по правилам работы на ПЭВМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков выявленных при контроле эффективности защиты информации.

Организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль правильности их использования.

Осуществлять периодический контроль порядка учета, создания, хранения и использования резервных и архивных копий массивов данных.

Участвовать в проведении внутреннего расследования по фактам разглашения ПДн, нарушения условий функционирования системы обработки и защиты ПДн.

4.2 Ответственному запрещается:

Использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, предоставлять такую возможность другим.

Производить действия, приводящие к нарушению обработки ПДн.

5. Права Ответственного

5.1. Ответственный имеет право:

получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и ПЭВМ пользователей;

требовать от пользователей ИСПДн выполнения правил обработки ПДн и инструкций по обеспечению безопасности ПДн в ИСПДн;

участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим отчетом главе администрации города.

5.2. Ответственный несет ответственность за:

реализацию утвержденных в администрации города документов, регламентирующих порядок обработки и обеспечения безопасности ПДн.

разглашение ПДн и сведений ограниченного распространения, ставших известными ему по роду работы;

качество и последствия проводимых им работ по контролю действий пользователей при работе в ИСПДн.

6. Проведение внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты персональных данных

6.1. Основными целями проведения внутреннего расследования являются:

выявление предпосылок утраты ПДн в результате нарушения порядка их обработки;

выявление лиц из числа муниципальных служащих (далее - служащий) администрации города виновных в утрате ПДн;

определение ущерба в результате утраты ПДн;

проверка полноты и качества исполнения нормативных документов по работе со средствами защиты ПДн;

документальное подтверждение соответствия обработки, хранения и передачи ПДн нормам и правилам, установленным федеральными правовыми и нормативными актами;

определение фактического состояния системы защиты ПДн.

6.2. Служащий администрации города, по вине которого произошло нарушение, обязан по требованию Ответственного представить объяснения в письменной форме не позднее одного рабочего дня с момента получения соответствующего требования. Ответственный вправе увеличить указанный срок, а также поставить перед служащим перечень вопросов, на которые служащий обязан ответить.

6.3. В целях внутреннего расследования все служащие администрации города, по первому требованию Ответственного, должны предъявить для проверки все числящиеся за ними материалы, содержащие ПДн представить

устные или письменные объяснения, в том числе об известных им фактах разглашения ПДн, утраты документов и изделий, содержащих ПДн.

6.4. В случае давления на служащего администрации города со стороны других служащих администрации города или третьих лиц (просьб, угроз, шантажа и др.) по вопросам, связанным с проведением внутреннего расследования, служащий администрации города обязан сообщить об этом Ответственному.

6.5. Для проведения внутреннего расследования глава администрации города формирует комиссию из опытных и квалифицированных служащих администрации города в составе не менее трех человек. Председателем комиссии является Ответственный.

6.6. До вынесения решения, членам комиссии запрещается разглашать сведения остальным служащим администрации города о ходе проведения внутреннего расследования и ставших известными им в связи с этим обстоятельствах.

6.7. В процессе проведения внутреннего расследования выясняются:

- перечень разглашенных сведений, составляющих ПДн;
- причины разглашения ПДн;
- круг лиц, виновных в разглашении ПДн;
- размер причиненного ущерба;
- недостатки и нарушения, допущенные служащими администрации города при работе с ПДн;
- иные обстоятельства.

6.8. По результатам расследования, комиссией составляется акт, с отражением в нем лиц, виновных в разглашении ПДн, размера причиненного ущерба администрации города, наличии ущерба субъектам персональных данных, а также иных выясненных обстоятельствах.

6.9. На основании акта комиссия выносит решение о:
применении мер дисциплинарного воздействия к служащему;
информировании регулятора о факте нарушения;
информировании правоохранительных органов;
информировании субъектов персональных данных.

7. Порядок реагирования на аварийную ситуацию

7.1. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

7.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться Ответственным в «Журнале по учету мероприятий по контролю».

7.3. В кратчайшие сроки, не превышающие одного рабочего дня, Ответственный предпринимает меры по восстановлению нарушенной работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

7.4. При реагировании на инцидент, важно правильно классифицировать критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 – Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты.

Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты.

Уровень 3 – Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к нарушению работоспособности ИСПДн и средств защиты на сутки и более.

7.5. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

системы жизнеобеспечения;
системы обеспечения отказоустойчивости;
системы резервного копирования и хранения данных;
системы контроля физического доступа.
Системы жизнеобеспечения ИСПДн включают:
пожарные сигнализации и системы пожаротушения;
системы вентиляции и кондиционирования;
системы резервного питания.

7.6. Все помещения администрации города, в которых размещаются элементы ИСПДн и средства защиты должны быть оборудованы средствами пожарной сигнализации.

7.7. Ответственным должно быть организовано обучение должностных лиц, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

оказание первой медицинской помощи;

пожаротушение;

эвакуация людей;

защита материальных и информационных ресурсов;

методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

выключение оборудования, электричества, водоснабжения, газоснабжения.

7.8. Администратор безопасности должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИСПДн.

7.9. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

С инструкцией ознакомлен _____

ПРИЛОЖЕНИЕ 2

УТВЕРЖДЕНЫ
распоряжением администрации города

от « 17 » апреля 2013 г.№104-р

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города (далее - Правила) относятся к основным организационно-распорядительным документам системы документов информационной безопасности администрации города и разработаны в соответствии с требованиями постановления Правительств 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 нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

В Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных (ПДн) в администрации города с целью своевременного выявления и предотвращения;

хищения технических средств и носителей информации;

утраты информации;

преднамеренных программно-технических воздействий на информацию и (или) средства вычислительной техники, вызывающих нарушение целостности информации и нарушение работоспособности автоматизированной системы;

несанкционированного доступа к ПДн с целью уничтожения, искажения, модификации (подделки), копирования и блокирования;

утечки информации по техническим каналам.

Внутренний контроль состояния защиты информации включает в себя:

контроль организации защиты информации;

контроль эффективности защиты информации.

2. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности персональных данных

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок условий обработки ПДн. Проверки осуществляются муниципальными служащими структурного подразделения администрации города, ответственного за организацию обработки ПДн в администрации города либо комиссией, образуемой главой администрации города, не реже одного раза в год в соответствии с утвержденным графиком.

При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям производится проверка:

соблюдения принципов обработки ПДн;

соответствия локальных актов в города ПДн администрации города действующему законодательству Российской Федерации;

выполнения служащими администрации города требований и правил обработки ПДн в информационных системах персональных данных (ИСПДн) администрации города;

перечней ПДн, используемых для решения задач и функций cпруктурными подразделениями администрации города и необходимости обработки ПДн в ИСПДн администрации города;

актуальности содержащихся в Правилах обработки ПДн в администрации города в каждой ИСПДн администрации города информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований но обработке и обеспечению безопасности ПДн;

правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн администрации города;

актуальности перечня должностей муниципальных служащих города, замещающих должности муниципальной службы в администрации города, уполномоченных на обработку ПДн, имеющих доступ к ПДн;

актуальности перечня должностей муниципальных служащих города, замещающих должности муниципальной службы в администрации города, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

соблюдения прав субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн администрации города;

соблюдения обязанностей администрации города как оператора ПДн, предусмотренных действующим законодательством в города ПДн;

порядка взаимодействия с субъектами персональных данных, ПДн которых обрабатываются в ИСПДн города, в том числе соблюдения сроков, предусмотренных действующим законодательством в города ПДн,

соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения (запросы) субъектов персональных данных, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами персональных данных;

наличия необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн администрации города;

актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;

актуальности перечня ИСПДн в администрации города;

наличия и актуальности сведений, содержащихся в Правилах обработки ПДн администрации города для каждой ИСПДн администрации города;

знания и соблюдения муниципальными служащими города, замещающими должности муниципальной службы в администрации города (далее - служащие администрации города) положений действующего законодательства Российской Федерации в города ПДн;

знания и соблюдения служащими администрации города положений локальных актов администрации города в города обработки и обеспечения безопасности ПДн;

знания и соблюдения служащими администрации города инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

соблюдения служащими администрации города конфиденциальности ПДн;

актуальности локальных актов администрации города в города обеспечения безопасности ПДн, в том числе в Технических паспортах ИСПДн;

соблюдения служащими администрации города требований по обеспечению безопасности ПДн;

наличия локальных актов администрации города, технической и эксплуатационной документации технических и программных средств ИСПДн администрации города;

по иным вопросам.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает главе администрации города.

При проведении внутреннего контроля на ИСПДн (отдельное автоматизированное рабочее место) администрации города составляется протокол контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте по форме, приведенной в приложении к настоящим Правилам.

3. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям в администрации города производится оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн в администрации города.

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн администрации города производится экспертное сравнение заявленной администрацией города в своих локальных актах оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и применяемых администрацией города мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в города ПДн и изложенных в настоящих Правилах осуществления внутреннего контроля соответствия обработки ПДн в администрации города.

По итогам сравнений принимается решение о достаточности применяемых администрацией города мер, направленных па обеспечение выполнения обязанностей, предусмотренных действующим законодательством в города ПДн и возможности или необходимости принятия дополнительных мер или изменения установленного в администрации города порядка обработки и обеспечения безопасности ПДн.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн, в администрации города оформляется в виде отдельного документа, подписывается председателем комиссии и утверждается главой администрации города.

По результатам пришлых решений структурным подразделением администрации города, ответственным за организацию обработки ПДн в администрации города, организуется работа по их реализации.

ПРИЛОЖЕНИЕ
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных требованиям к защите
персональных данных в администрации города

Форма

Протокол №_____
контроля выполнения требований по обеспечению безопасности информации,
содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте
(наименование структурного подразделения администрации города)

1. Объект контроля

Указать:

наименование автоматизированного рабочего места (АРМ); заводской (инвентарный) номер системного блока ПЭВМ АРМ; принадлежность к подразделению; адрес размещения АРМ.

2. Назначение объекта

Указать:

- тип информации, обрабатываемой (хранимой) на АРМ;
- уровень защищенности персональных данных при их обработке в информационной системе.

3. Контролируемые вопросы

Состояние организации технической защиты информации при обработке (хранении) информации ограниченного доступа.

Контроль наличия руководящих документов, инструкций, документации, регламентирующей обработку (хранение) информации ограниченного доступа:

перечня защищаемых ресурсов и уровня их конфиденциальности;

перечня лиц, обслуживающих АРМ;

перечня лиц, имеющих право самостоятельного доступа в помещение с АРМ;

перечня лиц, имеющих право самостоятельного доступа к штатным средствам АРМ и уровень их полномочий;

распоряжения о назначения комиссии для определении уровня защищенности персональных данных;

распоряжения о назначении администратора информационной безопасности;

данных по уровню подготовки персонала;

инструкции по обеспечению защиты информации, обрабатываемой на АРМ;

перечня программного обеспечения;

описания технологического процесса обработки информации;

схемы информационных потоков;

технического паспорта;

матрицы доступа субъектов к защищаемым информационным ресурсам;

акга установки системы активного зашумления (при наличии);
акта установки системы защиты информации от несанкционированного доступа (СЗИ НСД) (при наличии);
описания системы разграничения доступа и настроек СЗИ НСД;
инструкции администратору безопасности;
инструкции пользователю;
инструкции по антивирусному контролю;
распоряжения о допуске служащих;
распоряжения о вводе в эксплуатацию.
Контроль соответствия настройки подсистемы управления доступом, подсистемы регистрации и учета, подсистемы обеспечения целостности требованиям присвоенного класса защищенности от НСД.
В соответствии с требованиями руководящего документа "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите ипформации", утвержденного решением Председателя Гостехкомиссин от 30.03.1992, в настройках подсистемы управления доступом проверяется:
наличие требований к длине и сложности пароля;
ограничение максимального срока действия пароля;
настройки блокировки учетных записей при попытках несанкционированного доступа;
наличие административных прав у пользователей;
выполнение требований мандатного разграничения прав доступа к каталогам, программам, файлам.
В настройках подсистемы регистрации и учета контролируется:
отсутствие критических ошибок и несанкционированных запусков процессов, зарегистрированных в журнале приложений;
отсутствие зарегистрированных критических системных ошибок в системном журнале;
отсутствие зарегистрированных изменений действующих политик безопасности, прав доступа, настроек системы защиты информации в журнале системы защиты информации;
возможности несанкционированного доступа к информации, аудиты отказа, зарегистрированные в журнале безопасности.
В настройках подсистемы обеспечения целостности контролируется:
соответствие программного обеспечения, установленного на АРМ, аттестационным материалам;
отсутствие программных средств разработки и отладки приложений;
наличие средств антивирусного контроля, включая срок действия лицензии и периодичность обновления антивирусных баз.
Контроль наличия лицензионного программного обеспечения, установленного в процессе проведенной аттестации по требованиям безопасноти информации.

Контроль срока действия лицензии, порядка и периодичности обновления баз антивирусной программы.

Контроль наличия сетевых плат (в том числе интегрированных) и физической возможности их использования.

Контроль возможности и фактов подключения незарегистрированных магнитных и иных носителей информации.

4. Метод проведения контроля

Экспертно-документальный.

5. Средства контроля

Программные возможности операционной системы, установленной на контролируемом АРМ.

6. Перечень документов, регламентирующих выполнение требований по обеспечению безопасности информации

Контроль проводится в соответствии с требованиями:

Указа Президента Российской Федерации "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" от 17.03.2008 № 351;

специальных требований и рекомендаций по технической защите конфиденциальной информации (приказ Гостехкомиссии России от 30.08.2002 № 282);

руководящего документа "Автоматизировалшые системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" (решение Председателя Гостехкомиссии от 30.03.1992);

руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недскларированных возможностей" (приказ Председателя Гостехкомиссии России от 4.06.1999 № 114);

нормативных и руководящих документов ФСТЭК России по защите информации.

Контроль выполнили:

_____	_____	_____
должность	подпись	фамилия, инициалы
_____	_____	_____
должность	подпись	фамилия, инициалы

При проведении контроля присутствовали:

_____	_____	_____
должность	подпись	фамилия, инициалы
_____	_____	_____
должность	подпись	фамилия, инициалы

Дата проведения контроля:_____

(число, месяц, год)

Управляющий делами
администрации города
Г.М.Волкова
17.04.2013

Начальник юридического отдела
администрации города
И.Б.Епифанов
17.04.2013

Председатель комитета организационно-
контрольной работы и информатизации
администрации города
О.В.Данилова
17.04.2013