



Заместитель главы администрации города Нижнего Новгорода,
глава администрации Ленинского района

П Р И К А З

30.05.2014

№ 36

Об организации обработки персональных данных в администрации Ленинского района города Нижнего Новгорода

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», распоряжением администрации города Нижнего Новгорода от 31.08.2009 № 271-р «Об организации работ по защите персональных данных»,

ПРИКАЗЫВАЮ:

1.1. Утвердить Политику информационной безопасности в информационной системе персональных данных администрации Ленинского района города Нижнего Новгорода (приложение №1).

1.2. Утвердить Правила обработки персональных данных в администрации Ленинского района города Нижнего Новгорода (приложение №2).

1.3. Утвердить Правила рассмотрения запросов субъектов персональных данных или их представителей (приложение №3).

1.4. Утвердить Политику в отношении обработки персональных данных администрации Ленинского района города Нижнего Новгорода (приложение №4).

1.5. Утвердить Порядок доступа служащих администрации Ленинского района города Нижнего Новгорода в помещения, в которых ведется обработка

персональных данных (приложение №5).

1.6. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Ленинского района города Нижнего Новгорода (приложение № 6).

1.7. Утвердить Положение о комиссии по контролю соответствия обработки персональных данных установленным требованиям к защите персональных данных в администрации Ленинского района города Нижнего Новгорода (приложение № 7).

Исполняющий обязанности
главы администрации

Н.И. Рожкова

Приложение №1

к приказу исполняющего обязанности
главы администрации
Ленинского района
города Нижнего Новгорода

от "30" мая 2014 № 36

**Политика информационной безопасности
в информационной системе персональных данных
администрации Ленинского района
города Нижнего Новгорода**

СОДЕРЖАНИЕ

Термины и определения	5
ВВЕДЕНИЕ.....	9
1. Общие положения	9
2. Общие требования по защите персональных данных	10
2.1 Внутренняя защита	10
2.2 Внешняя защита	11
3. Система защиты персональных данных	12
4. Требования к подсистемам СЗПДн	13
4.1 Подсистемы управления доступом, регистрации и учета	13
4.2 Подсистема обеспечения целостности и доступности	14
4.3 Подсистема антивирусной защиты	14
4.4 Подсистема межсетевое экранирование.....	14
4.5 Подсистема анализа защищенности и обнаружения вторжений.....	15
4.6 Защита информации от утечки по техническим каналам.....	15
4.7 Подсистема криптографической защиты	15
5. Категории Пользователей ИСПДн	16
5.1 Администратор безопасности ИСПДн	16
5.2 Функции администратора безопасности ИСПДн.....	17
5.3 Администратор безопасности ИСПДн обязан.....	18
5.4 Администратор безопасности ИСПДн имеет право	18
5.5 Пользователь ИСПДн.....	18
5.6 Обязанности пользователя ИСПДн	18
5.7 Пользователям ИСПДн запрещается.....	19
6. Организация парольной защиты при работе на объектах информатизации... 20	
6.1 Порядок применения парольной защиты.	20
7. Требования к персоналу	21
8. Технологический процесс обработки персональных данных	22
8.1 Подготовка персонального компьютера (далее – ПК) к работе	23
8.2 Описание реализованных правил разграничения доступа	23
8.3 Исполнителю запрещается.....	24
9. Ответственность сотрудников ИСПДн администрации Ленинского района города Нижнего Новгорода	24

Термины и определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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

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

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

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.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

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

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

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.

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных 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 или наличия иного законного основания.

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.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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

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

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

В настоящем документе используются следующие сокращения.

АВС – антивирусные средства.

ИСПДн – информационная система персональных данных.

КЗ– контролируемая зона.

ЛВС – локальная вычислительная сеть.

МЭ – межсетевой экран.

НСД – несанкционированный доступ.

ОС – операционная система.

ПДн – персональные данные.

ПМВ – программно-математическое воздействие.

ПО – программное обеспечение.

ПЭМИН – побочные электромагнитные излучения и наводки.

САЗ – система анализа защищенности.

СЗИ – средства защиты информации.

СЗПДн – система (подсистема) защиты персональных данных.

СОВ – система обнаружения вторжений.

ТКУИ – технические каналы утечки информации.

УБПДн – угрозы безопасности персональных данных.

ВВЕДЕНИЕ

Настоящая Политика безопасности в информационной системе персональных данных администрации Ленинского района г. Нижнего Новгорода (далее – Политика безопасности) разработана в целях обеспечения безопасности персональных данных, является официальным документом.

Политика безопасности разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 01 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании:

- Приказа ФСТЭК России от 11.02.2013г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике безопасности определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн администрации Ленинского района г. Нижнего Новгорода.

1. Общие положения

Целью настоящей Политики безопасности является обеспечение безопасности объектов защиты администрации Ленинского района города Нижнего Новгорода от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения 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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожение данных.

Состав объектов защиты регламентируется в соответствии с «Перечнем персональных данных, разрешенных для обработки в ИСПДн администрации Ленинского района г. Нижнего Новгорода».

Состав ИСПДн подлежащих защите, представлен в «Сводном перечне информационных систем персональных данных администрации Ленинского района города Нижнего Новгорода».

2. Общие требования по защите персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой деятельности администрации Ленинского района города Нижнего Новгорода.

Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена за счет средств бюджета муниципального образования город Нижний Новгород в порядке, установленном федеральным законом.

2.1 Внутренняя защита

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами администрации Ленинского района города Нижнего Новгорода.

Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание сотрудником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделений, обрабатывающих ПДн;
- воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочее место только главе администрации, работникам отдела муниципальной службы и кадров и в исключительных случаях, по письменному разрешению главы администрации, руководителю структурного подразделения. (например, при подготовке материалов для аттестации сотрудника).

2.2 Внешняя защита

Для защиты конфиденциальной информации целенаправленно создаются неблагоприятные условия и труднопреодолимые препятствия для постороннего лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности структурного подразделения, обрабатывающего ПДн - посетители, сотрудники других структурных подразделений администрации. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и беседах.

Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных

данных.

По возможности персональные данные обезличиваются.

Требования настоящей Политики безопасности распространяются на всех сотрудников администрации Ленинского района города Нижнего Новгорода (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (посетители, подрядчики, аудиторы и т.п.).

3. Система защиты персональных данных

Система защиты персональных данных (СЗПДн) администрации Ленинского района города Нижнего Новгорода, строится на основании:

- **Перечня персональных данных, разрешенных для обработки в ИСПДн и подлежащих защите;**
- **Акта классификации информационной системы персональных данных;**
- **Модели угроз безопасности персональных данных;**
- Технического паспорта ИСПДн;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн администрации Ленинского района города Нижнего Новгорода.

На основании анализа актуальных угроз безопасности ПДн, описанного в «Модели угроз», делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- Сервера приложений;
- СУБД;
- Каналов передачи данных в сети.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевое экранирования;
- средства криптографической защиты информации при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн, операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты.

Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;

- обеспечение целостности данных;
- обнаружение вторжений.

Список используемых технических средств и средств защиты отражается в «Техническом паспорте ИСПДн». Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств, или средств защиты, или элементов ИСПДн, соответствующие изменения должны быть утверждены главой администрации Ленинского района города Нижнего Новгорода или лицом, ответственным за обеспечение защиты ПДн, и внесены в «Лист регистрации изменений «Технического паспорта ИСПДн».

4. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в «Акте классификации информационной системы персональных данных администрации Ленинского района города Нижнего Новгорода».

4.1 Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

- идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова;
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД).

Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

4.2 Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн администрации Ленинского района города Нижнего Новгорода, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

4.3 Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и рабочих станций пользователей ИСПДн администрации Ленинского района города Нижнего Новгорода.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

4.4 Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика;
- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
- идентификации и аутентификации администратора межсетевого экрана при его локальных запросах на доступ;

- регистрации входа (выхода) администратора межсетевого экрана в систему (из системы), либо загрузки и инициализации системы и ее программного останова;
- контроля целостности своей программной и информационной части;
- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрации с учетом входного и выходного сетевого интерфейса, как средство проверки подлинности сетевых адресов;
- регистрации и учета запрашиваемых сервисов прикладного уровня;
- блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования, классом не ниже 4.

4.5 Подсистема анализа защищенности и обнаружения вторжений

В ходе анализа содержания мер по обеспечению безопасности персональных данных установлено, что в ИСПНн 4 уровня защищенности к данной подсистеме требования не предъявляются.

4.6 Защита информации от утечки по техническим каналам

Для выполнения требования по защите информации от ПЭМИН в информационных системах 3 класса для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах 1 класса возможно применение сертифицированных средств защиты информации от ПЭМИН, прошедшие в установленном порядке процедуру оценки соответствия или размещение объектов защиты в соответствии с предписанием на эксплуатацию и на максимальном удалении от границ контролируемой зоны.

4.7 Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн администрации Ленинского района города Нижнего Новгорода, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

5. Категории Пользователей ИСПДн

В ИСПДн администрации Ленинского района города Нижнего Новгорода можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор безопасности ИСПДн;
- пользователи ИСПДн;
- технический специалист по обслуживанию оборудования;

На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

5.1 Администратор безопасности ИСПДн

Администратор безопасности ИСПДн - сотрудник администрации Ленинского района города Нижнего Новгорода, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора ИСПДн) к элементам, хранящим персональные данные.

Администратор безопасности ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, и к части ключевых элементов ИСПДн;
- имеет права доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных);
- имеет право реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;
- имеет право осуществлять аудит средств защиты;
- имеет право устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

Администратор безопасности назначается приказом главы администрации Ленинского района города Нижнего Новгорода и отвечает за обеспечение устойчивой работоспособности и информационной безопасности объекта информатизации.

Администратор безопасности несет ответственность за организацию работ по обеспечению безопасности информации, обрабатываемой,

передаваемой в ИСПДн, а также правильность использования и нормального функционирования средств защиты информации (СЗИ), подготовку сотрудников по вопросам безопасной обработки информации в ИСПДн.

5.2 Функции администратора безопасности ИСПДн.

Осуществляет настройку и сопровождение системы защиты от НСД в ИСПДн, при этом:

- реализует полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководством списка сотрудников, допущенных к работе в ИСПДн;
- вводит описание пользователей ИСПДн в информационную базу системы защиты от НСД;
- назначает пароли к информационным ресурсам и вводит в базу данных системы защиты описание полномочий доступа пользователей к защищаемым ресурсам;
- своевременно удаляет описание пользователя из базы данных при увольнении или перемещении сотрудника;
- периодически производит смену паролей пользователей для доступа в систему обработки информации ИСПДн.

Осуществляет настройку и сопровождение подсистемы регистрации и учета:

- вводит в базу данных системы защиты от НСД описания событий, подлежащих регистрации в системном журнале;
- проводит регулярный анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;
- своевременно информирует руководство о несанкционированных действиях сотрудников и организует расследование попыток НСД.

Сопровождает подсистемы обеспечения целостности программного обеспечения (ПО):

- проводит периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий исполнителей ИСПДн;
- осуществляет восстановление системы защиты от НСД при сбоях;
- проводит контроль соответствия общесистемной программной среды эталону;
- обеспечивает поддержание установленного порядка и соблюдение требований инструкции по антивирусной защите.

Требуется прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

Участвует в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

Производит выдачу исполнителям паролей для средств защиты информации (СЗИ) от несанкционированного доступа (НСД), а также осуществляет оперативный контроль за действиями пользователей ИСПДн.

5.3 Администратор безопасности ИСПДн обязан

Обеспечивать функционирование и поддерживать работоспособность средств защиты автоматизированных рабочих мест в пределах возложенных на них функций.

В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

Информировать главу администрации Ленинского района города Нижнего Новгорода о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

5.4 Администратор безопасности ИСПДн имеет право

Контролировать работу пользователей на автоматизированных рабочих местах ИСПДн.

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

5.5 Пользователь ИСПДн

Пользователь ИСПДн - сотрудник администрации Ленинского района города Нижнего Новгорода, осуществляющий обработку ПДн. Обработка ПДн включает в себя возможность:

- просмотра Пдн;
- ручного ввода Пдн в ИСПДн;
- формирования справок и отчетов по информации, полученной из ИСПДн.

Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

5.6 Обязанности пользователя ИСПДн

Пользователь ИСПДн обязан:

- выполнять в ИСПДн только те процедуры, которые определены для него в «Разрешительной системе доступа к информационным (программным) ресурсам объекта вычислительной техники»;
- перед обработкой персональных данных включать и проверять функционирование средства активной защиты;
- знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке машинных носителей информации в ИСПДн администрации Ленинского района города Нижнего

Новгорода, а также руководящих и организационно-распорядительных документов.

- перед началом обработки проводить антивирусную проверку файлов, хранящихся на съемных носителях информации.

- экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

- соблюдать установленный режим разграничения доступа к информационным ресурсам (получать у администратора безопасности ИСПДн пароль, надежно его запоминать и хранить в тайне).

- немедленно докладывать администратору безопасности ИСПДн обо всех фактах и попытках НСД к обрабатываемой в ИСПДн информации или об ее исчезновении (искажении).

5.7 Пользователям ИСПДн запрещается

- записывать и хранить информацию на неучтенных носителях информации (НИ);

- оставлять во время работы магнитные НИ (или ИСПДн с НИ) без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;

- отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами в ИСПДн;

- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

- обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам обработки информации;

- сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ИСПДн;

- работать на ИСПДн при обнаружении каких-либо неисправностей;

- хранить НИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

- хранить на учтенных НИ программы и данные, не относящиеся к рабочей информации;

- вводить в ОТСС персональные данные под диктовку или с микрофона;

- осуществлять электропитание и заземление ОТСС от нештатных сетей электропитания и заземления;

- привлекать посторонних лиц для производства ремонта ОТСС без согласования с администратором безопасности ИСПДн.

6. Организация парольной защиты при работе на объектах информатизации

Личные пароли доступа к объекту информатизации, системе защиты от НСД, выдаются пользователям администратором безопасности ИСПДн. Требования к сложности пароля:

- длина пароля должна быть не менее 6-ти буквенно-цифровых символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования ИСПДн, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;

- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- не использовать в качестве пароля комбинацию символов, набираемых последовательно на клавиатуре (например, 123456 и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

- не использовать ранее использованные пароли.

Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования инструкции и других руководящих документов по паролированию;

- своевременно сообщать администратору безопасности ИСПДн о всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

- хранить пароли в записанном виде на отдельных листах бумаги;

- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

6.1 Порядок применения парольной защиты.

Полная плановая смена паролей на ИСПДн проводится один раз в 3 месяца.

Удаление (в т.ч. внеплановая смена) личного пароля любого пользователя ИСПДн должна производиться в следующих случаях:

- в случае подозрения на дискредитацию пароля;

- по окончании срока действия;

- в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) пользователя после окончания последнего сеанса работы данного пользователя с системой;

- по указанию администратора безопасности ИСПДн.

Смена пароля осуществляется администратором безопасности ИСПДн.

Для предотвращения доступа к персональным данным, находящимся в ПЭВМ, минуя ввод пароля, пользователь во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню, или выключить ПЭВМ.

Порядок применения (смены) паролей при работе на ПЭВМ, оборудованных системой защиты от НСД, приведен в эксплуатационной документации на СЗИ.

При первичном допуске к работе на ИСПДн, пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает инструкцию пользователя, получает персональный идентификатор или личный текущий пароль у администратора безопасности ИСПДн. Перед началом обработки персональных данных пользователь включает ИСПДн, визуально убеждается в исправности и нормальном функционировании ИСПДн.

В процессе работы пользователь создает файлы и массивы информации на ИСПДн с применением операционных систем Windows.

При необходимости вывод персональных данных из ИСПДн осуществляется следующим образом:

- копированием на учетные носители информации;
- на печатающее устройство (принтер).

7. Требования к персоналу

Сотрудники администрации Ленинского района города Нижнего Новгорода, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника, непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники администрации Ленинского района города Нижнего Новгорода, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования

третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники администрации Ленинского района города Нижнего Новгорода должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники администрации Ленинского района города Нижнего Новгорода должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами администрации Ленинского района города Нижнего Новгорода, третьим лицам.

При работе с ПДн в ИСПДн сотрудники администрации Ленинского района города Нижнего Новгорода обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов ИСПДн или терминалов.

При завершении работы с ИСПДн, сотрудники обязаны защитить ИСПДн или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники администрации Ленинского района города Нижнего Новгорода должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятую политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и администратору безопасности ИСПДн.

8. Технологический процесс обработки персональных данных

В процессе обработки информации в информационных системах персональных данных администрации Ленинского района г. Нижнего Новгорода участвуют следующие группы пользователей:

- администратор безопасности ИСПДн – обладает всей полнотой доступа к ресурсам информационных систем персональных данных (ИСПДн), организует и контролирует работу ИСПДн.

- помощник администратора безопасности ИСПДн – обладает всей полнотой доступа к ресурсам информационных систем персональных данных (ИСПДн), организует и контролирует работу ИСПДн.

- пользователи, имеющие доступ к ИСПДн на основании приказа о допуске к ИСПДн.

Перечень объектов доступа:

- жесткие магнитные диски (ЖМД);
- оптические диски (CD-ROM);
- Flash-накопители;
- штатное программное обеспечение (ПО).

Перечень субъектов доступа:

- администратор безопасности ИСПДн;
- помощник администратора безопасности ИСПДн;
- пользователи.

К работе в ИСПДн допускаются только сотрудники в соответствии с утвержденной «Разрешительной системой доступа информационной системы персональных данных администрации Ленинского района г. Нижнего Новгорода», допущенные к обработке персональных данных (далее - информации), после изучения организационно-распорядительной документации.

8.1 Подготовка персонального компьютера (далее – ПК) к работе

Включить ПК, для чего: подключить сетевые шнуры электропитания к сети 220 В, включить устройства защиты и убедиться в их функционировании. Включить источник бесперебойного питания, включить системный блок и монитор. После запроса системы необходимо предъявить персональный идентификатор и набрать персональный пароль на клавиатуре.

При отсутствии НСД произойдет загрузка операционной системы Windows. При нарушении или сбое системы защиты от НСД и при отказе загрузки операционной системы - прекратить работу и пригласить администратора безопасности ИСПДн.

Запустить программу антивирусного контроля и проверить жесткий диск и используемые съемные носители на наличие вирусов.

Если во время работы на ПК появилась необходимость временно покинуть рабочее место, исполнитель обязан заблокировать ПК, для чего нужно нажать комбинацию клавиш <Ctrl-Alt-Del> и выбрать в диалоговом окне кнопку «Блокировать». Разблокирование ПК производится набором пароля разблокировки, который был создан при настройке системы блокировки.

8.2 Описание реализованных правил разграничения доступа

Обработка информации осуществляется только на предварительно учтенных носителях информации, прошедших антивирусный контроль, причем

каждый исполнитель для обработки информации использует только свой профиль пользователя, в котором администратором безопасности ИСПДн закреплены правила разграничения доступа: возможность доступа к дискам, папкам и файлам, возможность записи и чтения информации и т.д.

Администратор безопасности ИСПДн организует и контролирует доступ пользователей к ресурсам ИСПДн и состояние информации на носителях.

По окончании рабочего дня все съемные учетные носители информации, документы и материалы запираются в сейфе (металлическом шкафе), либо сдаются на хранение ответственному за защиту информации.

Исполнители обязаны предъявлять по требованию ответственного за защиту информации для проверки все числящиеся за ними носители информации.

8.3 Исполнителю запрещается

- обрабатывать информацию в присутствии посторонних лиц;
- записывать информацию на неучтенные носители информации, листах бумаги и т. д.;
- использовать в работе пароли, если есть подозрение на их компрометацию;
- разглашать сведения о применяемой системе защиты и содержании информации;
- изменять и тиражировать программное обеспечение.

9. Ответственность сотрудников ИСПДн администрации Ленинского района города Нижнего Новгорода

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273, 274 УК РФ).

Администраторы безопасности ИСПДн несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками администрации Ленинского района города Нижнего Новгорода правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников

администрации Ленинского района города Нижнего Новгорода, осуществляющих обработку ПДн в ИСПДн.

Необходимо внести в должностные инструкции сотрудников и руководителей подразделений администрации Ленинского района города Нижнего Новгорода, осуществляющих обработку ПДн в ИСПДн, сведения об ответственности за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

Ответственный за организацию
обработки персональных данных
в администрации Ленинского района

В.В. Лунев

Приложение №2

к приказу исполняющего обязанности
главы администрации
Ленинского района
города Нижнего Новгорода

от "30" мая 2014 № 36

**Правила
обработки персональных данных
в администрации Ленинского района города Нижнего Новгорода**

1. Общие положения

1.1. Настоящие правила обработки персональных данных в администрации Ленинского района города Нижнего Новгорода устанавливают: особенности организации обработки персональных данных с использованием средств автоматизации и без использования средств автоматизации;

сроки обработки и хранения персональных данных;
порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований.

1.2. В правилах используются понятия и термины, определенные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3. В структурных подразделениях администрации Ленинского района города Нижнего Новгорода осуществляется автоматизированная обработка персональных данных, а также обработка персональных данных без использования средств автоматизации.

1.1 Лица, осуществляющие обработку персональных данных, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также под роспись ознакомлены с настоящими правилами, положениями законодательства Российской Федерации, правовыми актами администрации города Нижнего Новгорода о порядке обработки персональных данных и требованиях к обеспечению безопасности персональных данных. Форма соответствующего листа ознакомления приводится в приложении к настоящим правилам.

**2. Особенности обработки персональных данных, осуществляемой
без использования средств автоматизации**

2.1. Порядок обработки персональных данных, осуществляемой без использования средств автоматизации, определяется постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и правовыми актами администрации города Нижнего Новгорода.

2.2. Обработка персональных данных без использования средств автоматизации осуществляется на материальных носителях информации (далее – материальные носители).

2.3. Персональные данные обособляются от иной информации путем фиксации их на отдельных материальных носителях.

2.4. Запрещается оставлять материальные носители без присмотра или передавать на хранение другим лицам, не имеющим на это полномочий.

2.5. Запрещается выносить из служебных помещений материальные носители.

2.6. Учет машинных съемных носителей информации осуществляется путем ведения журналов учета.

2.7. Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

2.8. В случае, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на этом носителе персональных данных или иной информации, принимаются следующие меры:

2.8.1. При необходимости использования или распространения определенных персональных данных осуществляется их копирование с целью последующего использования копии.

2.8.2. При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или копированию.

2.9. Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Особенности обработки персональных данных с использованием средств автоматизации

3.1. Основы обработки персональных данных, осуществляемой с использованием средств автоматизации, определяются Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ 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», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», распоряжением администрации города Нижнего Новгорода от 31.08.2009 № 271-р «Об организации работ по защите персональных данных», а также другими принятыми нормативно-методическими и организационно-распорядительными документами администрации города Нижнего Новгорода.

3.2. В администрации Ленинского района города Нижнего Новгорода один из заместителей главы администрации назначается ответственным за обеспечение безопасности информации ограниченного доступа на объектах вычислительной техники и осуществляет непосредственное руководство работами по защите информации.

3.3. Для обеспечения безопасности персональных данных при их обработке в информационных системах выполняются мероприятия, предусмотренные распоряжением администрации города Нижнего Новгорода от 31.08.2009 № 271-р «Об организации работ по защите персональных данных».

3.4. Лица, ответственные за безопасность персональных данных при их обработке в информационных системах, обеспечивают, в том числе:

3.4.1. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

3.4.2. Недопущение воздействия на программно-аппаратные средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование.

3.4.3. Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа.

3.4.4. Постоянный контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

3.4.5. Знание и соблюдение условий использования средств защиты информации лицами, осуществляющими обработку персональных данных.

3.4.6. Незамедлительное приостановление предоставления доступа к персональным данным лицам, осуществляющим обработку персональных данных, при обнаружении нарушений.

3.4.7. Незамедлительное доведение информации о фактах нарушений функционирования системы защиты информации до руководителя структурного подразделения с целью последующего уведомления лица, ответственного за организацию обработки персональных данных в администрации Ленинского района города Нижнего Новгорода, составление заключений по фактам нарушений.

3.5. Запрещается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

настроенных сертифицированных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств, в соответствии с требованиями безопасности информации;

утвержденных организационно-распорядительных документов по информационной системе персональных данных;

приказа о вводе в эксплуатацию информационной системы персональных данных с назначением ответственных лиц за безопасность информации.

3.6. В информационных системах персональных данных структурных подразделений администрации Ленинского района города Нижнего Новгорода не осуществляется обработка:

биометрических персональных данных;

специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

В случае принятия решения об обработке биометрических персональных данных и специальных категорий персональных данных, такие данные могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных или в случаях, установленных законодательством Российской Федерации.

3.7. Трансграничная передача персональных данных структурными подразделениями администрации Ленинского района города Нижнего Новгорода не осуществляется. В случае принятия решения о трансграничной передаче персональных данных такие данные могут передаваться только при наличии согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных или в случаях, установленных законодательством Российской Федерации, предусматривающих трансграничную передачу персональных данных без письменного согласия субъекта персональных данных.

3.8. Сведения об информационных системах персональных данных структурных подразделений администрации района содержатся в «Сводном перечне информационных систем персональных данных администрации Ленинского района города Нижнего Новгорода, в которых должна быть обеспечена безопасность информации», утверждённом главой администрации района.

4. Сроки обработки и хранения персональных данных

4.1. Сроки обработки персональных данных определяются в соответствии с целью обработки. Персональные данные подлежат уничтожению по достижении цели обработки персональных данных, если иное не предусмотрено федеральным законодательством.

4.2. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

4.3. Сроки обработки и хранения документов, содержащих персональные данные на материальных и электронных носителях определяются «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утверждённого приказом Министерства культуры Российской Федерации от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения».

5. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

5.1. Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2. Лица, осуществляющие обработку персональных данных, в рамках своих полномочий, проводят систематические проверки и выделение документов на бумажных и материальных съёмных носителях, а также данных, хранящихся в информационных системах персональных данных и содержащих персональные данные с истекшими сроками хранения, подлежащих уничтожению.

5.3. Решение об уничтожении документов, содержащих персональные данные, принимают руководители структурных подразделений, в которых осуществляется обработка персональных данных.

По окончании процедуры уничтожения составляется соответствующий акт с указанием даты и основания уничтожения.

Ответственный за организацию
обработки персональных данных
в администрации Ленинского района
города Нижнего Новгорода

В.В. Лунев

Приложение №3

к приказу исполняющего обязанности
главы администрации
Ленинского района
города Нижнего Новгорода

от "30" мая 2014 № 36

**Правила
рассмотрения запросов субъектов персональных данных
или их представителей**

1. Общие положения

1.1. Настоящие правила рассмотрения запросов субъектов персональных данных или их представителей (далее – правила) устанавливают единый порядок регистрации (учета) и рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы) в администрации Ленинского района города Нижнего Новгорода.

1.2. Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Трудовым кодексом Российской Федерации, Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации».

2. Права субъектов персональных данных

Субъект персональных данных имеет право на:

2.1. Получение информации, касающейся обработки его персональных данных, предусмотренной частью 7 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Данное право может быть ограничено в случаях, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.2. Уточнение персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

2.3. Обжалование действий (бездействия) сотрудников администрации Ленинского района города Нижнего Новгорода в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что структурные подразделения осуществляют обработку его персональных данных с нарушением

законодательства Российской Федерации или иным образом нарушают его права и свободы.

2.4. Защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3. Порядок рассмотрения запросов субъектов персональных данных или их представителей

3.1. Сведения, касающиеся обработки персональных данных, предусмотренные частью 7 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», предоставляются субъекту персональных данных или его представителю при направлении ими запроса или обращении в администрацию Ленинского района города Нижнего Новгорода.

3.2. Запрос должен содержать следующие сведения:

фамилию, имя, отчество субъекта персональных данных, а также, в случае направления запроса представителем субъекта персональных данных, его фамилию, имя, отчество;

сведения о документе, удостоверяющем личность субъекта персональных данных или его представителя;

сведения, подтверждающие факт обработки персональных данных администрацией Ленинского района города Нижнего Новгорода;

подпись субъекта персональных данных или его представителя;

доверенность, оформленную в установленном порядке, в случае направления запроса представителем субъекта персональных данных.

3.3. Запрос может быть направлен в электронной форме и подписан электронной подписью в соответствии с законодательством Российской Федерации.

3.4. Запрос регистрируется в течение трех дней со дня его поступления.

3.5. Запросы, поступающие в адрес главы администрации Ленинского района города Нижнего Новгорода, заместителей главы администрации Ленинского района города Нижнего Новгорода, регистрируются сотрудниками отдела документационного обеспечения и работы с обращениями граждан администрации Ленинского района города Нижнего Новгорода и передаются согласно резолюции вышеуказанных лиц в структурные подразделения.

3.6. Запросы, поступающие в адрес руководителей структурных подразделений, регистрируются сотрудниками данных подразделений, ответственными за делопроизводство.

3.7. Сведения по запросу либо отказ в предоставлении сведений направляются субъекту персональных данных или его представителю в срок, не превышающий тридцати дней с даты получения запроса.

3.8. Лицо, осуществляющее подготовку ответа на запрос, обязано:

разобраться в существе запроса, в случае необходимости истребовать дополнительные материалы или осуществить проверку фактов, изложенных в запросе;

принять законные, обоснованные и мотивированные решения и обеспечить их своевременное и надлежащее исполнение;

сообщить субъекту персональных данных или его представителю о решениях, принятых по его запросу, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса разъяснить порядок обжалования этого решения.

3.9. В ответе субъекту персональных данных или его представителю сообщается информация о наличии персональных данных, а также предоставляется возможность ознакомления с персональными данными при личном обращении.

3.10. Отказ в предоставлении информации о наличии персональных данных или в предоставлении возможности ознакомления с персональными данными должен содержать законное основание для такого отказа.

3.11. Сведения предоставляются субъекту персональных данных или его представителю в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких данных.

3.12. Возможность ознакомления с персональными данными предоставляется субъекту персональных данных или его представителю на безвозмездной основе.

3.13. В случае, если сведения были предоставлены для ознакомления субъекту персональных данных или его представителю по его запросу, субъект персональных данных вправе направить повторный запрос не ранее чем через 30 дней после первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого, либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

3.14. Субъект персональных данных вправе направить повторный запрос до истечения срока, указанного в подпункте 3.13., в случае если сведения не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального запроса. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

3.15. Администрация Ленинского района города Нижнего Новгорода и ее структурные подразделения отказывают субъекту персональных данных или его представителю в выполнении повторного запроса, если запрос не соответствует условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», с указанием оснований для отказа.

3.16. В случае предоставления субъектом персональных данных или его представителем сведений о том, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, лицо, обрабатывающее персональные данные, обязано уничтожить такие персональные данные на основании правового акта главы администрации Ленинского района города Нижнего Новгорода.

3.17. В случае поступления сведений о неправомерной обработке персональных данных от субъекта персональных данных, его представителя или уполномоченного органа по защите прав субъектов персональных данных, лицо,

обрабатывающее персональные данные, обязано приостановить обработку неправомерно обрабатываемых персональных данных, с момента получения запроса на период проведения проверки.

3.18. В случае выявления неправомерной обработки персональных данных, лицо, обрабатывающее персональные данные, в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку таких персональных данных. В случае невозможности обеспечения правомерности обработки персональных данных, лицо, обрабатывающее персональные данные, обязано уничтожить такие персональные данные либо обеспечить их уничтожение в установленный законом срок на основании правового акта главы администрации Ленинского района города Нижнего Новгорода. Об устранении допущенных нарушений или об уничтожении персональных данных структурные подразделения обязаны уведомить субъекта персональных данных или его представителя, а также в случае, если запрос был направлен уполномоченным органом по защите прав субъектов персональных данных, уведомить указанный орган.

3.19. В случае предоставления субъектом персональных данных, его представителем либо органом по защите прав субъектов персональных данных сведений о том, что персональные данные субъекта являются неполными, неточными или неактуальными, лицо, обрабатывающее персональные данные, обязано приостановить обработку таких персональных данных с момента получения запроса на период проведения проверки, если это не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.20. В случае подтверждения факта неточности персональных данных, лицо, обрабатывающее персональные данные, на основании сведений, представленных субъектом персональных данных или его представителем, либо уполномоченным органом по защите прав субъектов персональных данных или иных необходимых документов, обязано уточнить персональные данные в срок, не превышающий семи рабочих дней со дня представления сведений, возобновить обработку персональных данных и уведомить субъекта персональных данных или его представителя о внесенных изменениях, а также принять меры для уведомления третьих лиц, которым эти данные были переданы.

3.21. При необходимости, для проверки фактов, изложенных в запросах, организуются служебные проверки в соответствии с правовыми актами администрации города Нижнего Новгорода, администрации Ленинского района города Нижнего Новгорода.

3.22. По результатам служебной проверки составляется мотивированное заключение (акт), которое должно содержать объективный анализ собранных материалов. Если по результатам проверки выявлены факты совершения лицом, осуществляющим обработку персональных данных, действия (бездействия), содержащего признаки административного правонарушения или преступления, материалы передаются в правоохранительные органы. Результаты служебной проверки докладываются лицу, ответственному за организацию обработки персональных данных в администрации Ленинского района города Нижнего Новгорода.

3.23. Запрос считается рассмотренным, если в ответе на запрос рассмотрены все поставленные в нем вопросы, приняты необходимые меры, и субъекту персональных данных или его представителю дан исчерпывающий ответ.

3.24. Лицо, ответственное за организацию обработки персональных данных в администрации Ленинского района города Нижнего Новгорода, осуществляет контроль за соблюдением порядка рассмотрения запросов, а именно за:

- сроком исполнения поручений по запросам;
- полнотой рассмотрения запросов;
- объективностью проверки фактов, изложенных в запросах;
- законностью и обоснованностью принятых решений;
- своевременностью исполнения принятых решений;
- своевременностью направления ответов заявителям.

3.25. Нарушение настоящих правил влечет ответственность, предусмотренную законодательством Российской Федерации.

Ответственный за организацию
обработки персональных данных
в администрации Ленинского района
города Нижнего Новгорода

В.В. Лунев

Приложение №4

к приказу исполняющего обязанности
главы администрации
Ленинского района
города Нижнего Новгорода

от "30" мая 2014 № 36

ПОЛИТИКА
в отношении обработки персональных данных
администрации Ленинского района города Нижнего Новгорода

1. Общие положения.

1.1. Настоящая политика в отношении обработки персональных данных (далее - Политика) в администрации Ленинского района города Нижнего Новгорода разработана в соответствии с частью 2 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Целью Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Политика является общедоступным документом, декларирующим основы деятельности администрации Ленинского района города Нижнего Новгорода, связанной с обработкой персональных данных.

1.4. Действие Политики не распространяется на отношения, возникающие при:

1.4.1. организации хранения, комплектования, учета и использования содержащих персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

1.4.2. обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.5. В Политике используются термины и определения, установленные в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных».

1.6. Администрация Ленинского района города Нижнего Новгорода является оператором, организующим и осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными, в структурных подразделениях администрации.

1.7. Администрация Ленинского района города Нижнего Новгорода включена в Реестр операторов персональных данных за регистрационным номером 10-0085528 от 31.03.1995.

2. Принципы и цели обработки персональных данных, субъекты персональных данных.

2.1. Обработка персональных данных в администрации Ленинского района города Нижнего Новгорода основана на следующих принципах:

2.1.1. Соблюдение законности целей и способов обработки персональных данных.

2.1.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных целей.

2.1.3. Соответствие целей обработки персональных данных целям сбора персональных данных, содержанию и объему обрабатываемых персональных данных.

2.1.4. Недопустимость объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.1.5. Обеспечение точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных.

2.1.6. Выполнение правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке.

2.1.7. Соблюдение прав субъекта персональных данных на доступ к его персональным данным.

2.1.8. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

2.1.9. Уничтожение обрабатываемых персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Целями обработки персональных данных в администрации Ленинского района города Нижнего Новгорода являются:

2.2.1. Исполнение условий трудового договора (служебного контракта) и осуществление прав и обязанностей в соответствии с трудовым законодательством, законодательством о муниципальной службе.

2.2.2. Рассмотрение обращений граждан Российской Федерации в соответствии с законодательством.

2.2.3. Выполнение обязательств по гражданско-правовым договорам (контрактам) и иным соглашениям, заключаемым администрацией Ленинского района города Нижнего Новгорода.

2.2.4. Предоставление муниципальных услуг, реализация полномочий органа местного самоуправления.

2.2.5. Создание общедоступных источников персональных данных.

2.3. Субъектами обработки персональных данных в администрации Ленинского района города Нижнего Новгорода являются:

2.3.1. Граждане, состоящие с администрацией города Нижнего Новгорода в отношениях, регулируемых трудовым законодательством, законодательством о муниципальной службе.

2.3.2. Граждане, являющиеся кандидатами на включение во внешний кадровый резерв администрации города Нижнего Новгорода.

2.3.3. Граждане, обращающиеся в администрацию Ленинского района города Нижнего Новгорода, в том числе с целью получения муниципальных услуг.

2.3.4. Граждане, персональные данные которых обрабатываются в связи с реализацией полномочий органа местного самоуправления, в том числе предоставлением муниципальных услуг.

2.3.5. Граждане, состоящие с администрацией Ленинского района города Нижнего Новгорода, ее структурными подразделениями в гражданско-правовых отношениях.

2.4. Обработка персональных данных осуществляется с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие субъекта персональных данных должно отвечать требованиям, определенным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Обязанности администрации Ленинского района города Нижнего Новгорода при обработке персональных данных.

3.1. Издавать правовые акты по вопросам обработки персональных данных, а также правовые акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации и иных нормативных правовых актов, связанных с обработкой персональных данных, устранение последствий таких нарушений.

3.2. Определять состав и перечень правовых, организационных и технических мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

3.3. Назначать лицо, ответственное за организацию обработки персональных данных в администрации Ленинского района города Нижнего Новгорода, которое, в частности:

3.3.1. получает указания непосредственно от главы администрации Ленинского района города Нижнего Новгорода и подотчетно ему;

3.3.2. осуществляет внутренний контроль за соблюдением законодательства Российской Федерации и иных нормативных правовых актов о персональных данных, в том числе требований к защите персональных данных;

3.3.3. обеспечивает доведение до сведения сотрудников положений законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, правовых актов администрации

города Нижнего Новгорода, администрации Ленинского района города Нижнего Новгорода по вопросам обработки персональных данных;

3.3.4. организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль за приемом и обработкой таких обращений и запросов.

3.4. Обеспечивать выполнение лицами, осуществляющими обработку персональных данных и лицами, имеющими доступ к персональным данным, требований по защите персональных данных, установленных нормативными правовыми актами.

3.5. Обеспечивать конфиденциальность персональных данных, обрабатываемых в структурных подразделениях, кроме общедоступных персональных данных и случаев обезличивания персональных данных, если иное не предусмотрено федеральным законом.

3.6. Принимать меры по обеспечению безопасности персональных данных при их обработке в структурных подразделениях.

3.7. Не допускать обработку и приобщение к личному делу субъекта персональных данных сведений, касающихся состояния здоровья, расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, членства в общественных объединениях или его профсоюзной деятельности, если иное не предусмотрено федеральным законом.

3.8. Обеспечивать уничтожение персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.9. Выполнять иные требования в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

4. Порядок доступа к персональным данным и их предоставления.

4.1. К обработке персональных данных допускаются сотрудники структурных подразделений, должностными инструкциями которых предусмотрено выполнение обязанностей по обработке персональных данных.

4.2. Предоставление доступа сотрудникам структурных подразделений к персональным данным осуществляется на основании перечня должностей служащих, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, утвержденного руководителем администрации Ленинского района города Нижнего Новгорода.

4.3. Руководитель структурного подразделения при организации доступа сотрудника к персональным данным обязан ознакомить его с требованиями федерального законодательства и правовых актов администрации города Нижнего Новгорода, администрации Ленинского района города Нижнего Новгорода к обработке персональных данных и обеспечению безопасности персональных данных под роспись.

4.4. Лицам, допущенным к обработке персональных данных, предоставляется доступ только к персональным данным, необходимым для выполнения их служебных обязанностей в пределах задач и функций соответствующих структурных подразделений.

4.5. Каждое лицо, допущенное к автоматизированной обработке персональных данных, использует индивидуальный идентификатор и пароль, которые не имеет права передавать другим лицам.

4.6. Структурные подразделения администрации Ленинского района города Нижнего Новгорода вправе передавать (распространять, предоставлять, давать доступ) персональные данные третьим лицам с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора либо путем принятия администрацией Ленинского района города Нижнего Новгорода правового акта. В правовом акте должны быть определены перечень действий (операций) с персональными данными и цели их обработки, должна быть установлена обязанность лица, которому предоставлены персональные данные, соблюдать конфиденциальность и обеспечивать безопасность персональных данных, а также должны быть указаны требования к их защите в соответствии с Федеральным законом от 27.07.2006 № 152 «О персональных данных».

4.7. Основанием для отказа в предоставлении персональных данных третьим лицам являются:

4.7.1. Отсутствие согласия субъекта персональных данных.

4.7.2. Отсутствие условий, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», при которых согласие субъекта персональных данных не требуется.

5. Организация защиты персональных данных.

5.1. Персональные данные относятся к сведениям ограниченного доступа и подлежат защите в рамках функционирующей в администрации Ленинского района города Нижнего Новгорода системы защиты информации.

5.2. При организации защиты персональных данных при их обработке администрация Ленинского района города Нижнего Новгорода руководствуется, в том числе, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», распоряжением администрации города Нижнего

Новгорода от 31.08.2009 № 271-р «Об организации работ по защите персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», распоряжением администрации города Нижнего Новгорода от 04.04.2008 № 155-р «О назначении ответственных за обеспечение безопасности информации в структурных подразделениях администрации города и администрациях районов города Нижнего Новгорода».

5.3. Субъектами отношений при организации системы защиты для обеспечения безопасности персональных данных при их обработке в структурных подразделениях (далее – субъекты информационных отношений) являются:

администрация Ленинского района города Нижнего Новгорода как оператор, осуществляющий обработку персональных данных;

сотрудники структурных подразделений, допущенные к обработке персональных данных, в соответствии с возложенными на них полномочиями и функциями.

5.4. Под безопасностью информации понимают состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

5.5. Задачами системы защиты персональных данных являются исключение или минимизация ущерба от возможной реализации случайных или злонамеренных воздействий на персональные данные, а также прогнозирование и предотвращение таких воздействий.

5.6. Меры, принимаемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, подразделяются на правовые, организационные и технические.

5.6.1. К правовым мерам защиты персональных данных относится принятие правовых актов администрации города Нижнего Новгорода и администрации Ленинского района города Нижнего Новгорода в соответствии с федеральными законами в области защиты персональных данных и принятыми в их исполнение нормативными документами, закрепляющих права и обязанности субъектов информационных отношений в процессе обработки персональных данных, а также устанавливающих ответственность за нарушение этих правил.

5.6.2. К организационным мерам защиты персональных данных относятся, в том числе:

5.6.2.1. Назначение в структурных подразделениях ответственных за обеспечение безопасности информации.

5.6.2.2. Разработка и поддержание в актуальном состоянии организационно-распорядительных документов, регламентирующих порядок обработки персональных данных, создания и функционирования системы защиты персональных данных.

5.6.2.3. Организация деятельности субъектов информационных отношений, в том числе:

установление перечня должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

информирование лиц, осуществляющих обработку персональных данных, о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

обеспечение раздельной фиксации на материальных носителях персональных данных, имеющих различную цель обработки, или их раздельной обработки;

обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5.6.2.4. Осуществление внутреннего контроля соответствия обработки и безопасности персональных данных в администрации Ленинского района города Нижнего Новгорода требованиям законодательства Российской Федерации и иных нормативных правовых актов о персональных данных, в том числе требованиям к защите персональных данных.

5.6.2.5. Проведение мероприятий по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с персональными данными.

5.6.2.6. Обучение, периодическое повышение квалификации сотрудников, ответственных за организацию обработки и обеспечение безопасности информации, сотрудников, непосредственно выполняющих мероприятия по обеспечению безопасности персональных данных.

5.6.3. К техническим мерам защиты относится использование программно-аппаратных средств, выполняющих самостоятельно или в комплексе с другими средствами функции защиты персональных данных, и методов защиты, в том числе:

программной или программно-технической защиты от несанкционированного доступа к информационным ресурсам автоматизированных рабочих мест, на которых обрабатываются персональные данные;

программно-технических средств, позволяющих восстанавливать персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;

средств защиты персональных данных от утечки по техническим каналам при их обработке, хранении и передаче по каналам связи;

средств межсетевого экранирования при подключении автоматизированных рабочих мест к локальным сетям общего пользования или к сети Интернет;

криптографических средств защиты информации;
средств защиты от вредоносного программного обеспечения.

5.7. В структурных подразделениях применяются сертифицированные средства защиты информации, соответствующие требованиям, установленным уполномоченными органами в области технической защиты информации.

5.8. В случае принятия решения о проведении работ по обезличиванию персональных данных разрабатываются правила работы с обезличенными данными в соответствии с приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

5.9. Лицо, ответственное за организацию обработки персональных данных в администрации Ленинского района города Нижнего Новгорода, при обеспечении безопасности персональных данных, в частности, вправе:

иметь доступ к информации, касающейся обработки персональных данных;

привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в структурных подразделениях, сотрудников с возложением на них соответствующих обязанностей и закреплением ответственности.

6. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.

6.1. Ответственный за организацию обработки персональных данных в администрации Ленинского района города Нижнего Новгорода несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в структурных подразделениях в соответствии с законодательством Российской Федерации и иными нормативными правовыми актами в области персональных данных.

6.2. Лица, осуществляющие обработку персональных данных в структурных подразделениях администрации Ленинского района города Нижнего Новгорода в соответствии со своими полномочиями, несут гражданско-правовую, уголовную, административную, дисциплинарную ответственность за нарушение требований к обработке и защите персональных данных, предусмотренную законодательством Российской Федерации.

Ответственный за организацию
обработки персональных данных
в администрации Ленинского района

В.В. Лунев

Приложение №5

к приказу исполняющего обязанности
главы администрации
Ленинского района
города Нижнего Новгорода

от "30" мая 2014 № 36

ПОРЯДОК**доступа служащих администрации Ленинского района города Нижнего
Новгорода в помещения, в которых ведется обработка персональных
данных.**

1. Настоящий Порядок доступа служащих администрации Ленинского района города Нижнего Новгорода в помещения, в которых ведется обработка персональных данных (далее - Порядок), устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в администрации Ленинского района города Нижнего Новгорода и обеспечения соблюдения требований законодательства о персональных данных.

2. В помещениях, в которых ведется обработка персональных данных (далее - помещения), должна обеспечиваться сохранность информации и технических средств, с помощью которых ведется обработка персональных данных.

3. Помещения должны использоваться строго по назначению.

4. Доступ в помещения осуществляется согласно утвержденному главой администрации Ленинского района города Нижнего Новгорода списку служащих, допущенных в помещения (далее - служащие, имеющие допуск в помещения).

5. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка или иное выполнение работ (оказание услуг) в помещениях осуществляются только в присутствии служащих, имеющих допуск в помещение, которые обязаны принять меры по исключению возможности ознакомления сотрудников обслуживающих организаций с обрабатываемыми персональными данными.

6. Возможность бесконтрольного проникновения и пребывания посторонних лиц в помещениях должна быть исключена.

7. Сотрудники администрации Ленинского района города Нижнего Новгорода, не включенные в список, указанный в пункте 4 Порядка, а также посетители, прибывшие по служебной необходимости, допускаются в помещения с разрешения и находятся в помещениях в присутствии служащих, имеющих допуск в помещения, которые обязаны принять меры по исключению

возможности ознакомления прибывших лиц с обрабатываемыми персональными данными.

8. Помещения должны быть оснащены дверями, оборудованными запорными устройствами. В нерабочее время двери и окна помещений должны находиться в закрытом состоянии.

9. Материальные носители персональных данных (бумажные и электронные) должны храниться в запираемых шкафах, сейфах или тумбах.

10. Служащим, имеющим допуск в помещения, запрещается передавать ключи от помещений посторонним лицам. В случае утраты ключей от помещения запорное устройство должно быть немедленно заменено.

11. Открытие и закрытие помещений осуществляется служащими, имеющими допуск в помещение.

12. Перед закрытием помещений по окончании рабочего времени служащие, имеющие допуск в помещение, обязаны:

-убрать бумажные и электронные носители персональных данных в запираемые шкафы, сейфы или тумбы;

-отключить технические средства, кроме постоянно действующих, и электрические приборы;

-закрыть окна.

13. Перед открытием помещений служащие, имеющие допуск в помещение, обязаны провести внешний осмотр с целью установления целостности двери и запорного устройства, открыть дверь, осмотреть помещение.

14. При обнаружении повреждений запорных устройств или других признаков, указывающих на возможное проникновение в помещение, служащие, имеющие допуск в помещения, обязаны, не открывая помещения, составить акт о выявленных нарушениях и передать его на рассмотрение ответственному за организацию обработки персональных данных в администрации Ленинского района города Нижнего Новгорода.

15. Текущий внутренний контроль за соблюдением Порядка осуществляется ответственным за организацию работы по обработке персональных данных в администрации Ленинского района города Нижнего Новгорода.

Ответственный за организацию
обработки персональных данных
в администрации Ленинского района
города Нижнего Новгорода

В.В. Лунев

Приложение №6

к приказу исполняющего обязанности
главы администрации
Ленинского района
города Нижнего Новгорода

от "30" мая 2014 № 36

**Правила
осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных
в администрации Ленинского района города Нижнего Новгорода**

1. Общие положения.

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - правила), установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятые в соответствии с ним нормативные правовые акты, правовые акты администрации города Нижнего Новгорода и администрации Ленинского района города Нижнего Новгорода (далее – администрация района), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», правовыми актами администрации города Нижнего Новгорода и администрации района.

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

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных, администрация района организует проведение проверок соответствия обработки персональных данных установленным требованиям к защите персональных данных (далее – проверки) в структурных подразделениях администрации района.

2.2. Проверки осуществляются постоянно действующей комиссией по контролю соответствия обработки персональных данных установленным требованиям в структурных подразделениях администрации района (далее – Комиссия), состав которой утверждается приказом главы администрации района.

2.3. Проверки проводятся на основании:

2.3.1. Утвержденного ответственным за организацию обработки персональных данных в администрации района ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (плановые проверки);

2.3.2. Поступившего в администрацию района письменного заявления о нарушении выполнения требований к защите персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение 5 рабочих дней со дня регистрации соответствующего заявления.

2.4. В ходе проверки проводится полная, объективная и всесторонняя оценка:

2.4.1. Наличия и актуальности правовых и организационно-распорядительных документов, утверждаемых в соответствии с правовыми актами администрации района в области обработки персональных данных.

2.4.2. Информирования лиц, осуществляющих обработку персональных данных, о положениях законодательства Российской Федерации, правовых актах администрации города Нижнего Новгорода, администрации района о порядке обработки персональных данных и требованиях к обеспечению безопасности персональных данных.

2.4.3. Соответствия перечня служащих, фактически осуществляющих обработку персональных данных и имеющих доступ к персональным данным, утвержденному администрацией района либо администрацией города Нижнего Новгорода, перечню служащих, замещение должностей которых предусматривает осуществление обработки персональных данных.

2.4.4. Соблюдения установленного порядка доступа служащих структурных подразделений администрации района в помещения, в которых ведется обработка персональных данных.

2.4.5. Соблюдения сроков обработки и хранения персональных данных.

2.4.6. Соответствия обрабатываемых персональных данных, утвержденных администрацией района либо администрацией города Нижнего Новгорода,

перечням персональных данных, обрабатываемых в структурных подразделениях администрации района в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием муниципальных услуг, осуществлением муниципальных функций и исполнением отдельных государственных полномочий.

2.4.7. Соблюдения правил обработки персональных данных, осуществляемых без использования средств автоматизации, в том числе:

-раздельного хранения персональных данных, обработка которых осуществляется в разных целях;

-соответствия фактических мест хранения материальных носителей персональных данных местам хранения материальных носителей персональных данных, утвержденным правовым актом администрации района;

-состояния учета машинных съемных носителей информации.

2.4.8. Соблюдения правил обработки персональных данных в информационных системах для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных, в том числе применения технических мер:

-использования сертифицированных средств защиты информации и соблюдения условий их использования лицами, осуществляющими обработку персональных данных;

-наличия возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных в случае несанкционированного доступа.

2.5. Проверка должна быть завершена не позднее чем через 5 дней со дня начала проверки.

2.6. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений (в случае их наличия), в течение 5 рабочих дней со дня завершения проверки составляется акт. Акт подписывается всеми членами Комиссии и направляется руководителю структурного подразделения администрации района, в котором проводилась проверка. Акт должен содержать описание нарушений, в случае их наличия, и рекомендации по их устранению.

2.7. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений (в случае их наличия), главе администрации района докладывает ответственный за организацию обработки персональных данных в администрации района.

На основании результатов проведенной проверки при обнаружении фактов осуществления обработки персональных данных с нарушением требований законодательства Российской Федерации, ответственный за организацию обработки персональных данных в администрации района принимает решение о приостановлении или прекращении обработки персональных данных либо, в случае невозможности устранения нарушений (обеспечения правомерности обработки), об уничтожении таких персональных данных.

2.8. Члены Комиссии обязаны соблюдать конфиденциальность информации ограниченного доступа, ставшей известной им в ходе проведения проверки.

Ответственный за организацию
обработки персональных данных
в администрации Ленинского района
города Нижнего Новгорода

В.В. Лунев

Приложение №7

к приказу исполняющего обязанности
главы администрации
Ленинского района
города Нижнего Новгорода

от "30" мая 2014 № 36

Положение
о комиссии по контролю соответствия обработки персональных данных
установленным требованиям к защите персональных данных
в администрации Ленинского района города Нижнего Новгорода

1. Общие положения

1.1. Настоящее Положение определяет задачи, полномочия, порядок образования и деятельности комиссии по контролю соответствия обработки персональных данных установленным требованиям к защите персональных данных в администрации района, (далее – Комиссия).

1.2. Комиссия является постоянно действующим органом, образованным в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», подпунктом д) пункта 1 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 и муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 21.03.2012 № 211, постановлением администрации города Нижнего Новгорода от 04.02.2014 № 269 «Об организации обработки персональных данных в администрации города Нижнего Новгорода».

1.3. Комиссия в своей деятельности подотчетна главе администрации района.

1.4. Комиссия в своей работе руководствуется Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств

автоматизации», постановлением администрации города Нижнего Новгорода от 04.02.2014 № 269 «Об организации обработки персональных данных в администрации города Нижнего Новгорода», другими нормативными актами в области защиты персональных данных и настоящим Положением.

1.5. Задачами Комиссии являются:

1.5.1. определение соответствия обработки персональных данных установленным требованиям к защите персональных данных;

1.5.2. выявление нарушений требований к защите персональных данных;

1.5.3. подготовка рекомендаций о мерах, необходимых для устранения нарушений в случае их выявления.

2. Порядок образования Комиссии

2.1. Состав Комиссии утверждается приказом главы администрации района. Комиссия состоит из 5 членов.

2.2. В состав Комиссии включаются:

председатель Комиссии - заместитель главы администрации района, ответственный за организацию обработки персональных данных в администрации района;

заместитель председателя Комиссии из числа руководителей структурных подразделений администрации района;

3 члена Комиссии из числа руководителей или сотрудников структурных подразделений администрации района.

3. Полномочия Комиссии

3.1. В целях выполнения возложенных на нее задач, Комиссия:

3.1.1. Готовит ежегодный план осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных (плановых проверок) и представляет его на утверждение ответственному за организацию обработки персональных данных.

3.1.2. Организует и проводит плановые, а на основании поступившего в администрацию района письменного заявления о нарушении выполнения требований к защите персональных данных - внеплановые проверки, в соответствии с утвержденными в администрации района правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

3.1.3. Готовит акт по итогам проведенной проверки соответствия обработки персональных данных установленным требованиям, содержащий описание нарушений, в случае их наличия, и рекомендации по устранению.

3.1.4. Готовит рекомендации о приостановлении или прекращении обработки персональных данных, осуществляемой с нарушением требований действующего законодательства.

3.2. Председатель Комиссии и его заместитель при проведении проверки имеют право:

3.2.1. Запрашивать у структурных подразделений администрации района информацию, необходимую для осуществления проверки, а также копии правовых актов и организационно-распорядительных документов.

3.2.2. Привлекать сотрудников структурных подразделений администрации района, имеющих непосредственное отношение к предмету проверки, к участию в проверке, в том числе получать их объяснения по вопросам, относящимся к предмету проверок.

3.2.3. Требовать от лиц, обрабатывающих персональные данные в структурных подразделениях администрации района, обеспечения в установленном порядке уточнения или блокирования недостоверных или неправомерно обрабатываемых персональных данных до принятия решения ответственным за организацию обработки персональных данных в структурных подразделениях администрации района об обеспечении правомерности обработки персональных данных либо об уничтожении таких персональных данных.

3.2.4. Направлять главе администрации района предложения о совершенствовании правовых, организационных и технических мер, принимаемых для защиты персональных данных.

4. Организация работы Комиссии

4.1. Заседания Комиссии проводятся по мере необходимости.

4.2. Комиссия правомочна осуществлять свои функции, если в ее работе участвует не менее половины ее членов, включая председателя Комиссии и заместителя председателя Комиссии.

4.3. Все члены Комиссии пользуются равными правами в решении всех вопросов, рассматриваемых на заседании Комиссии.

4.4. Члены Комиссии обязаны соблюдать конфиденциальность информации ограниченного доступа, ставшей известной им в ходе проведения проверки.

4.5. В отсутствие председателя Комиссии его функции осуществляет заместитель председателя Комиссии.

Ответственный за организацию
обработки персональных данных
в администрации Ленинского района
города Нижнего Новгорода

В.В. Лунев