

**АДМИНИСТРАЦИЯ НЕВЬЯНСКОГО ГОРОДСКОГО ОКРУГА**

**РАСПОРЯЖЕНИЕ**

**от 16.01.2019 № 5 - р**

 г. Невьянск

*О работе с персональными данными*

*в администрации Невьянского городского округа*

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года № 149-ФЗ
«Об информации, информационных технологиях и о защите информации», 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», с целью защиты прав и свобод граждан Российской Федерации, предоставляющих администрации Невьянского городского округа свои персональные данные для обработки и хранения, руководствуясь Уставом Невьянского городского округа:

1. Утвердить [Положение](#P265) о работе с персональными данными в администрации Невьянского городского округа (прилагается).

2. Контроль за исполнением настоящего распоряжения и ответственность за работу с персональными данными возлагается на руководителей структурных подразделений и заместителей главы администрации Невьянского городского округа, курирующих соответствующее направление.

3. Управлению делами администрации Невьянского городского округа ознакомить сотрудников администрации Невьянского городского округа с настоящим распоряжением.

4. Разместить настоящее распоряжение на официальном сайте Невьянского городского округа в информационно-телекоммуникационной сети «Интернет».

Глава Невьянского

городского округа А.А. Берчук

 УТВЕРЖДЕНО

 распоряжением администрации

 Невьянского городского округа

 от \_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_\_\_\_

ПОЛОЖЕНИЕ

о работе с персональными данными

в администрации Невьянского городского округа

1. Общие положения

1. Настоящее Положение о работе с персональными данными в администрации Невьянского городского округа (далее - Положение) разработано в соответствии с частью 1 статьи 23, статьи 24 Конституции Российской Федерации, Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и определяет порядок организации работ по обеспечению безопасности персональных данных (далее – персональные данные) при их обработке в администрации Невьянского городского округа (далее - Администрация) и устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

2. Положение распространяется на физических лиц и представителей юридических лиц (субъект персональных данных), обратившихся в Администрацию.

3. Цель данного Положения:

1) определение основных принципов построения системы защиты персональных данных в Администрации;

2) определение основных мер защиты и областей ее внедрения для обеспечения выполнения федерального законодательства, требования и рекомендаций национальных и международных стандартов в области информационной безопасности персональных данных;

3) обеспечение прав и свобод человека и гражданина при обработке его персональных данных.

 2. Понятие персональных данных

4. В соответствии с пунктом 1 статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» под персональными данными субъекта (далее - персональные данные) понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

3. Права субъектов персональных данных

5. Субъект персональных данных вправе требовать от Администрации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6. Для реализации вышеуказанных прав субъект персональных данных, может в порядке, установленном статьей 14 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», обратиться в Администрацию с соответствующим запросом.

7. Если субъект персональных данных считает, что Администрация осуществляет обработку его персональных данных с нарушением требований Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Администрации в вышестоящий орган, в органы прокуратуры или в судебном порядке.

4. Передача персональных данных

8. Администрация не предоставляет и не раскрывает сведения, содержащие персональные данные субъектов персональных данных, третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами.

5. Методы и способы защиты персональных данных

9. Методы и способы защиты персональных данных определяются в соответствии с требованиями статей 18.1, 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119  «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

10. Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

11. Администрация при защите персональных данных субъектов принимает все необходимые организационно-распорядительные, юридические и технические меры, в том числе:

– шифровальные (криптографические) средства;

– антивирусная защита;

– анализ защищенности;

– обнаружение и предотвращение вторжений;

– управление доступом;

– использование систем контроля и управления доступом (СКУД);

– учет ключей, электронных ключей доступа;

– использование систем охранной сигнализации;

– использование систем видеонаблюдения;

– конструктивное усиление окон, дверей, стен и иных преград для исключения угрозы несанкционированного доступа.

– регистрация и учет документов;

– предотвращение несанкционированного доступа к персональным данным, обрабатываемых в информационных системах персональных данных;

– организация непрерывного и защищенного процесса обработки, хранения, передачи информации, содержащей персональные данные;

– в ходе эксплуатации систем, связанных с СМЭВ, обеспечивается шифрование передаваемой информации;

– разработка нормативно-методических локальных актов, регулирующих защиту персональных данных.

6. Организация безопасности

12. Информационная безопасность персональных данных должна обеспечиваться на всех этапах обработки информации и во всех режимах функционирования.

12.1. Основными направлениями политики информационной безопасности являются:

– соблюдение прав и свобод граждан Российской Федерации;

– соблюдение юридических норм Российской Федерации;

– обеспечение безопасности (конфиденциальности) данных;

– обеспечение непрерывного и корректного процесса обработки персональных данных, сохранение их целостности, корректности и доступности.

12.2. Информационная безопасность персональных данных основывается на следующих принципах:

1) принцип системности - системный подход к защите компьютерных систем предполагает необходимость взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов при всех видах информационной деятельности и информационного проявления. При обеспечении информационной безопасности информационных систем необходимо учитывать все слабые и наиболее уязвимые места системы, а также характер, возможные объекты и направления атак на систему со стороны нарушителя, пути проникновения распределенной системы и несанкционированного доступа к информации;

2) принцип комплексности - для обеспечения защиты имеется широкий спектр мер, методов и средств защиты компьютерных систем. Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающие все существующие каналы угроз и не содержащие слабых мест на стыках отдельных ее компонентов;

3) принцип непрерывности защиты - защита информации - это не разовое мероприятие и не конкретная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный направленный процесс предполагающий принятие соответствующих мер на всех этапах существования информационной системы. Разработка системы защиты должна вестись параллельно обработке самой защищаемой системы;

4) разумная достаточность - важно правильно выбрать тот уровень защиты при котором затраты, риск и размер возможного ущерба были бы приемлемы и не создавали неудобств пользователю;

5) гибкость системы защиты - часто приходится создавать систему защиты в условиях большой неопределенности, поэтому принятые меры и средства защиты особенно в начальный период их эксплуатации могут оказывать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения уровня варьирования защищенности средство защиты должно обладать определенной гибкостью, особенно если средство необходимо установить на работающую систему не нарушая процесса ее нормального функционирования;

6) принцип простоты применения средств защиты - механизмы защиты должны быть интуитивно понятны и просты в применении. Применение средств защиты не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на ее применение, а также не должно требовать выполнения рутинных малопонятных операций.

13. Любые инциденты безопасности должны сообщаться сотрудниками Администрации руководителю структурного подразделения***.*** По каждому сообщению руководитель структурного подразделения принимает соответствующие меры.

Инциденты безопасности:

– факты попыток и успешной реализации несанкционированного доступа в системы обработки информации, в помещения обработки информации и к хранилищам информации;

– факты сбоя или некорректной работы систем обработки информации;

– факты сбоя или некорректной работы средств защиты информации;

– факты разглашения информации, содержащей персональные данные;

– факты разглашения информации о методах и способах защиты и обработки информации, содержащей персональные данные.

14. Безопасность средств обработки обеспечивается организационными и техническими средствами и мерами:

1) организационными мерами осуществляется допуск работников Администрации и третьих лиц (в соответствии с действующим законодательством), при этом минимизируется круг лиц, имеющих доступ к персональным данным.

2) техническая безопасность обеспечивается корректной настройкой средств обработки информации и установкой наложенных средств защиты информации.

15. Обработка документов осуществляется в строгом соответствии с настоящим Положением и правовыми актами (административными регламентами), принятыми в Администрации.

16. Материальные носители информации должны храниться в сейфах или шкафах.

17. Все электронные носители информации должны быть промаркированы (возможно использование заводской маркировки) и перечислены в журнале учета.

7. Ответственность

18. Все сотрудники, работающие в Администрации, в связи с выполнением своих должностных обязанностей, имеют доступ (прямой или косвенный) к персональным данным, к обработке информации и хранилищам, содержащим персональные данные, и несут ответственность (дисциплинарную, административную, гражданско-правовую, уголовную) в случае нарушения норм и требований действующего законодательства, регулирующего правила обработки и защиты персональных данных.

19. Непосредственно субъект персональных данных отвечает за корректность своих данных, за соблюдение установленного порядка и мер по обеспечению безопасности персональных данных и самолично отвечает за разглашение информации конфиденциального характера, ставшей известной ему.