МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ ГОРОД НОЯБРЬСК

АДМИНИСТРАЦИЯ

Д Е П А Р Т А М Е Н Т Ф И Н А Н С О В

П Р И К А З

29 февраля 2016 года **№ 46**

По основной деятельности

Об утверждении Политики в отношении обработки персональных данных в департаменте финансов Администрации города Ноябрьска

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановления 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», руководствуясь Положением о департаменте финансов Администрации города Ноябрьска, утвержденным постановлением Администрации города от 03.03.2014 № П-195, **п р и к а з ы в а ю :**

1. Утвердить Политику в отношении обработки персональных данных в департаменте финансов Администрации города Ноябрьска согласно приложению к настоящему приказу.
2. Признать утратившим силу приказ департамента финансов Администрации города Ноябрьска от 28.06.2013 № 94 «Об утверждении Политики защиты персональных данных в информационных системах персональных данных департамента финансов Администрации города Ноябрьска».
3. Управлению правового обеспечения, кадровой работы и делопроизводства (Фицева Ю.В.) обеспечить размещение настоящего приказа на официальном сайте Администрации города Ноябрьска admnoyabrsk.ru в информационно-телекоммуникационной сети «Интернет».
4. Контроль за исполнением настоящего приказа возложить на заместителя начальника департамента, начальника управления доходов, долговой политики и программного обеспечения Ю.А. Винницкую, на начальника управления правового обеспечения, кадровой работы и делопроизводства Ю.В. Фицеву, на начальника управления казначейского исполнения бюджета, главного бухгалтера О.В. Панченко.

Заместитель Главы Администрации,
начальник департамента **Г.В. Жегальская**

Приложение
к приказу департамента финансов
от 29 февраля 2016 года № 46

Политика в отношении обработки персональных данных в департаменте финансов Администрации города Ноябрьска

1. Общие положения

1.1. Настоящий документ определяет политику департамента финансов Администрации города Ноябрьска (далее – департамент финансов) в отношении обработки персональных данных (далее – Политика), является общедоступным и декларирует концептуальные основы деятельности департамента финансов при обработке персональных данных.

1.2. При утверждении настоящей Политики департамент финансов считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение надлежащего уровня безопасности обрабатываемых в департаменте финансов персональных данных.

1.3. Действие настоящей Политики распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению, извлечению, использованию, передаче (распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению персональных данных, осуществляемых с использованием средств автоматизации и без использования средств автоматизации.

1.4. Департамент финансов при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, удаления, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

2. Термины, определения и принятые сокращения

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

2.2. Администратор АС - лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

2.3. Администратор защиты (безопасности) информации – лицо, ответственное за защиту АС от несанкционированного доступа к информации.

2.4. Безопасность информации - состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

2.5. Доступ к информации (доступ) - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

2.6. Защита информации от несанкционированного доступа (далее - защита от НСД) или воздействия - деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

2.7. Информационная система (далее – ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

2.8. Информационная система персональных данных (далее – 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.

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

2.10. Линии связи - линии передачи, физические цепи и линейно-кабельные сооружения связи.

2.11. Нарушитель безопасности персональных данных - физическое лицо или организация, случайно или преднамеренно совершающие действия, следствием которых является нарушение заданных характеристик безопасности персональных данных.

2.12. Обработка персональных данных – любые действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации (в том числе, с помощью средств вычислительной техники) или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передаче (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

2.14. Система защиты персональных данных (далее – СЗПДн) - совокупность организационных и технических мер защиты информации, направленных на предотвращение несанкционированного доступа к персональным данным, информационным системам персональных данных.

3. Основные цели и задачи обеспечения безопасности ПДн

3.1. Основной целью обеспечения безопасности ПДн является минимизация ущерба (как непосредственного, так и опосредованного), возникающего вследствие возможной реализации угроз безопасности ПДн.

3.2. Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту ПДн и может проявляться в виде:

3.2.1. нанесения вреда здоровью субъекта ПДн;

3.2.2. незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта ПДн;

3.2.3. потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием его ПДн;

3.2.4. нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь.

3.3. Опосредованный ущерб связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с ПДн.

3.4. Основной задачей обеспечения безопасности ПДн при их обработке в департаменте финансов является предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, копирования, блокирования, предоставления, распространения, утечки ПДн по

техническим каналам, предупреждение преднамеренных программно-технических воздействий с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения, а также иных неправомерных действий в отношении ПДн.

4. Объекты защиты ПДн

4.1. Объектами защиты ПДн в департаменте финансов являются:

4.1.1. ПДн, хранящиеся в документированном виде на бумажных носителях;

4.1.2. ПДн, обрабатываемые и хранящиеся на серверах, на автоматизированных рабочих местах (далее – АРМ) пользователей, на отчуждаемых (съемных) носителях информации;

4.1.3. ПДн, передаваемые по каналам и линиям связи;

4.1.4. прикладное и системное программное обеспечение серверов, АРМ, используемых для обработки ПДн;

4.1.5. аппаратные средства программно-технических комплексов, оборудование серверов, АРМ, используемых для обработки ПДн;

4.1.6. средства защиты информации ИСПДн;

4.1.7. съемные (отчуждаемые) машинные носители информации – накопители на гибких и жестких магнитных дисках, Flash-накопители (CD-R, CD-RW, DVD-R, DVD-RV).

5. Категории субъектов ПДн

5.1. Субъектами ПДн, которые обрабатываются в департаменте финансов являются:

5.1.1. физические лица, состоящие (состоявшие) в трудовых отношениях с департаментом финансов;

5.1.2. физические лица, состоящие (состоявшие) в договорных отношениях с департаментом финансов;

5.1.3. физические лица, обратившиеся в департамент финансов с целью заключения договора, в том числе трудового, получения информации;

5.1.4. иные физические лица, чьи персональные данные обрабатываются департаментом финансов в соответствии с требованиями действующего законодательства Российской Федерации;

5.1.5. представители физических лиц, указанных в пунктах 5.1.1 - 5.1.4.

6. Категории ПДн субъектов ПДн

6.1. Состав ПДн, обрабатываемых в департаменте финансов, должен соответствовать принципу их достаточности для достижения целей обработки (ПДн не должны быть избыточными по отношению к целям их обработки).

7. Меры по обеспечению безопасности ПДн при их обработке

7.1. Превентивные методы противодействия угрозам безопасности ПДн осуществляются на основе эффективного применения в процессе обработки ПДн и эксплуатации ИСПДн комплекса организационных и технических мероприятий, а также методов и средств обеспечения функциональной устойчивости и безопасности работы ИСПДн.

7.2. Организационные мероприятия по обеспечению безопасности ПДн являются мероприятиями общего характера по организации деятельности персонала, допущенного к обработке ПДн и эксплуатирующего ИСПДн, принятие необходимых локальных правовых актов.

7.3. Технические мероприятия по обеспечению безопасности ПДн заключаются в обслуживании, поддержании и управлении требуемым составом технических средств, обеспечивающих обработку ПДн в защищенном режиме.

7.4. Обеспечение безопасности персональных данных достигается, в частности:

7.4.1. назначением лиц, ответственных за организацию обработки персональных данных и обеспечение их безопасности;

7.4.2. осуществлением внутреннего контроля соответствия обработки ПДн требованиям к зашите ПДн, утвержденным Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним локальным актам;

7.4.3. ознакомлением работников, ответственных за организацию обработки ПДн и обеспечение безопасности ПДн, и работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о персональных данных, локальными актами и (или) обучением указанных работников.

7.4.4. строгим учетом всех подлежащих защите ресурсов (ПДн, сервисов, каналов связи, серверов, АРМ и т.д.);

7.4.5. установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

7.4.6. предотвращением несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

7.4.7. своевременным обнаружением фактов НСД к ПДн;

7.4.8. недопущением воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

7.4.9. возможностью незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

7.4.10. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

7.4.11. определением угроз безопасности ПДн при их обработке в ИСПДн;

7.4.12. постоянным контролем за обеспечением уровня защищенности ПДн и ИСПДн.

8. Общие характеристики ИСПДн

8.1. По структуре ИСПДн департамента финансов являются локальными информационными системами, состоящими из комплекса технических и программных средств, предназначенных для обработки ПДн, и функционирующих в доверенной среде эксплуатации.

9. Модель угроз безопасности ПДн в ИСПДн

9.1.В ИСПДн департамента финансов рассматриваются угрозы, связанные:

9.1.1.с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

9.2. Конечный перечень угроз безопасности ПДн определяется частными моделями угроз, разрабатываемыми применительно к конкретным ИСПДн на этапах их создания и (или) эксплуатации и зависит от характеристик ИСПДн, обусловливающих возникновение угроз безопасности ПДн. К таким характеристикам относятся: категория и объем обрабатываемых в ИСПДн персональных данных, структура ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки ПДн, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

10. Модель нарушителя безопасности ПДн

10.1. Основным источником угроз безопасности ПДн является нарушитель.

10.2. В качестве нарушителя безопасности ПДн могут выступать физические лица или организации, которые преднамеренно или случайно совершают действия, в результате которых нарушаются заданные характеристики безопасности ПДн.

10.3. Нарушитель может быть как законным пользователем (являться работником департамента финансов), так и посторонним лицом, пытающимся непосредственно или с помощью имеющихся у него технических и программных средств получить доступ к информационным ресурсам и инфраструктуре локальной вычислительной сети департамента финансов.

10.4. В зависимости от прав доступа к ресурсам ИСПДн нарушители подразделяются на два типа: внешние и внутренние.

10.5. Внешними нарушителями могут являться:

10.5.1. специализированные организации и структуры;

10.5.2. организованные преступные группы, сообщества;

10.5.3. взломщики программных продуктов информационных технологий;

10.5.4. бывшие работники департамента финансов;

10.5.5. недобросовестные контрагенты департамента финансов.

10.6. Внутренние (потенциальные) нарушители определяются в соответствии с организационно-штатной структурой департамента финансов и полномочий доступа к ресурсам ИСПДн.

10.7. Основными мотивами нарушения безопасности ПДн могут быть:

10.7.1. месть;

10.7.2. достижение личной материальной выгоды, в том числе за счет продажи полученной информации;

10.7.3. хулиганство и любопытство;

10.7.4. профессиональное самоутверждение;

10.7.5. иные мотивы.

11. Основные мероприятия по обеспечению безопасности ПД при их обработке в ИСПДн

11.1. Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн департамента финансов, руководителем департамента финансов или уполномоченным им лицом назначаются должностные лица (работники), ответственные за организацию обработки ПДн и обеспечение безопасности ПДн.

11.2. Основными мероприятиями по организации и техническому обеспечению безопасности ПДн в ИСПДн являются:

11.2.1. мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн, включающие мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн;

11.2.2. мероприятия по защите ПДн от несанкционированного доступа и определению порядка обработки в ИСПДн.

11.3. Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой СЗПДн.

11.4. Перечень реализуемых мероприятий по защите ПДн при их обработке в специальных ИСПДн департамента финансов определяется на основании анализа актуальности угроз, рисков безопасности ПДн и профилей защиты ПДн для ИСПДн департамента финансов, в соответствии с нормативными и методическим документами Федеральной службы безопасности Российской Федерации (далее – ФСБ России) и Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России).

11.5. ИСПДн по своим характеристикам и номенклатуре угроз безопасности ПДн близки к наиболее распространенным информационным системам, поэтому целесообразно при их защите

максимально использовать традиционные подходы к технической защите информации в автоматизированных системах.

11.6. Методы и способы защиты информации в информационных системах устанавливаются ФСТЭК России и ФСБ России в пределах их полномочий.

12. Идентификация и аутентификация

12.1. Управление доступом к ПДн должно осуществляться на основе принципа минимизации полномочий. Стандартным методом доступа является ролевой доступ, для чего определяются совокупности типов доступа - групповых прав и полномочий доступа пользователей (ролей), предоставляемых пользователям. Количество таких ролей должно быть ограниченным и подразумевать возможность эффективного управления. Назначение прав и полномочий конкретным пользователям осуществляется путем назначения им соответствующих ролей.

12.2. Каждый пользователь для получения соответствующих прав доступа при подключении к ИСПДн должен пройти процедуру идентификации, при этом должны использоваться уникальные признаки и имена. При этом подлинность личности пользователя должна быть проверена. Стандартное средство проверки подлинности (аутентификации) - пароль. Для обеспечения более высокой надежности аутентификации возможно использование таких средств как токены, смарт-карты и другие носители аутентифицирующей информации.

13. Обеспечение целостности

13.1. Департамент финансов обеспечивает целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонентов СЗПДн.

.

14. Антивирусная защита

14.1. Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн, осуществляющей обработку этой информации, необходимо применять специальные средства антивирусной защиты, выполняющие:

14.1.1. обнаружение и (или) блокирование деструктивных вирусных воздействий на общесистемное и прикладное программное обеспечение, реализующее обработку ПДн, а также на ПДн;

14.1.2. обнаружение и удаление неизвестных вирусов;

14.1.3. обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.

15. Обеспечение безопасного межсетевого взаимодействия

15.1. Для осуществления разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии должно применяться межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами. Межсетевой экран устанавливается между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран входит в состав защищаемой сети. Для него путем настроек отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

15.2. Межсетевое экранирование должно обеспечивать:

15.2.1. скрытие внутренней сетевой структуры ИСПДн;

15.2.2. разрешение только такого входящего и исходящего трафика, который является необходимым для работы ИСПДн;

15.2.3. блокирование любого входящего и исходящего трафика, не разрешенного явно.

16. Доступ к сетям международного информационного обмена

16.1. При использовании сети «Интернет» необходимо учитывать следующие положения:

16.1. сеть «Интернет» не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение);

16.2. провайдеры (посредники) сети «Интернет» могут обеспечить только те услуги, которые реализуются непосредственно ими;

16.3. существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети «Интернет»;

16.4. существует вероятность атаки злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные из сети «Интернет»;

16.5. гарантии по обеспечению безопасности ПДн при использовании сети «Интернет» никаким органом/учреждением/организацией не предоставляются.

17. Виды контроля эффективности системы защиты ПДн

17.1. Выполняются следующие виды контроля эффективности системы защиты ПДн:

- внутренний контроль;
- государственный контроль.

18. Внутренний контроль

18.1. Внутренний контроль эффективности системы защиты ПДн осуществляется департаментом финансов с целью поддержания заданного уровня эффективности СЗПДн, в соответствии с документированными методиками. Внутренний контроль включает:

18.1.1. мониторинг состояния технических и программных средств, входящих в состав СЗПДн;

18.1.2. контроль соблюдения требований по обеспечению безопасности ПДн (требований законодательства в области защиты ПДн, требований внутренних нормативно-методических и организационно-распорядительных документов департамента финансов, сформулированных на основе анализа рисков нарушения безопасности ПДн, договорных требований).

18.2. Оценка эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн проводится департаментом финансов с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, не реже одного раза в 3 года.

18.3. Ввод в эксплуатацию ИСПДн производится в соответствии с документально оформленными требованиями по безопасности ПДн, разрабатываемыми департаментом финансов в соответствии с требованиями законодательства и нормативно-методических документов федеральных органов исполнительной власти, осуществляющими функции по контролю и надзору в пределах своих полномочий.

18.4. Факт ввода в эксплуатацию ИСПДн в соответствии с техническими условиями оформляется Актом ввода в эксплуатацию и утверждается руководителем департамента финансов либо лицом, им уполномоченным.

18.5. Внутренний контроль в департаменте финансов осуществляется в соответствии с Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, утвержденными приказом департамента финансов.

19. Государственный контроль

19.1. Государственный контроль и надзор за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн осуществляется Роскомнадзором.

19.2. Контроль и надзор за выполнением требований безопасности персональных данных при их обработке в ИСПДн осуществляются ФСБ России и ФСТЭК России, в пределах их полномочий.

20. Порядок пересмотра Политики

20.1. Положения настоящей Политики пересматриваются в соответствии с изменениями в законодательстве Российской Федерации.

20.2. При внесении изменений в положения Политики учитываются:

20.2.1. уровень развития и внедрения информационных технологий в телекоммуникационной отрасли;

20.2.2. рекомендации российских и международных профильных организаций по информационной безопасности и защите ПДн;

20.2.3. рекомендации Консультационного совета при уполномоченном органе по защите прав субъектов ПДн.