АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА КРАСНОУФИМСК

П О С Т А Н О В Л Е Н И Е

06.08.2020 года № 448

г. Красноуфимск

ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ ГОРОДСКОГО ОКРУГА КРАСНОУФИМСК

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования автоматизированных средств», Администрация городского округа Красноуфимск

ПОСТАНОВЛЯЕТ:

1. Утвердить политику в области обеспечения безопасности персональных данных в Администрации городского округа Красноуфимск (прилагается).

2. Контроль за исполнением настоящего постановления оставляю за собой.

Глава городского округа Красноуфимск В.В. Артемьевских

Приложение
УТВЕРЖДЕНА
постановлением Администрации
городского округа Красноуфимск
от 06.08.2020 № 448

ПОЛИТИКА
в области обеспечения безопасности персональных данных
в Администрации городского округа Красноуфимск

Содержание

1. Общие положения

В целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Администрации городского округа Красноуфимск (далее - ИСПДн), в соответствии с требованиями Федерального закона от 27 июля 2006 года N° 152-ФЗ «О персональных данных», определяется политика в области обеспечения безопасности персональных данных, содержащая основные правила и порядок обработки персональных данных граждан.

Политика заключается в выполнении требований и норм обработки персональных данных, установленных в Постановлении Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Правовым основанием обработки персональных данных в Администрации городского округа Красноуфимск является осуществление видов деятельности, определенных в Уставе Администрации городского округа Красноуфимск, утвержденным Решением Красноуфимского городского Совета муниципального образования «город Красноуфимск» от 26.05.2005г № 15/2 с учетом последующих изменений.

2. Перечень персональных данных, обрабатываемых в информационных системах персональных данных и подлежащих защите

В ИСПДн защите подлежит любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- адрес;
- образование;
- профессия;
- доходы;
- фотография;
- контактный номер;
- сведения о документе, удостоверяющем личность;
- реквизиты ИНН, СНИЛС, пенсионного удостоверения, расчетных счетов.

Фамилия, имя и отчество не являются информацией, позволяющей определить субъекта персональных данных.

3. Принципы и условия обработки персональных данных

Обработка персональных данных в Администрации городского округа Красноуфимск осуществляется на основе следующих принципов:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки;
- обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- 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.

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

Обработка персональных данных осуществляется на основании условий, предусмотренных Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».

4. Меры по обеспечению защиты персональных данных

Администрации городского округа Красноуфимск предпринимает необходимые организационные и технические меры по защите персональных данных. Принимаемые меры основаны на требованиях статей 18.1, 19 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без

использования средств автоматизации», постановления Правительства Российской Федерации от 01 ноября 2012 года N° 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

В целях координации действий по обеспечению безопасности персональных данных в Администрации городского округа Красноуфимск осуществляются меры организационного и технического характера.

Реализованы следующие меры организационного характера:

- назначены лица, ответственные за организацию обработки персональных данных, а также за обеспечение безопасности персональных данных в ИСПДн;
- разработаны и внедрены локальные акты по вопросам организации и проведению работ по обеспечению безопасности персональных данных.

Осуществляются меры технического характера, направленные на:

- предотвращение несанкционированного доступа к персональным данным, обрабатываемых в ИСПДн;
- резервирование и восстановление персональных данных, программного обеспечения, средств защиты информации в ИСПДн модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- иные необходимые меры безопасности.

4.1. Лица, ответственные за обеспечение безопасности персональных данных

В Администрации городского округа Красноуфимск производится назначение следующих ответственных лиц:

1) ответственного за организацию работ по обеспечению безопасности персональных данных, на которого распоряжением Администрации городского округа Красноуфимск (далее - Распоряжение) возлагаются следующие обязанности:

- утверждение списка лиц, доступ которых к персональным данным, необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему;
- проведение разбирательств по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;
- приостановка предоставления персональных данных пользователям информационной системы при обнаружении нарушений порядка предоставления персональных данных;
- руководство работами по обеспечению безопасности персональных данных при их обработке в ИСПДн.

2) ответственного пользователя средств криптографической защиты информации, на которого Распоряжением возлагаются соответствующие должностные обязанности.

3) ответственного (специалиста или подразделение) за выполнение работ по обеспечению безопасности персональных данных, на которого Распоряжением возлагаются:

- организация парольной защиты;
- организация учета средств защиты информации, эксплуатационной и технической документации к ним;
- администрирование средств и систем защиты персональных данных в ИСПДн, включая средства антивирусной защиты (за исключением средств криптографической защиты информации);
- учет лиц, допущенных к работе с персональными данными в информационных системах;
- учет носителей персональных данных, используемых в ИСПДн (как с использованием средств автоматизации, так и без их использования);
- периодическая (не реже одного раза в квартал) проверка электронного журнала обращений пользователей ИСПДн;
- инструктаж пользователей ИСПДн о порядке и правилах использования средств защиты информации, включая средства антивирусной защиты;
- контроль за соблюдением условий использования средств защиты информации (за исключением средств криптографической защиты информации).

4.2. Учет лиц, допущенных к работе с персональными данными в информационных системах персональных данных

Лица, допущенные к работе с персональными данными в ИСПДн, утверждаются соответствующим Распоряжением.

Основанием для допуска сотрудника к персональным данным, обрабатываемым в ИСПДн, является соответствующее Распоряжение, а также необходимость обработки персональных данных в связи с выполнением должностных обязанностей.

Основанием для прекращения допуска сотрудника к персональным данным, обрабатываемым в ИСПДн, может служить Распоряжение об увольнении сотрудника или его переводе на другую должность, не требующую работы с персональными данными.

4.3. Организация резервирования и восстановления программного обеспечения, баз персональных данных информационных системах персональных данных

В ИСПДн данных резервированию подлежат:

- базы персональных данных;

- специальное программное обеспечение;
- средства защиты информации;
- общее программное обеспечение;
- средства вычислительной техники;
- средства обеспечения функционирования информационных систем.

Резервные носители персональных данных хранятся в подразделении, эксплуатирующем ИСПДн.

Резервные носители персональных данных не могут быть переданы за пределы подразделения, эксплуатирующего ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения машинных носителей дистрибутивов данных программ и машинных носителей обновлений к ним в подразделениях, отвечающих за их установку, настройку и сопровождение.

Машинные носители обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны быть маркированы датой их получения (датой выхода обновления).

В случаях сбоев, отказов, аварий технических средств и программного обеспечения ИСПДн осуществляется обязательное восстановление работоспособности ИСПДн.

4.4. Организация парольной защиты в информационных системах персональных данных

Защите паролем подлежит доступ к:

- базовым системам ввода вывода компьютеров;
- настройкам сетевого оборудования;
- настройкам операционных систем;
- настройкам средств защиты информации, в том числе средств антивирусной защиты;
- запуску специализированного программного обеспечения, предназначенного для обработки персональных данных;
- ресурсам автоматизированных рабочих мест пользователей и баз данных ИСПДн.

Базовые системы ввода-вывода, сетевое оборудование, операционные системы, средства защиты информации и файловые массивы (далее - объекты парольной защиты) должны бггь настроены таким образом, чтобы:

- исключить возможность просмотра ранее вводимых паролей;
- блокировать доступ пользователей после нескольких ошибок подряд (но не более 5) при вводе пароля и сигнализировать о наступлении данного события.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями возлагается на сотрудников отдела организационной работы, внутренней политики и информационных технологий Администрации городского округа Красноуфимск (далее - отдел ИТ) в соответствии с возложенными обязанностями.

Пользователь обязан запомнить личные пароли и никому их не передавать, и не записывать их на местах, где их могут увидеть другие лица.

Информация о паролях пользователей является информацией ограниченного доступа, предназначенной для идентификации и доступа каждого конкретного пользователя к ресурсам ИСПДн согласно разрешительной системы доступа.

Запрещается:

- умышленное и неумышленное ознакомление с парольной информацией сотрудников и посторонних лиц независимо от их должности;
- передача личного пароля сослуживцам или посторонним лицам;
- запись личного пароля на бумагу и хранение его в потенциально доступном для ознакомления посторонними лицами и другими сотрудниками месте;
- вход в систему с использованием чужих идентификаторов или паролей;
- оставление без присмотра рабочего места при работе в ИСПДн.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на сотрудников отдела ИТ Администрации городского округа Красноуфимск в соответствии с возложенными обязанностями.

4.5. Антивирусная защита в информационных системах персональных данных

К использованию в ИСПДн допускаются только лицензионные и сертифицированные по требованиям безопасности информации средства антивирусной защиты (далее - САЗ).

Установка и настройка средств антивирусного контроля на компьютерах осуществляется в соответствии с руководствами по применению конкретных САЗ.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы, файлы офисных приложений, файлы данных, исполняемые файлы) на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить

непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже 1 раза в 3 месяца.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения, должна быть выполнена антивирусная проверка на всех компьютерах ИСПДн.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно должен провести внеочередной антивирусный контроль своего компьютера.

Ответственность за организацию антивирусного контроля в соответствии с вышеуказанными требованиями возлагается на сотрудников отдела ИТ в соответствии с возложенными обязанностями.

Ответственность за проведение мероприятий антивирусного контроля и соблюдение вышеуказанных требований возлагается на сотрудников отдела ИТ и всех сотрудников, являющихся пользователями ИСПДн.

Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований по антивирусной защите осуществляется ответственным за организацию работ по обеспечению безопасности персональных данных при их обработке в ИСПДн.

5. Порядок предоставления персональных данных

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц.

До передачи любых персональных данных за пределы организации от каждого субъекта персональных данных должно быть получено письменное согласие на распространение его персональных данных, оформленное в соответствии с требованиями статьи 9 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», в каждом конкретном случае.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

Персональные данные, обрабатываемые в ИСПДн, могут быть предоставлены органам власти и органам местного самоуправления без согласия субъекта персональных данных, если данные действия осуществляются в соответствии с федеральными законами Российской Федерации в целях защиты основ конституционного строя, нравственности,

здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. При этом решение о распространении персональных данных должно содержать ссылку на соответствующую статью федерального закона Российской Федерации.

6. Права субъектов персональных данных

Субъект персональных данных вправе требовать от Администрации городского округа Красноуфимск 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.

Для реализации вышеуказанных прав субъект персональных данных, может в порядке, установленном статьей 4 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», обратиться в Администрацию городского округа Красноуфимск с соответствующим запросом. Если субъект персональных данных считает, что Администрация городского округа Красноуфимск 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, то субъект персональных данных вправе обжаловать действия или бездействие Администрации городского округа Красноуфимск в вышестоящий орган, в органы прокуратуры или в судебном порядке.

Кроме того, действующее законодательство может устанавливать ограничения и другие условия, касающиеся упомянутых выше прав.

7. Гарантии конфиденциальности

Сотрудники Администрации городского округа Красноуфимск, которым в связи с выполнением ими своих функций стали известны персональные данные субъектов персональных данных, предупреждены о возможной дисциплинарной, административной, гражданско-правовой или уголовной ответственности в случае нарушения норм и требований действующего законодательства, регулирующего правила обработки и защиты персональных данных.

8. Порядок приостановки предоставления персональных данных, в случае обнаружения нарушений порядка их предоставления, и порядок разбирательств по фактам, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям

При обнаружении нарушений порядка предоставления персональных данных пользователям информационной системы незамедлительно

приостанавливается до выявления причин нарушений и устранения этих причин.

Основаниями для приостановки обработки персональных данных в ИСПДн и проведения разбирательства являются:

- выявление недостоверных персональных данных в ИСПДн;
- предоставление персональных данных в нарушение установленных правил;
- допуск к ИСПДн лица, не имеющего на то разрешения;
- утрата носителя персональных данных;
- нарушение правил хранения носителей персональных данных;
- нарушение правил эксплуатации средств защиты информации;
- нарушение правил парольной защиты;
- нарушение правил антивирусной защиты;
- нарушение правил резервирования и восстановления общего и специального программного обеспечения, а также баз персональных данных;
- выявление в ИСПДн вредоносных программ;
- выявление в электронных журналах средств защиты информации несанкционированных действий пользователей, нарушающих безопасность персональных данных или целостность программного обеспечения ИСПДн;
- выявление несанкционированного внесения изменений в состав технических средств и программного обеспечения ИСПДн.

Разбирательство проводится структурным подразделением или должностным лицом, ответственным за обеспечение безопасности персональных данных, с обязательным привлечением руководителя структурного подразделения, осуществляющего эксплуатацию ИСПДн. В ходе разбирательства составляется заключение, в котором отражается:

- состав группы проводившей разбирательство;
- период времени, в который проводилось разбирательство;
- основание для проведения разбирательства;
- факты, выявленные в ходе разбирательства и имеющие значение в определении наличия нарушений конфиденциальности персональных данных или нарушений правил использования средств защиты информации, а также иные факты, которые могут привести к нарушению конфиденциальности персональных данных или к снижению уровня защищенности персональных данных;
- вывод о значимости нарушений, их причинах и виновных, допустивших данные нарушения;
- рекомендации по совершенствованию обеспечения безопасности персональных данных, исключающие в дальнейшем подобные нарушения.

Заключение представляется ответственному за организацию обработки персональных данных, который принимает решение на возобновление обработки персональных данных и принятие дополнительных мер защиты.

9. Заключительные положения

Настоящий документ является общедоступным. Настоящий документ подлежит изменению в следующих случаях:

- при изменении законодательства Российской Федерации в сфере защиты персональных данных;
- по результатам контроля выполнения требований по обработке и обеспечению безопасности персональных данных;
- по решению руководства.

В случае внесения в настоящий документ существенных изменений к ним будет обеспечен неограниченный доступ всем заинтересованным субъектам персональных данных.