Приложение 15
к распоряжению
администрации района от
«15» 06 2017
№ 92

ПОЛОЖЕНИЕ
об обработке персональных данных в администрации Тракторозаводского района города Челябинска с использованием средств автоматизации

1. Общие положения

1.1. Настоящее Положение устанавливает требования к обеспечению безопасности информации (персональных данных) при ее обработке в информационных системах персональных данных (далее – ИСПДн) администрации Тракторозаводского района города Челябинска, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации и без использования таковых.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и другими нормативно-правовыми актами, регламентирующими обращение и защиту персональных данных.

2. Порядок определения защищаемых информационных ресурсов

2.1. В соответствии с действующим законодательством администрация Тракторозаводского района города Челябинска является оператором персональных данных и обрабатывает информационные ресурсы, содержащие персональные данные, в пределах своих полномочий, установленных в соответствии с федеральным и областным законодательством, а также организационно-распорядительными документами администрации Тракторозаводского района города Челябинска (далее – ОРД) в целях обеспечения реализации прав субъектов персональных данных (далее Субъектов ПДн).

2.2. В соответствии с ОРД в администрации Тракторозаводского района города Челябинска определяется и утверждается содержание, состав и объём обрабатываемых персональных данных.

2.3. В соответствии с ОРД в администрации Тракторозаводского района города Челябинска определяется и утверждается перечень ИСПДн.

2.4. При проектирования вновь создаваемой или документировании ранее созданной (эксплуатируемой) ИСПДн определяются цели и содержание обработки персональных данных, определяемые действующим законодательством, и утверждается перечень обрабатываемых персональных данных.

3. Основные условия проведения обработки персональных данных в ИСПДн

3.1. Должностные лица администрации Тракторозаводского района города Челябинска, осуществляющие обработку персональных данных в ИСПДн, являются пользователями ИСПДн и обязаны принимать необходимые организационные и технические меры для их защиты.

3.2. Пользователи ИСПДн или иные должностные лица, на законных основаниях получившие доступ к персональным данным, обязаны не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

3.3. Для планирования, разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн распорядительным документом назначаются ответственные должностные лица.

3.4. Должностными лицами администрации Тракторозаводского района города Челябинска, получающими доступ к персональным данным в ИСПДн администрации Тракторозаводского района города Челябинска, должна обеспечиваться конфиденциальность таких данных.

4. Обработка персональных данных в ИСПДн

4.1. Не допускается обработка персональных данных в ИСПДн при отсутствии комплексной системы защиты информации, соответствующей требованиям нормативно-правовых актов и организационно-распорядительных документов администрации Тракторозаводского района города Челябинска.

5. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн

5.1. Допуск к обработке персональных данных ответственных должностных лиц осуществляется на основании утверждённого списка (перечня).

5.2. Должностные лица администрации Тракторозаводского района города Челябинска (далее – пользователи) имеют право в отведенное им рабочим распорядком или распоряжением руководителя структурного подразделения время решать поставленные задачи в соответствии с полномочиями доступа к информационным ресурсам ИСПДн.

5.3. Доступ пользователей к ресурсам ИСПДн осуществляется на основании персональных идентификаторов или паролей.

5.4. Запись и хранение информации, содержащей ПДн, может осуществляться пользователями только на учтённых в установленном порядке электронных носителях информации.

5.5. Пользователи, участвующие в автоматизированной обработке ПДн и имеющие доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несут персональную ответственность за свои действия и обязаны:

- соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и выполнять правила работы со средствами защиты информации,

установленными на АРМ;

- обеспечивать конфиденциальность персональных паролей и сохранность персональных идентификаторов (ключей);

- выполнять требования по проведению антивирусной защиты в полном объеме.

5.6. Пользователи обязаны извещать администратора информационной безопасности в случае:

- утери персонального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей;

- обнаружения нарушений целостности пломб (наклеек), нарушении или несоответствии номеров печатей на составляющих узлах и блоках автоматизированных рабочих мест (далее - АРМ) или иных фактов совершения в их отсутствие попыток несанкционированного доступа (далее - НСД);

- несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств;

- обнаружения ошибок или сбоев функционирования средств защиты информации;

- непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств.

5.7. Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

- создавать (преднамеренно или непреднамеренно) возможность для ознакомления с защищаемой информацией лиц, не допущенных к ПДн, в том числе оставлять без личного присмотра на рабочем месте персональный идентификатор, машинные носители и документы, содержащие защищаемую информацию, либо размещать средства отображения информации таким образом, чтобы создавалась возможность визуального просмотра информации;

- записывать и хранить ПДн и другую конфиденциальную информацию на неучтенных носителях информации;

- оставлять АРМ без присмотра во включенном состоянии, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению предпосылок или угроз утечки (неправомерной модификации) ПДн.

6. Порядок резервирования информации и восстановления работоспособности технических средств и программного обеспечения ИСПДн, а также средств защиты информации в ИСПДн

6.1. Для создания резервной копии конфиденциальной информации, обрабатываемой в ИСПДн, используются только учтённые (зарегистрированные) в установленном порядке носители информации.

6.2. Пользователи обязаны осуществлять резервное копирование конфиденциальной информации, в том числе содержащей ПДн, с периодичностью, регламентированной организационно-распорядительной документацией и технологией обработки информации в ИСПДн.

6.3. Перед резервным копированием пользователь обязан проверить носитель информации на отсутствие вредоносных программ.

6.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

6.5. Запрещается запись посторонней информации на учтённые носители информации, предназначенные для копирования ПДн.

6.6. Ответственность за проведение резервного копирования в ИСПДн в возлагается на пользователя или администратора информационной безопасности.

6.7. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения возлагается на администратора информационной безопасности.

6.8. Ответственность за проведение мероприятий по восстановлению работоспособности средств защиты информации (далее - СЗИ) возлагается на администратора информационной безопасности.

6.9. При использовании для резервного копирования персональных данных, к носителям информации предъявляются следующие требования:

6.9.1. Носители информации, содержащие персональные данные, подлежат учёту (регистрации);

6.9.2. К каждому носителю информации оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

6.9.3. Все носители ПДн, в том числе бумажные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых (при необходимости) шкафах (сейфах). При этом должны быть созданы условия, обеспечивающие их сохранность.

7. Правила антивирусной защиты ИСПДн

7.1. Организация антивирусной защиты возлагается на администратора информационной безопасности. Ответственность за проведение мероприятий антивирусной защиты непосредственно на автоматизированных рабочих местах, входящих в состав ИСПДн (далее – АРМ), возлагается на пользователей данных АРМ. При выполнении работ по антивирусной защите необходимо руководствоваться инструкцией по организации антивирусной защиты.

7.2. К использованию на АРМ допускаются только лицензионные антивирусные средства.

7.3. Установка и начальная настройка средств антивирусного контроля на АРМ может осуществляться специализированными организациями, а также администратором информационной безопасности.

7.4. Администратор информационной безопасности осуществляет обновление антивирусных баз с периодичностью, установленной порядком проведения антивирусного контроля или в соответствии с рекомендациями производителя.

7.5. Настройка антивирусных программных средств должны предусматривать проверку на наличие вредоносных программ в начале работы в режиме автозагрузки всех информационных ресурсов АРМ.

7.6. При выявлении признаков наличия на АРМ вредоносных программ (нештатная работа программного обеспечения, появление графических и звуковых эффектов, искажений данных, немотивированная утрата массивов данных, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно обязан провести внеочередную антивирусную обработку своего АРМ и известив об этом администратора информационной безопасности.

8. Организация парольной защиты в ИСПДн

8.1. Организация процессов генерации паролей, контроль периодичности смены паролей, а также прекращения их действия во всех подсистемах ИСПДн возлагается на администратора информационной безопасности и выполняется в соответствии с инструкцией по организации парольной защиты.

8.2. Персональные пароли пользователей могут генерироваться пользователями самостоятельно с извещением администратора информационной безопасности.

8.3. Полная смена паролей пользователей должна проводиться регулярно не реже одного раза в квартал.

8.4. В случае прекращения полномочий пользователя (увольнение, смена исполняемых функций внутри администрации Тракторозаводского района города Челябинска и т.п.) внеплановая смена личного пароля или удаление учетной записи пользователя должны производиться администратором информационной безопасности, с внесением изменений в разрешительную систему доступа ИСПДн.

9. Аудит обращений к информационным ресурсам ИСПДн

9.1. С целью выявления фактов несанкционированного доступа к конфиденциальной информации в ИСПДн система защиты информации в ИСПДн должна предусматривать подсистему аудита обращений.

9.2. Право настройки электронных журналов, а также проверки и контроля обращений к ИСПДн имеет администратор информационной безопасности.

10. Правила обновления общесистемного и прикладного программного обеспечения ИСПДн, а также технического обслуживания

10.1. Организация обновления (модификации) общесистемного и прикладного программного обеспечения, технического обслуживания возлагается

на администратора информационной безопасности.

10.2. Изменения в конфигурацию аппаратно-программных средств защиты информации, входящих в состав ИСПДн, осуществляется администратором информационной безопасности с внесением соответствующих отметок в организационно-распорядительные документы ИСПДн.

10.3. Все изменения конфигураций технических и программных средств должны производиться на основании заявок сотрудников, которые эксплуатируют ИСПДн.

10.4. Заявка на внесение изменений в конфигурацию системных и прикладных программных средств, входящих в состав ИСПДн, может предусматривать установку (развертывание), обновление, а также удаление на АРМ программных средств, используемых для решения задач ИСПДн;

10.5. Решение по существу содержащихся в заявке предложений с учётом мнения администратора информационной безопасности принимает руководитель структурного подразделения.

10.6. Установка и обновление программного обеспечения на АРМ производится только с оригинальных лицензионных дистрибутивных носителей, полученных в установленном порядке, прикладного программного обеспечения - с эталонных копий программных средств.

10.7. После установки (обновления) программного обеспечения системы защиты информации ИСПДн администратор информационной безопасности должен произвести соответствующую отметку в «Техническом паспорте на объект информатизации (ИСПДн)».

10.8. При возникновении ситуаций, требующих передачи компонент АРМ, входящего в состав ИСПДн, специализированной сервисной организации для ремонта и обслуживания, носители информации, содержащие персональные данные, извлекаются и помещаются для хранения в специально отведённое для этих целей хранилище. Носители информации, извлечённые из системных блоков АРМов, и содержащие персональные данные выносу за пределы администрации Тракторозаводского района города Челябинска не подлежат.

11. Осуществление контроля состояния защиты информации в ИСПДн

11.1. Контроль состояния защиты информации в ИСПДн - проверка организационных и технических мероприятий, предпринятых для обеспечения безопасности ПДн при обработке в ИСПДн, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

11.2. Основными мероприятиями по контролю состояния защиты информации в ИСПДн являются:

- проверка соответствия условий эксплуатации ИСПДн требованиям

нормативных правовых и организационно-распорядительных документов по защите информации в ИСПДн;

- выявление возможных каналов утечки информации и внешних программно-технических воздействий на информацию, обрабатываемую в ИСПДн;

- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

- проверка выполнения требований по антивирусной защите всех компонент ИСПДн;

- оперативное принятие мер по пресечению нарушений требований и норм защиты информации в ИСПДн.

11.3. Контроль защиты информации осуществляется с учетом реальных условий эксплуатации ИСПДн как непосредственно на АРМ ИСПДн, в том числе с применением средств аудита обращений к ИСПДн, так и путём ознакомления с организационно-распорядительными документами на ИСПДн.

11.4. С целью проверки эффективности применения организационных и технических мероприятий по защите информации могут проводиться необходимые инструментальные исследования и расчеты с привлечением специалистов специализированной организации, обладающей соответствующими лицензиями на проведение указанных работ.

11.5. Основными видами технического контроля на объекте организации являются визуальный контроль условий эксплуатации объектов информатизации, контроль эффективности защиты информации от утечки по техническим каналам, контроль эффективности защиты от несанкционированного доступа к информации и программно-технических воздействий на информацию.

11.6. Невыполнение установленных нормативных требований по защите ПДн считается предпосылкой утечки (утраты) защищаемой информации.

11.7. В случае выявления предпосылок утечки (утраты) защищаемой информации с целью установления обстоятельств их возникновения может проводиться служебное расследование.

11.8. Контроль защиты информации осуществляется путем проведения как плановых, так и внеплановых проверок объектов защиты. Плановые проверки проводятся не реже одного раза в год.

11.9. Обследование объектов информатизации проводится с целью определения соответствия объектов информатизации ИСПДн требованиям по защите информации, установленным «Аттестатом соответствия требованиям по безопасности информации». В ходе обследования объектов информатизации проверяется:

- соответствие класса (уровня) защищенности ИСПДн условиям, сложившимся на момент проверки;

- выполнение требований предписаний на эксплуатацию технических средств и систем, организации электропитания и заземления (при

необходимости);

- соответствие выполняемых в ИСПДн мероприятий по защите информации данным, изложенным в организационно-распорядительной документации;

- выполнение требований по защите автоматизированных систем от несанкционированного доступа;

- выполнение требований по антивирусной защите;

- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты;

- наличие электробытовой, радио- телевизионной и иной аппаратуры, которые могут способствовать возникновению каналов утечки информации.

11.10. Государственный контроль состояния защиты информации вправе осуществлять федеральные уполномоченные органы в соответствии с действующим законодательством Российской Федерации. В части обеспечения технической защиты информации (персональных данных) без применения криптографических средств государственный контроль осуществляет Федеральная служба по техническому и экспортному контролю Российской Федерации. В части защиты информации с применением криптографических средств государственный контроль осуществляет Федеральная служба безопасности Российской Федерации.

12. Ответственность должностных лиц

12.1. Должностные лица администрации Тракторозаводского района города Челябинска, допущенные к обработке персональных данных в ИСПДн, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Председатель комиссии: А.А. Дорин

Заместитель
председателя комиссии: Н.Н. Свертилова

Члены комиссии: Е.В. Смирнова

О.С. Сизоненко