УТВЕРЖДЕНО

приказом ГУП СК «Ставропольккоммунэлектро»

от 16 ноября 2022 г. № 296-п

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГУП СК «СТАВРОПОЛЬККОММУНЭЛЕКТРО»

Ставрополь, 2022

Содержание

Термины и определения 3

Перечень используемых сокращений 4

1. Общие положения 5

2. Принципы обработки персональных данных 7

3. Информационные системы персональных данных 9

4. Система защиты персональных данных 10

4.1 Организация СЗПДн 10
4.2 Эксплуатация СЗПДн 11
4.3 Мониторинг СЗПДн 12

5. Правила обработки персональных данных 14

5.1 Сбор персональных данных 14
5.2 Порядок отзыва согласия субъекта ПДн на обработку ПДн. 16
5.3 Запись, систематизация и накопление персональных данных 16
5.4 Хранение персональных данных 16
5.5 Использование, извлечение и уточнение персональных данных 17
5.6 Передача персональных данных 18
5.7 Блокирование персональных данных 19
5.8 Удаление, уничтожение и обезличивание персональных данных 20

6. Обучение работников Предприятия правилам обработки персональных данных 21

7. Управление доступом к персональным данным 22

7.1 Физический доступ к компонентам ИСПДн 22
7.2 Управление идентификаторами и средствами аутентификации 22
7.3 Управление доступом работников к персональным данным 23
7.4 Идентификация и аутентификация объектов и субъектов доступа 25
7.5 Управление доступом третьих сторон к персональным данным 26
7.6 Поручение обработки персональных данных 26

8. Контроль защищенности персональных данных 28

9. Взаимодействие с субъектами персональных данных и органами власти 29

9.1 Взаимодействие с субъектами персональных данных 29
9.2 Взаимодействие с органами власти 29

10. Ответственность 30

Термины и определения

Автоматизированное рабочее место – комплекс технических и программных средств, предназначенный для автоматизации деятельности работника.

Информационная безопасность – процесс обеспечения конфиденциальности, целостности и доступности информации.

Информационная инфраструктура – совокупность информационных технологий, аппаратных и программных средств, средств связи и телекоммуникаций, предназначенных для обеспечения бизнес-процессов Предприятия.

Информационный ресурс – отдельный документ или массив документов, документ и массив документов, содержащийся в информационной системе, а также сама информационная система

Информационная система – комплекс программных и аппаратных компонентов информационной инфраструктуры Предприятия, предназначенных для автоматизации процессов сбора, обработки, хранения и выдачи информации.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Конфиденциальная информация – сведения, включающие в себя персональные данные, информацию ограниченного распространения («Для служебного пользования») и сведения, связанные с коммерческой деятельностью (коммерческая тайна), доступ к которым ограничен, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим конфиденциальности.

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Средство защиты информации – программное или программно-аппаратное средство, предназначенное для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Перечень используемых сокращений

АРМ – автоматизированное рабочее место.

ИС – информационная система.

ИСПДн – информационная система персональных данных.

ПДн – персональные данные.

СВТ – средство вычислительной техники.

СЗПДн – система защиты персональных данных.

Предприятие – ГУП СК «Ставрополькоммунэлектро».

1. Общие положения

В настоящем Положении об обработке и защите персональных данных (далее – Положение) установлены требования по организации и непосредственному функционированию процессов обработки персональных данных (далее – ПДн) в ГУП СК «Ставрополькоммунэлектро» (далее – Предприятие) в соответствии с требованиями нормативных правовых актов Российской Федерации в области обработки и защиты ПДн.

Требования настоящего Положения распространяются на структурные подразделения Предприятия и отдельных должностных лиц, принимающих участие в процессах обработки ПДн.

Требования настоящего Положения распространяются на все процессы обработки ПДн, независимо от формы их представления.

Настоящее Положение разработано в соответствии со следующими нормативными правовыми документами:

- Конституция Российской Федерации;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утвержден Приказом ФСТЭК России от 18.02 2013 № 21);
- Состав и содержание организационных и техническим мер по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (утвержден Приказом ФСБ России от 10.07.2014 № 378).

При работе с ПДн во всех случаях, не урегулированных внутренними документами Предприятия, необходимо руководствоваться действующим законодательством Российской Федерации.

Работники Предприятия, получившие доступ к персональным данным, обязаны соблюдать конфиденциальность таких данных, не разглашать и иным образом не делать доступными персональные данные субъекта без его согласия.

На Предприятии для реализации настоящего Положения приказом руководителя Предприятия назначаются Ответственный за обработку и защиту информации, Администратор информационной безопасности, Администратор ИС.

Настоящее Положение должно быть доведено до всех работников Предприятия под подпись. Подпись работника на листе ознакомления означает его согласие со всеми требованиями, указанными в настоящем Положении.

Контроль над соблюдением настоящего Положения осуществляет Ответственный за обработку и защиту информации.

2. Принципы обработки персональных данных

Обработка ПДн на Предприятии должна осуществляться в соответствии со следующими принципами:

- обработка ПДн должна осуществляться на законной и справедливой основе;
- обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями их сбора;
- не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только ПДн, которые отвечают целям их обработки;
- содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке ПДн должны быть обеспечены их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Необходимо принимать меры по удалению или уточнению неполных или неточных данных;
- хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- не допускается использовать ПДн в целях причинения имущественного и (или) морального вреда субъектам ПДн, затруднения реализации их прав и свобод;

– все работники должны быть ознакомлены под подпись с документами Предприятия, устанавливающими порядок обработки их ПДн, а также их правами и обязанностями в этой области, в соответствии с действующими нормативными документами.

На Предприятии должен проводиться регулярный анализ соответствия процессов обработки ПДн указанным выше принципам. Данный анализ проводится в следующих случаях:

– создание новых или внесение изменений в существующие процессы обработки ПДн;
– создание новых или внесение изменений в существующие ИСПДн;
– изменение нормативной базы, затрагивающей принципы и (или) процессы обработки ПДн на Предприятии;
– проведение внутренних контрольных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

3. Информационные системы персональных данных

Комплексы баз данных, средств вычислительной техники, технических средств обработки объединяются в информационные системы персональных данных. При этом в одну ИСПДн может входить любое количество компонентов.

Для ИСПДн Предприятия в обязательном порядке должны быть разработаны следующие документы:

- Модель угроз безопасности информации ИСПДн;
- Акт определения уровня защищенности ПДн.

В случае включения ИСПДн в состав иной системы, подлежащей классификации, допускается приведение модели угроз безопасности персональных данных в составе общей модели угроз безопасности на систему.

4. Система защиты персональных данных

4.1 Организация СЗПДн

С целью выполнения требований законодательства Российской Федерации в области ПДн, важнейшей задачей является обеспечение конфиденциальности, целостности и доступности ПДн при их обработке.

Для решения данной задачи на Предприятии введена, функционирует и проходит периодический пересмотр (контроль) система защиты персональных данных (далее – СЗПДн), которая состоит из следующих компонентов:

- организационная структура (участники обработки и ответственные лица);
- организационно-распорядительная документация;
- средства обработки ПДн;
- меры и средства обеспечения безопасности ПДн.

СЗПДн Предприятия основана на следующих принципах:

- вовлеченность руководства – деятельность по обеспечению безопасности ПДн инициирована и контролируется руководством Предприятия;
- соответствие мер и средств защиты актуальным угрозам безопасности ПДн;
- соответствие мер и средств защиты требованиям нормативных документов Российской Федерации в области обработки и обеспечения безопасности ПДн;
- комплексность – с целью обеспечения безопасности ПДн на Предприятии используется совокупность организационных и технических мер;
- удобство персонала – при построении и модернизации СЗПДн на Предприятии учитываются и, по возможности, сводятся к минимуму возможные затруднения персонала в работе со средствами защиты и при выполнении основных процедур обеспечения безопасности ПДн;
- законность организационных и технических мер по обеспечению безопасности ПДн;

– непрерывность повышения уровня знаний работникона Предприятии в сфере обеспечения безопасности ПДн;
– стремление к постоянному совершенствованию СЗПДн.

В соответствии с принципами обработки ПДн на Предприятии определены правила обработки ПДн, а также методы и способы обеспечения безопасности ПДн.

Предприятие самостоятельно либо с привлечением организаций, обладающих лицензией на техническую защиту конфиденциальной информации, не реже 1 раза в год проводит аудит соответствия обработки и защиты ПДн требованиям законодательства Российской Федерации и подзаконных актов.

Контроль может осуществляться с применением автоматизированных средств инвентаризации и средств анализа защищенности.

4.2 Эксплуатация СЗПДн

На Предприятии в рамках деятельности по обеспечению защиты информации в ИСПДн осуществляются:

– управление доступом субъектов к объектам доступа;
– идентификация и аутентификация субъектов доступа и объектов доступа;
– ограничение программной среды;
– управление доступом к машинным носителям информации и их защита;
– регистрация событий информационной безопасности;
– реализация антивирусной защиты;
– обнаружение вторжений;
– защита среды виртуализации;
– контроль (анализ) защищенности;
– обеспечение целостности;
– обеспечение доступности;
– защита технических средств;
– защита ИС, ее средств, систем связи и передачи данных;
– выявление инцидентов и реагирование на них;
– управление конфигурацией.

Изменения конфигурации ИСПДн, включая обновления и/или замену программного обеспечения, технических средств, средств защиты информации, подлежат контролю и учету администратором информационной безопасности с возможностью установления даты изменения и перечня произведенных действий.

Перед внесением изменений в конфигурацию ИСПДн должен осуществляться анализ потенциального воздействия этих изменений на ИСПДн и СЗПДн и согласование потенциальных изменений в конфигурации ИСПДн с администратором информационной безопасности.

Вносить изменения в существующую конфигурацию ИСПДн могут только администраторы ИС и администраторы информационной безопасности на основании заявки от пользователя ИСПДн, распоряжения начальства и Ответственного за обработку и защиту информации и в других случаях, предусматривающих внесение изменений в конфигурацию.

4.3 Мониторинг СЗПДн

Мониторинг СЗПДн осуществляется с целью актуализации существующей СЗПДн в соответствии с текущими процессами обработки ПДн, элементами ИТ- и ИБ-инфраструктуры, и требованиями по безопасности ПДн.

В ходе мониторинга СЗПДн обеспечивается контроль отсутствия НСД к ПДн.

В процессе мониторинга СЗПДн решаются задачи по актуализации:

- сведений о процессах обработки ПДн:
  - перечень ПДн, обрабатываемых на Предприятии;
  - объем обрабатываемых ПДн;
  - категории субъектов, чьи ПДн обрабатываются на Предприятии;
  - пользователи ПДн (структурные подразделения и отдельные работники) и третьи стороны (контрагенты, аутсорсинговые и обслуживающие организации и т. п.), имеющие доступ к ПДн;
  - структура и состав ИСПДн;
  - мероприятия и технические меры обеспечения безопасности ПДн.
- уровня защищенности ПДн при их обработке в ИСПДн, в т. ч.:

- вреда, который может быть причинен субъектам ПДн в случае нарушения безопасности ПДн, и соответственно показателя опасности угроз безопасности в отдельных ИСПДн;
- угроз безопасности ПДн.

– требований к СЗПДн;
– документации на СЗПДн;
– вариантов реализации СЗПДн (в т. ч. проведение дополнительных мероприятий по защите ПДн).

Мониторинг СЗПДн организуется и контролируется Ответственным за обработку и защиту информации с администратора информационных систем, администратора информационной безопасности и подразделений, обрабатывающих ПДн в ИСПДн.

5. Правила обработки персональных данных

5.1 Сбор персональных данных

Предприятие получает ПДн из следующих источников:

- непосредственно от субъекта ПДн;
- от третьей стороны, в целях исполнения договорных обязательств или исполнения требований нормативных документов Российской Федерации;
- от другого субъекта ПДн в целях реализации его законных прав.

Если предоставление ПДн является обязательным в соответствии с федеральным законом и субъект ПДн отказывается предоставить его ПДн, необходимо разъяснить субъекту ПДн юридические последствия такого отказа, в частности, указать на положения законодательных актов Российской Федерации, предусматривающих сбор ПДн и последствия отказа в предоставлении ПДн.

При сборе ПДн субъекту ПДн по его просьбе необходимо предоставить следующую информацию:

- подтверждение факта обработки ПДн;
- правовые основания и цели обработки ПДн;
- применяемые на Предприятии способы обработки ПДн;
- наименование и фактический адрес Предприятия, сведения о лицах (за исключением работников Предприятия), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Предприятия, если обработка поручена или будет поручена такому лицу.

Если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн необходимо предоставить субъекту ПДн следующую информацию:

– наименование Предприятия;
– цель обработки ПДн и ее правовое основание;
– предполагаемые пользователи ПДн;
– права субъекта ПДн;
– источник получения ПДн.

Указанная информация может не предоставляться в следующих случаях:

– субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;
– ПДн получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
– ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
– предоставление субъекту ПДн указанных сведений нарушает права и законные интересы третьих лиц.

Сбор персональных данных организуется исключительно на законных основаниях. При сборе ПДн до или в момент их получения необходимо осуществлять сбор согласий на обработку ПДн. Согласие может быть получено в любой позволяющей подтвердить факт его получения форме. Во всех случаях, когда это возможно, следует получать письменное согласие субъекта (формы согласия приведены в Приложениях 1-2 к настоящему Положению).

Ответственность за сбор и хранение согласий возлагается на работников Предприятия, осуществляющих сбор ПДн субъектов ПДн. Хранение согласий субъектов ПДн осуществляется в бумажном и/или электронном виде.

5.2 Порядок отзыва согласия субъекта ПДн на обработку ПДн.

Если право или обязанность обработки ПДн субъекта ПДн Предприятием установлена законом, то субъект ПДн обязан не препятствовать реализации Предприятием этого права или исполнению этой обязанности.

В случае отзыва субъектом ПДн согласия на обработку его ПДн работники Предприятия осуществляют в срок до 30 календарных дней удаление персональных данных на всех носителях, при необходимости оставляя обезличенные сведения, необходимые для ведения статистики и реализации законных интересов Предприятия. При отзыве согласия субъектом не удаляются сведения, обработка которых производится во исполнение требований законодательства Российской Федерации

5.3 Запись, систематизация и накопление персональных данных

Предприятие осуществляет запись, систематизацию и накопление полученных ПДн в базах данных и иных электронных хранилищах данных с использованием аппаратных средств и программного обеспечения.

5.4 Хранение персональных данных

На Предприятии обеспечивается раздельное хранение ПДн при разных целях обработки и не допускается на одном носителе фиксация ПДн, цели обработки которых заведомо несовместимы.

На Предприятии обеспечивается раздельное хранение ПДн, собранных с разными целями обработки.

Хранение ПДн на Предприятии осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки и требования нормативных документов Российской Федерации, связанных с хранением документов, после чего данные могут быть обезличены (при необходимости).

Работники Предприятия, имеющие доступ к ПДн субъектов ПДн в связи с исполнением трудовых обязанностей, обязаны обеспечивать хранение информации, содержащей ПДн субъектов ПДн, исключающее неправомерный или случайный доступ к ним.

В случае необходимости работник обязан передать документы и иные носители, содержащие ПДн субъектов ПДн, работнику, на которого организационно-распорядительным актом (приказом, распоряжением) или должностной инструкцией возложено исполнение его трудовых обязанностей.

В случае увольнении работника, имеющего доступ к ПДн субъектов ПДн, документы и иные носители, содержащие ПДн субъектов ПДн, передаются другому работнику, имеющему доступ к ПДн субъектов ПДн, по указанию руководителя структурного подразделения.

5.5 Использование, извлечение и уточнение персональных данных

На Предприятии запрещено принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

При использовании ПДн допускается:

- извлечение ПДн из баз данных или иных электронных хранилищ данных;
- формирование документов (как в электронном виде, так и на бумажных носителях), содержащих ПДн, в случаях, предусмотренных технологическими процессами обработки ПДн;
- передача таких документов как внутри Предприятия между работниками, в том числе различных структурных подразделений, так и третьим лицам.

Субъект персональных данных обязан предоставлять Предприятию достоверные сведения о себе и своевременно сообщать ей об изменении своих ПДн.

Предприятие обязано уточнять обрабатываемые ПДн и вносить в них необходимые изменения (при выявлении неполных или неточных ПДн субъекта ПДн) в следующих случаях:

- по требованию субъекта ПДн;
- по требованию уполномоченного органа по защите прав субъектов ПДн;
- по результатам внутренних контрольных мероприятий.

Предприятие обязано уведомить субъекта ПДн или его представителя о внесенных изменениях и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта ПДн были переданы.

Лицом, ответственным за организацию и контроль своевременного внесения изменений в ПДн субъектов ПДн и направления уведомлений субъектам ПДн, их представителям и третьим лицам, является Ответственный за организацию обработки ПДн.

5.6 Передача персональных данных

Передача ПДн может осуществляться посредством использования корпоративной сети, а также с использованием бумажных носителей ПДн.

Передачу ПДн с использованием съемных машинных носителей (магнитных дисков, флеш-дисков, оптических дисков (CD-RW, CD-ROM, ROM DVD, DVD-RW) и других устройств хранения данных) разрешается осуществлять только в случае невозможности использования корпоративной сети.

При необходимости передачи ПДн другим работникам Предприятия для исполнения ими своих трудовых обязанностей, допускается осуществлять передачу только работникам, имеющим доступ к ПДн субъектов ПДн согласно в соответствии с «Перечнем лиц и подразделений, допущенных к обработке персональных данных».

Предоставление Предприятием доступа к ПДн субъекта ПДн третьим лицам осуществляется при соблюдении следующих условий:

- передача ПДн, в том числе поручение Предприятием обработки ПДн третьим лицам осуществляется с согласия субъекта ПДн или без такового согласия при наличии правовых оснований, предусмотренных федеральным законодательством, в частности, статьей 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- в том случае, если Предприятие поручает обработку ПДн третьему лицу на основании договора, в условиях такого договора определяется:
- обязанность лица, осуществляющего обработку ПДн по поручению Предприятия, по соблюдению принципов и правил обработки ПДн;

- перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн по поручению;
- цели обработки ПДн;
- обязанность лица, осуществляющего обработку ПДн по поручению Предприятия, по соблюдению конфиденциальности ПДн и обеспечению безопасности ПДн;
- требования по обеспечению безопасности ПДн, которые должны быть выполнены лицом, осуществляющим обработку ПДн по поручению Предприятия.

ПДн субъекта могут быть предоставлены его законному представителю в порядке, установленном действующим законодательством Российской Федерации при предоставлении документов, подтверждающих полномочия представителя.

Предоставление ПДн субъекта государственным органам и органам местного самоуправления производится в соответствии с требованиями действующего законодательства Российской Федерации.

Ответственность за соблюдение порядка предоставления ПДн субъекта третьим лицам несет работник Предприятия, а также руководитель структурного подразделения, осуществляющего передачу ПДн субъекта ПДн третьему лицу.

На Предприятии не осуществляется трансграничная передача персональных данных (передача персональных данных на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

5.7 Блокирование персональных данных

Предприятие блокирует обрабатываемые ПДн при выявлении их недостоверности или неправомерных действий в отношении субъекта ПДн в следующих случаях:

- по требованию субъекта ПДн;
- по требованию уполномоченного органа по защите прав субъектов ПДн;
- по результатам внутренних контрольных мероприятий.

5.8 Удаление, уничтожение и обезличивание персональных данных

Предприятие уничтожает ПДн в случае:

- достижения целей обработки ПДн или утраты необходимости в их достижении;
- получения соответствующего запроса от субъекта ПДн, при условии, что данный запрос не противоречит требованиям законодательства Российской Федерации;
- отзыва согласия субъекта на обработку его ПДн, если отзыв согласия влечет за собой уничтожение ПДн;
- получения соответствующего предписания от уполномоченного органа по защите прав субъектов.

Персональные данные кандидатов на вакантные должности Предприятия подлежат удалению из информационных систем персональных данных по достижению цели обработки – приема кандидата на вакантную должность либо отказу кандидату. В случае приема кандидата на вакантную должность сведения о нем обрабатываются в рамках процессов обработки персональных данных работников Предприятия и подлежат удалению из программного обеспечения, предназначенного для обработки сведений о кандидатах. Удаление осуществляется работниками Отдела управления персоналом. Не реже 1 раза в 3 месяца работники Отдела управления персоналом осуществляют контроль наличия в информационных системах сведений о субъектах, в приеме на вакантную должность которым было отказано, и в случае выявления удаляют такие сведения.

ПДн работников, уволенных более 5 лет назад, подлежат удалению из ИСПДн. Допустимо создание архивной копии информации на учтенном носителе ПДн для хранения у ответственного лица из числа работников, допущенных к обработке ПДн и определяемого Ответственным за обработку и защиту информации. Проверка наличия в ИСПДн данных работников, уволенных более 5 лет назад, и контроль удаления таких данных осуществляется работниками Отдела управления персоналом не реже 1 раза в 3 месяца под контролем Ответственного за обработку и защиту информации.

Предприятие может заключать договоры с третьими сторонами на оказание услуг по уничтожению материальных носителей. При этом Предприятие и третья сторона соблюдают все правила для обеспечения конфиденциальности уничтожаемых данных.

6. Обучение работников Предприятия правилам обработки персональных данных

На Предприятии все работники, участвующие в обработке ПДн, в обязательном порядке должны проходить внутренний инструктаж по следующим темам:

- общие вопросы обеспечения информационной безопасности на Предприятии;
- правила обработки ПДн;
- правила использования средств защиты информации, входящих в состав СЗПДн Предприятия;
- ответственность за нарушение правил обработки и обеспечения безопасности ПДн.

Новые работники в обязательном порядке проходят вводный инструктаж по указанным темам.

Ответственным за организацию проведения инструктажа работников Предприятия, участвующих в обработке и обеспечении безопасности ПДн, является Ответственный за обработку и защиту информации.

7. Управление доступом к персональным данным

7.1 Физический доступ к компонентам ИСПДн

Для помещений с расположенными в них защищаемыми техническими средствами, коммуникационным оборудованием и автоматизированными рабочими местами (далее – АРМ) должен обеспечиваться контроль доступа.

Для помещений с расположенными в них защищаемыми техническими средствами, входящими в состав ИСПДн, контроль доступа должен обеспечиваться с помощью организационных мер и технических средств – систем контроля и управления доступом, механических или электромеханических кодовых замков и т.п.

Помещения с расположенными в них защищаемыми техническими средствами, должны находиться в зонах, доступ в которые посетителей ограничивается.

Помещения, в которых установлены данные технические средства, при отсутствии работников, должны быть закрыты.

Постоянный доступ в помещения с расположенными в них защищаемыми техническими средствами, может быть предоставлен только работникам Предприятия, которым этот доступ необходим для выполнения ими своих функциональных обязанностей.

Временный доступ в помещения с расположенными в них защищаемыми техническими средствами, может быть предоставлен работникам Предприятия и специалистам сторонних организаций для выполнения ими своих функциональных обязанностей.

Нахождение работников сторонних организаций в помещениях с расположенными в них защищаемыми техническими средствами без присутствия работников Предприятия запрещается.

7.2 Управление идентификаторами и средствами аутентификации

На Предприятии ответственным за управление идентификаторами пользователей и устройств и средствами аутентификации является администратор информационной безопасности.

Управление идентификаторами и средствами аутентификации включает:

- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству;
- выдача средств аутентификации и (или) генерация и выдача аутентификационной информации пользователям;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение года;
- блокирование идентификатора пользователя после его неиспользования в течение 90 дней;
- принятие мер в случае утраты или компрометации средств аутентификации;
- изменение аутентификационной информации (средств аутентификации), заданной их производителями и используемой при внедрении системы защиты информации;
- установление характеристик средств аутентификации;
- замена, блокирование утерянных, скомпрометированных и поврежденных средств аутентификации;
- обновление аутентификационной информации с заданной периодичностью;
- защита аутентификационной информации от неправомерного доступа к ней и модификации.

7.3 Управление доступом работников к персональным данным

Для определения работников Предприятия, допущенных к работе с ПДн, разрабатывается «Перечень лиц и подразделений, допущенных к обработке информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну» и утверждается руководителем Предприятия.

Ответственным за внесение изменений в «Перечень лиц и подразделений, допущенных к обработке информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну», является Ответственный за обработку и защиту информации.

Инициатором внесения изменений в «Перечень лиц и подразделений, допущенных к обработке информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну», выступают:

- руководители вновь созданных структурных подразделений, предполагающих участие их работников в обработке ПДн;
- руководители структурных подразделений, внутри которых произошли изменения организационно-штатной структуры, касающиеся работников, должностные обязанности которых связаны с обработкой ПДн;
- руководители структурных подразделений, внутри которых произошли изменения в должностных обязанностях работников, связанных с допуском или отменой допуска к ПДн, обрабатываемым на Предприятии.

Руководители перечисленных структурных подразделений оформляют служебные записки на имя Ответственного за обработку и защиту информации, в которых указывают работников и категории субъектов ПДн, доступ к которым указанным работникам необходимо изменить или предоставить для выполнения ими своих функциональных (должностных) обязанностей. Ответственный за обработку и защиту информации подготавливает новую редакцию «Перечня лиц и подразделений, допущенных к обработке персональных данных», с внесенными на основании служебной записки изменениями, которая утверждается Начальником Предприятия.

Ответственный за обработку и защиту информации осуществляет контроль актуальности «Перечня лиц и подразделений, допущенных к обработке персональных данных», и при необходимости предоставляет к утверждению новую редакцию не реже 1 раза в 3 месяца.

Работник допускается к обработке ПДн только после:

– ознакомления с требованиями настоящего Положения и иными организационно-распорядительными документами на СЗПДн, выполнение требований которых обязательно для соответствующих работников;
– прохождения инструктажа по правилам обработки и обеспечения безопасности ПДн;
– ознакомления с видами ответственности за нарушение установленных на Предприятии правил обработки и обеспечения безопасности ПДн.

На Предприятии реализован ролевой метод управления доступом субъектов к объектам доступа и назначены типы доступа субъектов к объектам доступа, присваиваемые пользователям в зависимости от выполняемых ими ролей. Роли в ИСПДн присваиваются пользователям на основании их должностных обязанностей.

За управление учетными записями пользователей отвечают администраторы информационной безопасности.

В ИСПДн правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам и объектам, создаваемым общесистемным программным обеспечением.

На Предприятии используются автоматизированные средства поддержки управления учетными записями пользователей.

Пользователи ИСПДн имеют ограниченные права по доступу и возможным действиям с ПДн, минимально необходимые для выполнения ими своих должностных обязанностей, определяемые руководителем подразделения пользователя и согласуемые с администратором информационной безопасности. Пользователи ИСПДн не могут иметь права администратора, в ИСПДн без соответствующего приказа руководителя Предприятия.

7.4 Идентификация и аутентификация объектов и субъектов доступа

Для доступа в ИСПДн осуществляется идентификация и аутентификация пользователей, являющихся работниками Предприятия, и процессов запускаемых от имени этих пользователей.

В ИСПДн осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не

имеющими на это полномочий, посредством отображения вводимых символов условными знаками «•» или «*».

До прохождения процедуры аутентификации в ИСПДн пользователи не должны иметь возможность работы с данными в ИСПДн. Пользователи ИСПДн должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех, которые разрешены до прохождения идентификации и идентификации. До прохождения аутентификации допускается:

- включение/выключение рабочего места, перезагрузка операционной системы;
- смена пользователя;
- смена раскладки клавиатуры.

7.5 Управление доступом третьих сторон к персональным данным

Предприятие в ходе своей деятельности осуществляет предоставление доступа (в т. ч. осуществляет передачу) к ПДн третьим лицам в целях исполнения договорных обязательств перед субъектами ПДн, а также с целью обеспечения своей деятельности или исполнения требований нормативных документов Российской Федерации. При этом субъект ПДн может беспрепятственно получить доступ к перечню третьих сторон, которым предоставляется доступ к его ПДн, если это не противоречит требованиям законодательства Российской Федерации.

Предприятием передаются ПДн только в объеме, необходимом для достижения заявленных целей обработки.

Существенным условием договоров с третьими сторонами, в рамках исполнения которых предоставляется доступ к ПДн, является обязанность соблюдения сторонами мер обеспечения безопасности ПДн при их обработке. Кроме того, в договорах в обязательном порядке определяется порядок передачи ПДн.

7.6 Поручение обработки персональных данных

Предприятие может поручать обработку ПДн другим лицам (третьим сторонам), а также выступать в роли лица, осуществляющего обработку ПДн по поручению других операторов ПДн.

Предприятие поручает обработку ПДн третьим сторонам только с согласия субъекта ПДн или при наличии иного законного основания при обязательном условии соблюдения стороной, осуществляющей обработку ПДн по поручению Предприятия, соблюдения правил обработки и обеспечения безопасности ПДн, установленных Предприятием.

При обработке ПДн по поручению третьих сторон Предприятия соблюдаются установленные соответствующими поручениями (договорами) требования к обеспечению безопасности ПДн.

В поручении на обработку ПДн должны быть в обязательном порядке определены:

- перечень действий (операций) с ПДн, которые будут совершаться лицом (перечень действий не должен противоречить целям и действиям, заявленным перед субъектом – в договоре, согласии и т. д.);
- цели обработки (цели не должны противоречить целям, заявленным перед субъектом – в договоре, в согласии и т. д.);
- обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке;
- требования к защите ПДн (требования по защите, предъявляемые к лицу, осуществляющему обработку, не должны быть выше требований, выполняемых самим оператором – в идеальном случае требования должны быть идентичны).

8. Контроль защищенности персональных данных

На Предприятии на этапах создания и эксплуатации СЗПДн осуществляются выявление (поиск), анализ и устранение уязвимостей в ИСПДн, включающее:

- выявление уязвимостей, связанных с ошибками кода ПО, ПО СЗИ, установкой и настройкой СЗИ;
- разработка и анализ отчетов о результатах поиска уязвимостей с планом мероприятий по их устранению;
- устранение выявленных уязвимостей, в том числе путем установки обновлений ПО;
- информирование Ответственного за обработку и защиту информации о результатах поиска уязвимостей и достаточности мер по их устранению.

Получение и установка обновлений осуществляется только из доверенных источников, при установке обновлений осуществляется проверка соответствия версий общесистемного, прикладного и специального ПО. При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты.

Администратор ИС осуществляет контроль работоспособности ПО, проверку правильности функционирования ПО и СЗИ, контроль соответствия настроек ПО и СЗИ параметрам настроек, приведенных в эксплуатационной документации на СЗИ, восстановление работоспособности ПО и СЗИ.

На Предприятии проводится контроль состава технических средств, ПО и СЗИ, применяемых в ИСПДн, включающее:

- контроль соответствия состава технических средств, ПО и СЗИ приведенному в эксплуатационной документации с целью поддержания актуальной конфигурации ИСПДн и принятие мер, направленных на устранение выявленных недостатков;
- контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава ИСПДн несанкционированно установленных (удаленных) технических средств, ПО и СЗИ.

9. Взаимодействие с субъектами персональных данных и органами власти

9.1 Взаимодействие с субъектами персональных данных

Предприятие осуществляет учет и реагирование на все запросы субъектов ПДн. В случае получения запроса от субъекта, касающегося обработки его ПДн, Ответственный за обработку и защиту информации осуществляет регистрацию запроса и организует реагирование на запрос в соответствии с настоящим Положением и требованиями законодательства Российской Федерации. Субъект в обязательном порядке уведомляется о результатах реагирования на его запрос.

9.2 Взаимодействие с органами власти

Взаимодействие с органами власти осуществляется в соответствии с законодательством Российской Федерации.

Оценка законности и мотивированности запросов органов власти на предоставление информации о процессах обработки ПДн (в т. ч. на предоставление ПДн) проводится Ответственным за обработку и защиту информации.

В случае получения запроса от органов власти, касающихся обработки ПДн, Ответственный за обработку и защиту информации осуществляет регистрацию запроса и организует реагирование на запрос в соответствии с настоящим Положением, требованиями законодательства Российской Федерации и указаниями в запросе органа власти. Орган власти уведомляется о реагировании на запрос в срок, установленный в тексте запроса.

10. Ответственность

За нарушение требований настоящего Положения работники Предприятия несут персональную ответственность в соответствии с действующим законодательством Российской Федерации.