Негосударственное частное общеобразовательное учреждение
«Международная школа «АЛЬНАИР»
НЧОУ «Международная школа «АЛЬНАИР»

УТВЕРЖДЕНО
Решением Учредителя НЧОУ
«Международная школа «АЛЬНАИР»
№23/12 от 22.12.2023
Генеральный директор ООО «СИРИУС»
_____ Желтоухова А.А.
«22» декабря 2023 года

Положение
о порядке обработки и защиты персональных и биометрических персональных данных в НЧОУ «Международная школа «АЛЬНАИР»

(новая редакция)

Московская область, город Истра,
2023 год

1. Порядок обработки персональных и биометрических персональных данных.

1.1 Определения и основные принципы.

1.1.1. Персональными данными (далее также – ПД, ПДн) признается любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.1.2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.1.3. Субъектом персональных данных является лицо, к которому указанные персональные данные относятся.

1.1.4. Положение о порядке обработки и защиты персональных и биометрических персональных данных в НЧОУ «Международная школа «АЛЬНАИР» (далее - **Положение**) издано и применяется в НЧОУ «Международная школа «АЛЬНАИР» (далее – **Оператор, Учреждение**) в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – **Федеральный закон**).

1.1.5. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законодательством.

1.1.6. К биометрическим персональным данным (далее также – ПД, ПДн) относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

1.1.7. Обработка биометрических персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законодательством, в том числе:

- соблюдение прав Субъектов персональных данных при обработке их ПДн;
- осуществление обработки ПДн на законной и справедливой основе для достижения целей их обработки;
- недопущение обработки ПДн, которые не отвечают целям обработки, избыточны или содержатся в базах данных, цели обработки которых несовместимы;
- обеспечение точности, достаточности и актуальности ПДн при их обработке по отношению к целям их обработки;
- хранение ПДн не дольше, чем этого требуют цели обработки;
- уничтожение или обезличивание ПДн при достижении целей их обработки или в случае утраты необходимости в достижении этих целей.

1.1.8. Обработка ПДн осуществляется при наличии согласия в письменной форме субъекта персональных данных на обработку его персональных и биометрических персональных данных.

1.1.9. Действующее законодательство предоставляет субъектам персональных данных следующие основные права:

1.1.9.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1.1.9.1.1. подтверждение факта обработки персональных данных Оператором;

1.1.9.1.2. правовые основания, цели и применяемые Оператором способы обработки персональных данных;

1.1.9.1.3. наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

1.1.9.1.4. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

1.1.9.1.5. сроки обработки персональных данных, в том числе сроки их хранения;

1.1.9.1.6. порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законодательством;

1.1.9.1.7. информацию об осуществленной или о предполагаемой трансграничной передаче данных;

1.1.9.1.8. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

1.1.9.1.9. информацию о способах исполнения Оператором обязанностей, установленных статьей 18.1 Федерального закона;

1.1.9.1.10. иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

1.1.9.2. право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами;

1.1.9.3. субъект персональных данных вправе требовать от Оператора 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;

1.1.9.4. субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

1.1.10. Учреждение как Оператор персональных и биометрических персональных данных строго соблюдает действующее законодательство о персональных данных и принимает меры, необходимые и достаточные для обеспечения их конфиденциальности в соответствии с Положением. К таким мерам, в частности, относятся:

1) назначение ответственных лиц за организацию обработки и обеспечение безопасности персональных и биометрических персональных данных;
2) применение правовых, организационных и технических мер по обеспечению безопасности персональных и биометрических персональных данных, в том числе:

a. разграничение доступа к персональным и биометрических персональным данным;

b. возложение на работников и контрагентов, получающих персональные и биометрические персональные данные, обязательств по обеспечению их конфиденциальности;

c. защита персональных и биометрических персональных данных в информационных системах посредством аппаратных и программных средств;

d. обеспечение регистрации и учета всех действий, совершаемых с персональными и биометрическими персональными данными в информационных системах персональных данных;

e. ограничение доступа к средствам обработки информации, с помощью которых возможно получить доступ к информационным системам, содержащим персональные данные;

f. ограничение доступа в помещения, в которых персональные и биометрические персональные данные хранятся вне информационных систем (на бумажных и аналогичных носителях);

g. хранение персональных и биометрических персональных данных в любом формате исключительно в охраняемых помещениях с соблюдением противопожарных и иных технических норм с осуществлением учета носителей персональных данных;

h. уничтожения персональных и биометрических данных согласно требованиям Федерального закона.

3) в отношении персональных и биометрических персональных данных установлен режим конфиденциальности;
4) осуществляется регулярный внутренний контроль соответствия обработки персональных и биометрических персональных данных требованиям действующего законодательства.

1.1.11. Учреждение может возлагать выполнение отдельных мероприятий по защите персональных и биометрических персональных данных на сторонние организации в соответствии с договором об оказании услуг, обязывающим соблюдать режим конфиденциальности и требования действующего законодательства в отношении переданных ПДн. В случае заключения договоров с третьими лицами, в рамках которых предполагается передача персональных и биометрических персональных данных, в таких договорах должна предусматриваться обязанность третьих лиц соблюдать требования действующего законодательства в отношении персональных и биометрических персональных данных.

1.1.12. Учреждение не осуществляет обработку персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, когда такие персональные данные являются общедоступными. Учреждение может в виде

исключения осуществлять обработку персональных данных, касающихся состояния здоровья, при условии, что (1) получено предварительное письменное согласие субъекта персональных данных на такую обработку, и (2) осуществление обработки указанной категории персональных данных необходимо в рамках хозяйственной деятельности Учреждения, в том числе для реализации прав его работников.

1.1.13. Решения, порождающие юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, не могут приниматься Учреждением на основании исключительно автоматизированной обработки персональных данных.

1.1.14. Предоставление (передача) персональных и биометрических персональных данных, обрабатываемых Учреждением, в адрес третьих лиц (т.е. юридических лиц и физических лиц, не являющихся работниками Учреждения) допускается лишь при наличии письменного согласия субъекта персональных данных на такое их распространение или в случае, когда такое распространение прямо разрешено законом, при этом все условия, предусмотренные Положением (в т.ч. п. 1.2.1) должны неукоснительно соблюдаться. Ни в каких случаях не допускается передача ПДн лицам, полномочия которых на получение соответствующих ПДн невозможно установить достоверно, а также способами, не обеспечивающими конфиденциальность передаваемых данных (в том числе по телефону, по электронной почте без использования соответствующих мер защиты)

1.1.15. В Учреждении приказом директора назначено соответствующее уполномоченное подразделение (уполномоченное лицо), ответственное за организацию обработки и защиты персональных и биометрических персональных данных (далее - «Уполномоченное подразделение по защите», «Уполномоченное лицо»). В случае отсутствия такого приказа, ответственным за защиту персональных и биометрических персональных данных является директор.

1.1.16. С письменного согласия субъекта персональных данных к общедоступным персональным и биометрическим персональным данным на период действия трудового договора могут быть отнесены следующие персональные и биометрические персональные данные: фамилия, имя, отчество, место работы, дата приема на работу, подразделение, должность, данные об образовании и квалификации, квалификационная категория, трудовой стаж, координаты рабочего места, личный и табельный номер, рабочий телефон, рабочий электронный адрес, портретный снимок.

1.1.17. Общедоступные персональные и биометрические персональные данные могут быть размещены в общедоступных корпоративных источниках (справочниках Учреждения).

1.1.18. Письменное согласие субъекта персональных данных на обработку своих персональных и биометрических персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
3) наименование и адрес Учреждения;
4) цели обработки персональных и биометрических персональных данных;
5) перечень персональных и биометрических персональных данных, на обработку которых дается согласие субъекта персональных данных;
6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных и биометрических персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными и биометрическими персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки персональных и биометрических персональных данных;
8) срок, в течение которого действует согласие, а также порядок его отзыва.

1.1.19. В целях обеспечения прав и свобод человека и гражданина Учреждение и его представители при обработке персональных и биометрических персональных данных субъекта персональных данных должны соблюдать следующие общие требования:

1) при определении объема и содержания обрабатываемых персональных и биометрических персональных данных Учреждение должно руководствоваться Конституцией РФ, Трудовым кодексом РФ, Гражданским кодексом РФ и иными федеральными законами;
2) в той степени, в которой это требуется согласно действующему законодательству и Положению, Учреждение знакомит субъектов персональных данных и их представителей с документами Учреждения, устанавливающими порядок обработки их персональных и биометрических персональных данных;
3) в процессе хранения персональных и биометрических персональных данных должны обеспечиваться:
   - соблюдение требований нормативных документов, устанавливающих правила хранения конфиденциальных сведений;
   - сохранность имеющихся данных, ограничение доступа к ним в соответствии с законодательством РФ и Положением;
   - контроль достоверности и полноты персональных и биометрических персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

1.1.20. Учреждение использует в процессе обработки персональных и биометрических персональных данных следующие способы обработки персональных и биометрических персональных данных:

1) автоматизированную обработку персональных и биометрических персональных данных;
2) обработку персональных и биометрических персональных данных без использования средств автоматизации.

1.1.21. При передаче персональных и биометрических персональных данных, за исключением общедоступных персональных данных, должны соблюдаться следующие требования:

1) не сообщать персональные данные субъекта персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных федеральным законом;
2) не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;
3) если иное не предусмотрено законом, передавать персональные и биометрические персональные данные только при условии принятия на себя лицами, их получающими от Учреждения, обязательства по охране конфиденциальности и соблюдению ограничений использования ПДн (в частности, такие данные могут быть использованы лишь в целях, для которых они переданы (сообщены)) и требовать от этих лиц подтверждения того, что указанные обязательства соблюдаются;
4) осуществлять передачу персональных и биометрических персональных данных в пределах Учреждения и третьим лицам в соответствии с Положением;

5) разрешать доступ к персональным и биометрическим персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные и биометрические персональные данные, которые необходимы для выполнения конкретной функции;

6) передавать персональные и биометрические персональные данные работника представителям работников в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными и биометрическими персональными данными работника, которые необходимы для выполнения указанными представителями их функции, при этом предоставление персональных и биометрических персональных данных субъектов персональных данных внешним для Учреждения потребителям по устному или телефонному запросу не допускается.

1.1.22. Режим конфиденциальности персональных и биометрических персональных данных снимается в случаях их обезличивания или по истечении срока их хранения, установленного законодательством РФ об архивном деле, или продлевается на основании, если иное не определено законом.

1.2 Доступ к персональным и биометрическим персональным данным.

1.2.1 Обязательными условиями доступа к персональным и биометрическим персональным данным, обрабатываемым Учреждением, как для его работников, так и для его контрагентов, являются:

1) ознакомление под роспись с Перечнем обрабатываемых Учреждением персональных и биометрических персональных данных и Положением;
2) принятие обязательства по обеспечению конфиденциальности персональных и биометрических персональных данных осуществляется путем подписания Соглашения о конфиденциальности и неразглашении информации.

1.2.2 Неограниченный доступ ко всем персональным и биометрическим персональным данным, обрабатываемым Учреждением, предоставляется директору Учреждения.

1.2.3 Директор Учреждения вправе предоставлять доступ к персональным и биометрическим персональным данным, обрабатываемым Учреждением, путем утверждения списка должностей сотрудников, допущенных к работе с персональными и биометрическими персональными данными. К персональным и биометрическим персональным данным также могут быть допущены сотрудники, замещающие должности, входящие в указанный список, при обязательном выполнении п. 1.2.1 Положения.

1.2.4 Директор Учреждения вправе своими приказами определить работников Учреждения, уполномоченных на предоставление допуска к персональным и биометрическим персональным данным (далее – «Лица со специальными полномочиями»). Лица со специальными полномочиями отражены в электронных Реестрах ИСПДн и АПД.

1.2.5 Лица со специальными полномочиями принимают решение о допуске работников подразделений Учреждения, работников организаций, оказывающих услуги Учреждению по договору, к персональным и биометрическим персональным данным работников, контрагентов Учреждения и других субъектов ПДн для выполнения своих должностных обязанностей или условий договора, и организуют учет сотрудников, допущенных к ПДн.

1.2.6 При увольнении работника, имеющего доступ к обработке персональных и биометрических персональных данных, его учетная запись (права доступа в ИСПДн) должна быть заблокирована.

1.2.7 Во избежание сомнений соблюдение условий допуска к персональным и биометрическим персональным данным, обрабатываемым Учреждением (п.1.2.1 Положения), является обязательным для всех лиц, указанных в п. п. 1.2.2-1.2.6 Положения.

1.3 Перечень персональных данных, обрабатываемых Учреждением.

1.3.1. Перечень персональных данных, обрабатываемых Учреждением (далее – «Перечень»), утверждается и в дальнейшем актуализируется директором Учреждения. В Перечне указываются персональные данные по категориям граждан, чьи данные обрабатываются в Учреждении, и видам персональных данных.

1.3.2. Для каждой цели обработки указывается:

1) категория и перечень обрабатываемых ПДн;
2) категории субъектов, персональные данные которых обрабатываются;
3) основание для обработки;
4) способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований.

1.3.3. Непосредственно персональные данные в Перечень не включаются.

1.3.4. Директор ведет:

1) Реестр информационных систем персональных и биометрических персональных данных (далее – ИСПДн), в котором содержится информация обо всех имеющихся в Учреждении ИСПДн, представляющих собой совокупность персональных и биометрических персональных данных, содержащихся в базах данных.
2) Реестр архива персональных и биометрических персональных данных (далее - АПД), т.е. совокупности персональных и биометрических персональных данных на бумажном или ином носителе, объединенных на основе критерия места хранения и цели обработки, обработка которых осуществляется без использования средств автоматизации. Обработка персональных и биометрических персональных данных считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными и биометрическими персональными данными, как использование, уточнение, распространение, уничтожение персональных и биометрических персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.3.5. Реестры ведутся в электронном виде, непосредственно персональные данные в Реестры не включаются (за исключением ПДн лиц со специальными полномочиями).

1.3.6. Лица, ответственные за работу с ИСПДн и АПД, обязаны незамедлительно информировать директора, о любых известных изменениях, подлежащих отражению в Реестре. Директор на регулярной основе запрашивает у указанных выше лиц информацию о текущих характеристиках ИСПДн и АПД, необходимых для ведения Реестра.

1.4 Обработка запросов субъектов персональных данных.

Запросы субъекта ПДн могут осуществляться в письменной или устной форме согласно (1) Трудового Кодекса Российской Федерации (документы, связанные с трудовой деятельностью, их копии) или (2) согласно 152-ФЗ «О персональных данных». На основании 152-ФЗ субъект ПДн вправе требовать от Оператора:

1) подтверждение факта обработки ПДн;
2) правовые основания, цели обработки ПДн и применяемые Оператором способы обработки ПДн;
3) получения сведений об Операторе, о месте его нахождения;
4) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
5) сроки обработки ПДн, в том числе сроки их хранения;
6) уточнения своих ПДн, их блокирования или уничтожения, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
7) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу.

1.5 Уничтожение ПДн.

1.5.1. Учреждение обязано уничтожать ПДн в случаях окончания срока обработки ПДн, отзыва согласий на обработку ПДн, достижения цели обработки ПДн, по требованию Роскомнадзора и в других случаях, установленных законодательством.

1.5.2. В случае обращения субъекта персональных данных к Оператору с требованием о прекращении обработки персональных данных Оператор обязан в срок, не превышающий десяти рабочих дней с даты получения Оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных Федеральным законом. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Подтверждение уничтожения персональных данных в случаях, предусмотренных настоящим пунктом, осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.

1.5.3. Уничтожение ПДн без использования средств автоматизации осуществляется в порядке, применяемом в Учреждении.

1.5.4. Учреждение вправе заключать договоры с третьими лицами на оказание услуг по уничтожению материальных носителей ПДн. При этом в договоре должны быть определены порядок уничтожения ПДн, порядок взаимодействия третьего лица с Учреждением в части обработки запросов на уничтожения и предоставления отчетной документации по уничтожению материальных носителей ПДн.

1.5.5. В случае, если обработка персональных данных осуществляется Оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

1.5.6. В случае, если обработка персональных данных осуществляется Оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных.

Выгрузка из журнала должна содержать обязательные сведения, установленные Роскомнадзором.

1.5.7. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

2. Защита персональных данных и биометрических персональных данных в ИСПДн.

2.1 Основные принципы защиты персональных и биометрических персональных данных в ИСПДн.

2.1.1. При обработке персональных и биометрических персональных данных в информационной системе Учреждение обеспечивает:

(1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным и биометрическим персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

(2) своевременное обнаружение фактов несанкционированного доступа к персональным и биометрическим персональным данным;

(3) недопущение воздействия на технические средства автоматизированной обработки персональных и биометрических персональных данных, в результате которого может быть нарушено их функционирование;

(4) возможность незамедлительного восстановления персональных и биометрических персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

(5) постоянный контроль за обеспечением уровня защищенности персональных и биометрических персональных данных.

2.2 Действия в случае обнаружения нарушения правил использования ИСПДн.

2.2.1. Лицо, обнаружившее факт нарушения правил использования ИСПДн (несанкционированные доступ, изменение ИСПДн, несоблюдение условий хранения персональных и биометрических персональных данных и т.п.), обязано сообщить об этом директору Учреждения.

2.2.2. По факту обращения, указанного в п. 2.2.1, директор инициирует проверку, для проведения которой могут привлекаться любые необходимые специалисты Учреждения.

2.2.3. Проверка должна быть проведена и закончена в течение 10 рабочих дней с момента обнаружения факта нарушения правил пользования ИСПДн.

2.2.4. Срок, предусмотренный п. 2.2.3 Положения, может быть продлен, но не более чем на 20 рабочих дней.

2.2.5. Результаты проверки должны быть оформлены в виде заключения, содержащего:

2.2.5.1. описание выявленных фактов нарушения правил пользования ИСПДн;

2.2.5.2. выводы о причинах и условиях, приведших к допущенным нарушениям;

2.2.5.3. предложения о дальнейших действиях, связанных с выявленными нарушениями (инициирование юридических процедур, направленных на привлечение виновных лиц к ответственности и взыскании с них сумм причиненного ущерба, принятие мер по минимизации негативных последствий нарушения для субъектов персональных данных и Учреждения и т.п.);

2.2.5.4. предложения по устранению причин и условий, приведших к допущенным нарушениям (совершенствование ИСПДн, изменение режима доступа к ней, пересмотр результатов классификации ИСПДн и т.п.).

3. Особенности обработки и защиты персональных и биометрических персональных данных в АПД.

3.1 Основные способы защиты персональных и биометрических персональных данных в АПД.

3.1.1 Лица, осуществляющие обработку персональных и биометрических персональных данных в АПД, наряду с соблюдением условий, установленных п. 1.2.1 Положения, должны быть проинформированы об особенностях и правилах такой обработки, установленных Положением, об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждены Постановлением Правительства РФ от 15 сентября 2008 г. № 687) (далее в настоящем разделе – «Правила»), иными нормативными актами Российской Федерации и Положением.

3.1.2 Все ПДн, имеющие различные цели обработки, должны храниться отдельно.

3.1.3 Доступ к АПД предоставляется исключительно лицам, имеющим допуск к соответствующим АПД (их частям).

3.1.4 Материальные носители, входящие в состав АПД и содержащие персональные и биометрические персональные данные, должны соответствовать п. п. 4,5,7,8, 9 и 11 Правил.

3.2 Хранение материальных носителей, содержащих персональные и биометрические персональные данные в составе АПД.

3.2.1 В целях обеспечения сохранности персональных и биометрических персональных данных в составе АПД и исключения несанкционированного доступа к ним Учреждением приняты следующие меры:

1) ограничение и контроль доступа в помещения, в которых хранятся АПД;
2) осуществление обработки персональных и биометрических персональных данных в АПД способами, исключающими доступ к ним не уполномоченных лиц, в том числе посредством дистанционного наблюдения;
3) поддержание помещений, в которых хранятся АПД, в технически пригодном состоянии, в т.ч. в строгом соответствии с противопожарными нормами и правилами;
4) недопустимость перевода документов АПД в электронный формат, за исключением случаев использования в составе ИСПДн в соответствии с Положением;
5) возложение на работников Учреждения обязанности по соблюдению Положения, Правил и иных нормативных актов Российской Федерации при обработке персональных и биометрических персональных данных в составе АПД, привлечение работников к дисциплинарной ответственности за нарушение данной обязанности.

3.2.2 Меры, перечисленные в п. 3.2.1 Положения, реализуются безусловно, непрерывно и в отношении всех имеющихся в распоряжении Учреждения АПД.

3.2.3 Ответственность за реализацию мер, предусмотренных п. 3.2.1 Положения в отношении каждого конкретного АПД, возлагается на лицо, ответственное за работу с ним.

3.3 Действия в случае обнаружения нарушения правил использования АПД.

3.3.1. Лицо, обнаружившее факт нарушения правил использования АПД (несанкционированный доступ, несоблюдение мер, перечисленных в п. 3.2.1 Положения и т.п.), обязано незамедлительно сообщить об этом директору Учреждения.

3.3.2. По факту обращения, указанного в п. 3.3.1, директор инициирует проверку, для проведения которой могут привлекаться любые необходимые специалисты Учреждения.

3.3.3. Проверка должна быть проведена и закончена в течение 10 рабочих дней с момента обнаружения факта нарушения правил пользования АПД.

3.3.4. Срок, предусмотренный п. 3.3.3 Положения, может быть продлен директором, но не более чем на 20 рабочих дней.

3.3.5. Результаты проверки должны быть оформлены в виде заключения (представления), содержащего:

1) описание выявленных фактов нарушения правил пользования АПД;
2) выводы о причинах и условиях, приведших к допущенным нарушениям;
3) предложения о дальнейших действиях, связанных с выявленными нарушениями (инициирование юридических процедур, направленных на привлечение виновных лиц к ответственности и взыскании с них сумм причиненного ущерба, принятие мер по минимизации негативных последствий нарушения для субъектов персональных данных и Учреждения и т.п.);
4) предложения по устранению причин и условий, приведших к допущенным нарушениям (совершенствование АПД, изменение режима доступа к нему и т.п.).

3.3.6. Результаты проверки должны быть доведены до сведения лица, ответственного за работу с АПД, не позднее пяти рабочих дней с момента их оформления.

4. Ответственность

Неисполнение или ненадлежащее исполнение Положения работниками, ответственными за его исполнение в силу должностных обязанностей, влечет за собой применение к ним мер дисциплинарного или иного воздействия, предусмотренных действующим законодательством и локальными нормативными актами Учреждения.