Приложение 1

УТВЕРЖДАЮ

Директор школы _____ Э.А. Исаева

Приказ№50-Д от «31 » августа 2020 г

Политика МКОУ «Тандовская СОШ» в отношении персональных данных

1. Общие положения

Политика обработки персональных данных (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ-152).

Настоящая Политика определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных в муниципальном казенном общеобразовательном учреждении «Тандовская средняя общеобразовательная школа» (далее – Оператор) с целью защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В Политике используются следующие основные понятия:

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических средств;

обезличивание персональных данных – действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных;

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;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

персональные данные – любая информация, относящаяся к прямо или косвенно

определенному или определяемому физическому лицу (субъекту персональных данных);

предоставление персональных данных – действия, направленные на раскрытие персональных

данных определенному лицу или определенному кругу лиц;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

трансграничная передача персональных данных –передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;

уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) результате которых уничтожаются материальные носители персональных данных.

Оганизация обязана опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике обработки персональных данных в соответствии с ч. 2 ст. 18.1. ФЗ-152.

2. Принципы и условия обработки персональных данных

2.1. Принципы обработки персональных данных

Обработка персональных данных у Оператора осуществляется на основе следующих принципов:

- законности и справедливой основы;
- ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;
- недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработки только тех персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- недопущения обработки персональных данных, избыточных по отношению к заявленным целям их обработки;
- обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;
- уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Оператором допущенных нарушений персональных данных, если иное не предусмотрено федеральным законом.

2.2. Условия обработки персональных данных

Оператор производит обработку персональных данных при наличии хотя бы одного из следующих условий:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее -

общедоступные персональные данные); – осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2.3. Конфиденциальность персональных данных

Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.4. Общедоступные источники персональных данных

В **целях** информационного обеспечения у Оператора могут создаваться общедоступные источники персональных данных субъектов, в том числе справочники и адресные книги. В общедоступные источники персональных данных с письменного согласия субъекта могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адрес электронной почты и иные персональные данные, сообщаемые субъектом персональных данных.

Сведения о субъекте должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта либо по решению суда или иных уполномоченных государственных органов.

2.5. Специальные категории персональных данных

Обработка Оператором специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, не производится.

Обработка Оператором специальных категорий персональных данных, касающихся состояния здоровья, производится в случаях, предусмотренных ФЗ № 152 «О персональных данных» от 27.07.2006 статья 10 часть 2 подпункты 1, 2.3, 3, 4.

2.6. Биометрические персональные данные

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность – биометрические персональные данные – могут обрабатываться Оператором только при наличии согласия в письменной форме субъекта.

2.7. Поручение обработки персональных данных другому лицу

Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные ФЗ-152.

2.8. Трансграничная передача персональных данных

Трансграничная передача персональных данных Оператором не производится.

3. Права субъекта персональных данных

3.1. Согласие субъекта персональных данных на обработку его персональных данных

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в ФЗ-152, возлагается на Оператора.

3.2. Права субъекта персональных данных

Субъект персональных данных имеет право на получение у Оператора информации, касающейся обработки его персональных данных, если такое право не ограничено в соответствии с федеральными законами. 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, а также принимать предусмотренные законом меры по защите своих прав.

Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если Организация не докажет, что такое согласие было получено.

Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в вышеуказанных целях.

Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные

интересы, за исключением случаев, предусмотренных федеральными законами, или при наличии согласия в письменной форме субъекта персональных данных.

Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований ФЗ-152 или иным образом нарушает его правасвободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в Уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4. Обеспечение безопасности персональных данных

Безопасность персональных данных, обрабатываемых Оператором, обеспечивается реализацией правовых, организационных и технических мер, необходимых для обеспечения требований федерального законодательства в области защиты персональных данных.

Для предотвращения несанкционированного доступа к персональным данным Оператором применяются следующие организационно-технические меры:

- назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- ограничение состава лиц, имеющих доступ к персональным данным;
- ознакомление субъектов с требованиями федерального законодательства и нормативных документов Оператора по обработке и защите персональных данных;
- организация учета, хранения и обращения носителей информации;
- определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;
- разработка на основе модели угроз системы защиты персональных данных;
- проверка готовности и эффективности использования средств защиты информации;
- разграничение доступа пользователей к информационным ресурсам и программно-аппаратным средствам обработки информации;
- регистрация и учет действий пользователей информационных систем персональных данных;
- использование антивирусных средств и средств восстановления системы защиты персональных данных;
- применение в необходимых случаях средств межсетевого экранирования, обнаружения вторжений, анализа защищенности и средств криптографической защиты информации;
- организация пропускного режима на территорию Оператора, охраны помещений с техническими средствами обработки персональных данных.

5. Заключительные положения

Иные права и обязанности Оператора как оператора персональных данных определяются законодательством Российской Федерации в области персональных данных.

Должностные лица Оператора, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Приложение 2

УТВЕРЖДАЮ

Директор школы _____Э.А. Исаева

Приказ№50-Д от «31 » августа 2020 г

Правила осуществления внутреннего контроля соответствия персональных данных законодательству РФ

1. **Общие положения**

1.1. Настоящие Правила осуществления внутреннего контроля соответствия персональных данных законодательству РФ в МКОУ «Тандовская СОШ» (далее - Правила) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством, в том числе Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных".

1.2. Правила разработаны с учетом требований Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 21.03.2011 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами", иных нормативных правовых актов.

2. **Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства**

2.1. Цель проведения внутреннего контроля состоит в проверке и оценке соответствия обеспечения безопасности персональных данных (далее - ПДн) требованиям действующего законодательства, в том числе Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", политики школы №37 в отношении обработки ПДн.

2.2. При проведении контроля используются процедуры документальной проверки, опрос и интервью с работниками школы. При необходимости уточнения результатов документальной проверки, опросов и интервью в рамках внутреннего контроля в качестве дополнительного способа может применяться "проверка на месте", которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования.

2.3. При проведении внутреннего контроля должно быть обеспечено документальное и, если это необходимо, техническое подтверждение того, что:

- политика в отношении обработки ПДн соответствует требованиям законодательства Российской Федерации;
- организационная структура обеспечения безопасности ПДн создана;
- процессы выполнения требований безопасности ПДн исполняются и удовлетворяют поставленным целям;
- защитные меры (межсетевые экраны, средства защиты информации от несанкционированного доступа и т.п.) настроены и используются правильно:
- остаточные риски безопасности ПДн оценены и остаются приемлемыми;
- рекомендации предшествующих проверок реализованы.

2.4. При проведении внутреннего контроля могут использоваться журналы средств защиты информации для выявления попыток несанкционированного доступа к защищаемым ресурсам, а также журнал учета нештатных ситуаций информационных систем персональных данных (далее - ИСПДн), ведущийся лаборантом.

3. **План внутренних проверок режима защиты персональных данных**

N п/п	Мероприятие	Периодичность	Исполнитель
1.	Контроль выполнения требований по режиму доступа в защищаемые помещения и на автоматизированные рабочие места, на которых производится обработка персональных данных	Постоянно	Ответственные работники
2.	Контроль соблюдения правил работы с носителями персональных данных	Постоянно	Ответственные работники
3.	Контроль целостности средств вычислительной техники, используемых для обработки персональных данных. Контроль корректной работы системного и прикладного программного обеспечения, средств защиты информации. Контроль состава технических средств.	Постоянно	Ответственные работники
4.	Контроль за соблюдением режима обработки персональных данных	Постоянно	Ответственные работники
5.	Пересмотр и, при необходимости, корректировка учетных записей пользователей	Еженедельно	Ответственный за АСИОУ
6.	Контроль за выполнением антивирусной защиты, неизменностью настроек средств антивирусной защиты и своевременным обновлением антивирусных баз	Еженедельно	Зам. директора по АХР
7.	Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации	Еженедельно	Лаборант
8.	Контроль за обеспечением резервного копирования, проверка работоспособности резервных копий	Ежемесячно	Ответственный за АСИОУ

9.	Поддержание в актуальном состоянии организационно-распорядительных документов	Ежемесячно	Заместитель директора, ответственный за проведение работы по защите персональных данных
10.	Пересмотр организационно-распорядительной документации, регламентирующей порядок обработки персональных данных и требования по защите персональных данных, с учетом проводимых мероприятий по контролю	Ежегодно По факту изменения целей, технологии или иного значимого аспекта информационной безопасности	Заместитель директора, ответственный за проведение работы по защите персональных данных
11.	Обучение и повышение осведомленности работников в области защиты ПДн	Ежегодно В случае изменения законодательной базы, внутренних нормативных актов в области защиты персональных данных не позднее одного месяца с момента изменений Раз в	Заместитель директора, ответственный за проведение работы по защите персональных данных
12.	Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных	три года	Заместитель директора, ответственный за проведение работы по защите персональных данных
13.	Контроль заведения и удаления учетных записей пользователей	Прием/увольнение работника	Ответственный за АСИОУ

Приложение №3

УТВЕРЖДАЮ

Директор школы _____Э.А. Исаева

Приказ№50-Д от «31 » августа 2020 г

Порядок доступа в помещения с обработкой персональных данных

1. Порядок доступа работников в помещения, в которых ведёт обработку персональных данных МКОУ «Тандовская СОШ» (далее — Оператор), устанавливается в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
2. Порядок доступа в помещения распространяется на всех работников Оператора.
3. В помещениях, в которых хранятся и обрабатываются персональные данные, должна быть исключена возможность бесконтрольного проникновения посторонних лиц и несанкционированного доступа к персональным данным.
4. В контролируемые помещения допускаются только работники, уполномоченные на обработку персональных данных в соответствии с данным приказом. Иные лица допускаются только в присутствии допущенных работников Оператора.
5. Входные двери помещений оборудуются замками, гарантирующими надёжное закрытие в нерабочее время и при выходе из помещения в рабочее время. В случае утери ключей, замок заменяется.
6. Уборка в помещениях, где хранятся и обрабатываются персональные данные, производится только в присутствии допущенного работника.
7. При обнаружении повреждений замков или других признаков, указывающих на возможное проникновение посторонних лиц в помещения, в которых ведется обработка персональных данных, составляется акт и о случившемся немедленно ставится в известность ответственный за обработку персональных данных.
8. Контроль за соблюдением порядка доступа в помещение, в котором ведется обработка персональных данных, проводится лицом, заместителем директором по АХР.

Приложение №4
УТВЕРЖДАЮ
Директор школы _____Э.А. Исаева
Приказ№50-Д от «31 » августа 2020 г

Порядок пользования сервером, содержащим персональные данные

1. Порядок доступа работников к серверу, содержащим персональные данные МКОУ «Тандовская СОШ» (далее — Оператор), устанавливается в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
2. Порядок доступа к серверу распространяется на всех работников Оператора.
3. Доступ к серверу, содержащему персональные данные разрешается работникам в соответствии с таблицей

Перечень работ, требующих физического доступа к серверам.

№ п/п	Наименование работ	Описание	Ответственные за выполнение	Обоснование для физического доступа
1	Перезагрузка сервера	Выполняется нажатием кнопки Reset на **сервере**	Лаборант	Невозможность выполнения перезагрузки удаленным способом
2	Работы по техническому обслуживанию серверов	Замена, установка, переустановка оборудования и ПО	Лаборант	Работа с серверным оборудованием невозможна без физического контакта

4. В случае возникновения необходимости доступа в серверное помещение лицам, не входящих в список допуска, оформляется заявка с обоснованием физического доступа. Данная заявка рассматривается и подписывается директором. При наличии разрешительного документа лица, которым разрешен физический доступ к серверу, должны сопровождаться лаборантом.
5. Лица, имеющие доступ в серверное помещение несут ответственность за: надлежащее выполнение своих функциональных обязанностей; обеспечение надлежащих условий сохранности, доступности, конфиденциальности обрабатываемой информации, в рамках своей компетенции. Лица, нарушившие требования настоящего документа, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.

Приложение №5

УТВЕРЖДАЮ

Директор школы _____Э.А. Исаева

Приказ№50-Д от «31 » августа 2020 г

Инструкция
по работе ответственного лица за обеспечение безопасности персональных данных в МКОУ «Тандовская СОШ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности, права и ответственность ответственного лица за обеспечение безопасности персональных данных *в муниципальном казенном общеобразовательном учреждении «*Тандовская СОШ»*»* (далее–Учреждение).

1.2. Ответственное лицо за обеспечение безопасности персональных данных является штатным работником Учреждения и назначается приказом руководителя Учреждения.

1.3. Ответственное лицо за обеспечение безопасности персональных данных (далее-Ответственный) - лицо, отвечающее за организацию и состояние процесса обработки персональных данных в информационных системах персональных данных.

1.4. Решение вопросов организации защиты персональных данных, обрабатываемых в информационных системах Учреждения, входит в прямые трудовые обязанности Ответственного.

1.5. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

1.6. Ответственный в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства, руководящими и нормативными документами ФСТЭК России, а также другими нормативными правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами Учреждения.

1.7. Требования Ответственного, связанные с выполнением им своих трудовых обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к персональным данным.

1.8. Ответственный обладает правами доступа к любым носителям персональных данных Учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Блокирование персональных данных -временное прекращение обработки персональных данных.

2.2.Доступ к информации –возможность получения информации и ее использования.

2.3. Защита информации —деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

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

2.5. Информационная система персональных данных (ИСПДн) –совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.6. Несанкционированный доступ (НСД) –доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.7. Носитель информации -любой материальный объект или среда, используемый для хранения или передачи информации.

2.8. 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.

2.9. Персональные данные -любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.10. Средство защиты информации (СЗИ) –техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

Ответственный обязан:

3.1. Обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации ИСПДн, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью.

3.2. Знать и предоставлять ответственному за организацию обработки персональных данных изменения к списку лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей.

3.3. Проводить инструктаж и консультации пользователей ПЭВМ по соблюдению режима конфиденциальности.

3.4. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

3.5. Организовывать периодический контроль пользователей по соблюдению имирежима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами.

3.6. Взаимодействовать с заместителем по безопасности по вопросам обеспечения и выполнения требований обработки персональных данных.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты.

3.8. Организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

3.9. Контролировать периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации.

3.10. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и по правилам обработки персональных данных.

3.11. Знать перечень и условия обработки персональных данных в Учреждении.

3.12. Знать перечень установленных в подразделениях технических средств, входящихв состав информационных систем, и перечень задач, решаемых с их использованием.

3.13. Обеспечивать соблюдение работниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационных систем.

3.14. Осуществлять контроль за порядком учета, создания, хранения и использования машинных носителей, содержащих персональные данные.

3.15. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем подразделения, сообщать о них Руководителю Учреждения.

3.16. Инструктировать работников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами зашиты информации.

3.17. Знать законодательство Российской Федерации о персональных данных, следить за его изменениями.

3.18. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.19. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

4. ПРАВА ОТВЕТСТВЕННОГО

Ответственный имеет право:

4.1. Требовать от всех пользователей ИСПДн выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

4.2. Инициировать блокирование доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

4.3. Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

4.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

4.5. Обращаться к руководителю подразделения с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

4.6. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

5. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГОДОСТУПА

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. Сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

5.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа Ответственный обязан:

5.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

5.2.2. доложить Руководителю Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

5.2.4. известить ответственного за организацию обработки персональных данных и администратора безопасности о факте несанкционированного доступа.

6. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный несет персональную ответственность за:

6.1.1.соблюдение требований настоящей Инструкции,

6.1.2.правильность и объективность принимаемых решений,

6.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных,

6.1.4. за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.