МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«ГИМНАЗИЯ № 1»

г. Воронеж

УТВЕРЖДАЮ

Директор МБОУ «Гимназия № 1»

_____ Л.А. Валаева

«__1__» сентября 2017 года

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных в информационных системах персональных данных

Содержание

Термины и определения

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения

доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Перечень сокращений

ИСПДн - информационная система персональных данных

НСД - несанкционированный доступ

ПДн - персональные данные

СЗПДн - система защиты персональных данных

ТКУИ - технический канал утечки информации

ФЗ - федеральный закон

ФСБ России - Федеральная служба безопасности

ФСТЭК России - Федеральная служба по техническому и экспортному контролю

1. Общие положения

Настоящее положение определяет цели, задачи, содержание, порядок организации и выполнения мероприятий по защите персональных данных (ПДн), при их обработке в информационной системе персональных данных (далее – ИСПДн) муниципального бюджетного общеобразовательного учреждения «Гимназия № 1» г. Воронежа (далее – Оператор).

Настоящее Положение разработано на основании следующих основных нормативных правовых актов и документов в области обеспечения безопасности ПДн:

- Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при ее обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

ПДн – информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, хранимая, обрабатываемая и циркулирующая на объектах информатизации, является критичным ресурсом и требует постоянного поддержания таких свойств, как конфиденциальность, целостность и доступность, вследствие чего необходимо принятие адекватных мер по обеспечению ее безопасности.

Обработка ПДн в ИСПДн Оператора осуществляется в целях кадрового учета работников учреждения и учета физических лиц, проходящих обучение в

муниципальном бюджетном общеобразовательном учреждении средней общеобразовательной школе № 51.

Защита ПДн, обрабатываемых в ИСПДн, является составной частью работ по созданию и эксплуатации ИСПДн и должна осуществляться в установленном настоящим Положением порядке во взаимосвязи с другими мерами по защите информации.

Основной целью мероприятий по защите ПДн, обрабатываемой в ИСПДн, является снижение риска получения ущерба в условиях действия преднамеренных и непреднамеренных угроз информационной безопасности, а также возможного ущерба в случае утечки ПДн и ожидаемых затрат на достижение поставленной цели. Достижение требуемого уровня безопасности ПДн должно быть обеспечено системным применением организационных, организационно-технических, технических и программно-технических мер на всех этапах разработки, испытаний, внедрения и эксплуатации ИСПДн.

Должностные лица, осуществляющие обработку ПДн, а также организующие эксплуатацию (разработку) ИСПДн, несут персональную ответственность за соблюдение требований настоящего Положения.

Технические и программные средства, применяемые в целях закрытия технических каналов утечки информации (ТКУИ) в ходе ее автоматизированной обработки, а также в целях защиты от несанкционированного доступа (НСД), должны иметь сертификат соответствия требованиям безопасности информации, выданный уполномоченным в области безопасности информации органом, в случае, если применение таких средств будет необходимо для нейтрализации угроз безопасности ПДн.

Действие настоящего Положения распространяется на вопросы, связанные с обработкой ПДн, осуществляемой с использованием средств автоматизации. Вопросы обработки ПДн, осуществляемой без использования средств автоматизации, отражены в Положении об особенностях обработки ПДн, осуществляемых без использования средств автоматизации.

Изменения в текст настоящего Положения вносятся порядком, предусмотренным для его утверждения.

2. Должностные лица Оператора и их обязанности

В целях организации работ по защите ПДн ИСПДн Оператором назначаются следующие лица:

- ответственный за обеспечение безопасности ПДн;
- администратор безопасности;
- пользователи ИСПДн;

Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн назначается ответственный за обеспечение безопасности ПДн соответствующим приказом Оператора. Обязанности, ответственность и права ответственного за обеспечение безопасности ПДн описаны в Инструкции ответственного за обеспечение безопасности ПДн .

Для поддержания установленного режима обеспечения безопасности ПДн в ИСПДн назначается администратор безопасности соответствующим приказом Оператора. Обязанности, ответственность и права администратора безопасности описаны в Инструкции администратора безопасности.

Непосредственное выполнение мероприятий по защите информации (ПДн) в ИСПДн с использованием средств автоматизации возлагается на пользователей ИСПДн. Перечень пользователей ИСПДн определяется Оператором в Перечне лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей. Обязанности, ответственность и права пользователей ИСПДн описаны в Инструкции пользователя ИСПДн.

3. Порядок обработки персональных данных

Обработка ПДн субъектов ПДн осуществляется с их письменного согласия. Оператор обеспечивает защиту ПДн субъектов ПДн от неправомерного их использования или утраты. Обработка ПДн осуществляется как с использованием средств автоматизации, так и без использования средств автоматизации.

При обработке ПДн субъектов ПДн уполномоченные должностные лица Оператора обязаны соблюдать следующие требования:

- объем и характер обрабатываемых ПДн, способы обработки ПДн должны соответствовать целям обработки ПДн;
- защита ПДн субъектов ПДн от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами РФ;
- передача ПДн не допускается без письменного согласия субъекта ПДн, за исключением случаев, установленными федеральными законами. В случае, если лицо, обратившееся к Оператору с запросом, не обладает соответствующими полномочиями на получение ПДн субъекта ПДн либо отсутствует письменное согласие субъекта ПДн на передачу его ПДн, Оператор вправе отказать в предоставлении ПДн. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;
- обеспечение конфиденциальности ПДн субъектов ПДн, за исключением случаев обезличивания ПДн и в отношении общедоступных ПДн;
- хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн не дольше, чем этого требует цели их обработки. Указанные сведения подлежат уничтожению по достижению цели их обработки или в случае утраты необходимости в их достижении, если иное не установлено законодательством РФ. Факт уничтожения ПДн оформляется соответствующим актом;
- опубликование и распространение ПДн субъектов ПДн допускается в случаях, установленных законодательством РФ.

Обработка иных категорий ПДн субъектов ПДн осуществляется с их письменного согласия, за исключением случаев, предусмотренных законодательством РФ в области ПДн. Использование и хранение иных категорий ПДн вне ИСПДн может осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают

защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

В целях обеспечения защиты ПДн субъекты ПДн вправе:

- получать полную информацию о своих ПДн и способе обработки этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, за исключением случаев, предусмотренных 152-ФЗ «О персональных данных»;
- требовать внесения необходимых изменений, уничтожения или блокирования соответствующих ПДн, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- обжаловать в порядке, установленном законодательством РФ, действия (бездействия) уполномоченных должностных лиц.

Классификация ИСПДн осуществляется в порядке, установленным законодательством РФ. Безопасность ПДн, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного доступа к ПДн.

Уполномоченными должностными лицами Оператора при обработке ПДн в ИСПДн должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

Обмен ПДн при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи ПДн к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет, не допускается.

Доступ пользователей ИСПДн к ПДн должен требовать обязательного прохождения процедуры идентификации и аутентификации.

Структурными подразделениями (должностными лицами) Оператора, ответственными за обеспечение безопасности ПДн при их обработке в информационных системах, должно быть обеспечено:

- своевременное обнаружение фактов несанкционированного доступа к ПДн и немедленное доведение этой информации до руководства;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности ПДн;
- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;
- при обнаружении нарушений порядка предоставления ПДн незамедлительное приостановление предоставления ПДн пользователям информационной системы до выявления причин нарушений и устранения этих причин;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

В случае выявления нарушений порядка обработки ПДн в информационных системах, уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

4. Порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных

Под организацией работ по обеспечению безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности мероприятий, осуществляемых на всех стадиях жизненного цикла ИСПДн, согласованных по цели, задачам, месту и времени, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, восстановление нормального функционирования ИСПДн после нейтрализации угроз с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

Безопасность ПДн при их обработке в ИСПДн обеспечивает Оператор или лицо, осуществляющее обработку персональных данных по поручению Оператора в соответствии с законодательством Российской Федерации.

Для выполнения работ по обеспечению безопасности ПДн при их обработке в ИСПДн в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

Для обеспечения защиты информации, содержащейся в ИСПДн, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в ИСПДн;
- разработка СЗИ ИСПДн;
- внедрение СЗИ ИСПДн;
- аттестация ИСПДн по требованиям защиты информации (далее – аттестация ИСПДн) и ввод ее в действие;

- обеспечение защиты информации в ходе эксплуатации аттестованной ИСПДн;
- обеспечение защиты информации при выводе из эксплуатации аттестованной ИСПДн или после принятия решения об окончании обработки информации.

Меры по обеспечению безопасности ПДн реализуются в рамках системы защиты ПДн (СЗПДн), создаваемой в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01.11.2012 г. N 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности ПДн.

Выбор мер по обеспечению безопасности ПДн, подлежащих реализации в ИСПДн в рамках СЗПДн проводится согласно приказу ФСТЭК России от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Порядок разработки СЗПДн, ввода в действие и эксплуатацию объектов информатизации проводится с учетом требований Положения о порядке организации и проведения работ по защите конфиденциальной информации.

Меры по обеспечению безопасности ПДн реализуются в том числе посредством применения в ИСПДн средств защиты информации, прошедших процедуру оценки соответствия согласно Федеральному закону от 27.12.2002 г. N 184-ФЗ «О техническом регулировании», в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн.

Оценка эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн проводится Оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, в соответствии с Федеральным законом от

04.05.2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности». Указанная оценка проводится не реже одного раза в 3 года.

При внедрении организационных мер защиты информации осуществляются:

- реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения (разрешительная система доступа);
- проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и ответственных лиц за обеспечение безопасности информации по реализации организационных мер защиты информации;
- отработка действий должностных лиц и структурных подразделений, ответственных за реализацию мер защиты информации.

Ввод в эксплуатацию СЗПДн осуществляется на основании нормативного правового акта Оператора, который издается на основании положительных результатов оценки соответствия ИСПДн требованиям безопасности ПДн (аттестации или декларации ИСПДн на соответствие требованиям безопасности информации).

Эксплуатация СЗПДн осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией с учетом требований и положений, изложенных в настоящем документе.

При определении порядка проведения технического обслуживания и ремонтных работ серверного оборудования ИСПДн исполнения данных работ осуществляется только администратором безопасности информации ИСПДн либо уполномоченными работниками Оператора в присутствии администратора безопасности информации ИСПДн или по согласованию с администратором безопасности информации ИСПДн.

Все процедуры, связанные с изменением конфигурации СЗПДн, проведением технического обслуживания и ремонтных работ на технических средствах СЗПДн

предусматривают документирование объемов и сроков выполненных работ, а также лиц (организаций), проводивших эти работы.

5. Порядок организации обучения пользователей информационной системы персональных данных правилам и мерам защиты персональных данных, а также работе со средствами защиты персональных данных

Решение основных вопросов обеспечения защиты ПДн предусматривает соответствующую подготовку пользователей ИСПДн. Проведение обучения позволит организовать обработку информации в соответствии с требованиями законодательства и нормативно-методических документов в области обеспечения безопасности ПДн при ее обработке в ИС и реализовать установленный комплекс организационных и технических мер по защите ПДн.

Систему внутреннего обучения пользователей в области защиты ПДн составляет:

- проведение ознакомления пользователей ИСПДн, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;
- самостоятельное изучение пользователями ИСПДн необходимых для работы документов, средств и продуктов;
- повышение квалификации пользователей ИСПДн на курсах повышения квалификации в области защиты ПДн.

В результате прохождения обучения пользователи ИСПДн получат необходимые знания и навыки в отношении:

- правил использования СЗИ ИСПДн;
- содержания основных нормативных правовых актов, руководящих и нормативно-методических документов в области обеспечения

безопасности ПДн при их обработке в ИСПДн;

- основных мероприятий по организации и техническому обеспечению безопасности ПДн при их обработке в ИСПДн;
- планирования, организации и контроля выполнения мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн.

Пользователи ИСПДн, допущенные к работе с ПДн, обязаны пройти инструктаж по вопросам обеспечения безопасности ПДн с целью подтверждения своих знаний и уяснения своих обязанностей по поддержанию установленного режима защиты ПДн.

Инструктаж представляет собой ознакомление пользователей ИСПДн с положениями настоящего Положения и действующих нормативных документов по обеспечению безопасности информации при их обработке в ИСПДн, в том числе с Инструкцией пользователя ИСПДн, а также устный инструктаж администратора безопасности информации ИСПДн по вопросам эксплуатации средств защиты ПДн.

Ознакомление с положениями нормативной документации пользователь ИСПДн подтверждает своей личной подписью в Журнале ознакомления.

Контроль проведения ознакомления и периодическая проверка знания пользователями ИСПДн положений нормативной документации по вопросам обеспечения безопасности ПДн возлагается на ответственного за обеспечение безопасности информации ИСПДн.

Пользователи ИСПДн, не прошедшие инструктаж, к работе в ИСПДн не допускаются.

Проверка знаний пользователями ИСПДн положений нормативной документации по вопросам обеспечения безопасности ПДн проводится ответственным за обеспечение безопасности информации не реже одного раза в год в ходе периодического контроля соблюдения режима безопасности информации.

При самостоятельной подготовке пользователями ИСПДн, а также ответственным за обеспечение безопасности информации самостоятельно изучаются (в части, касающейся):

- руководящие и нормативно-методические документы в области обеспечения безопасности ПДн;

– правила (инструкции) по использованию программных и аппаратных СЗИ;
– внутренние положения (локальные акты) Оператора, устанавливающие порядок обращения с ПДн и их защиты.

Время для самостоятельного изучения определяется непосредственным руководителем пользователя ИСПДн или руководителем Оператора.

6. Планирование работ по защите персональных данных и контролю

Работа по защите ПДн проводится в рамках выполнения годовых планов мероприятий по защите информации, утверждаемых Оператором.

В разделе План работ по защите информации в части обеспечения безопасности ПДн ИСПДн должны быть отражены следующие мероприятия:

– выполнение решений ФСТЭК России;
– уточнение перечня угроз безопасности ПДн ИСПДн;
– уточнение классов ИСПДн;
– аттестация (декларирование) ИСПДн на соответствие требованиям безопасности ПДн;
– разработка, корректировка и согласование организационно-методических документов, планов, отчетов;
– проверка соответствия принимаемых мер защиты информации в ИСПДн требованиям руководящих документов в области безопасности ПДн;
– периодическое обследование аппаратных и программных средств ИСПДн, средств защиты ПДн.

Для каждого мероприятия устанавливается срок исполнения, ответственный за исполнение, ответственный за контроль, отметка о выполнении.

Защита ПДн считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

7. Контроль состояния защиты персональных данных

Контроль состояния защиты ПДн – комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях исключения или существенного затруднения НСД к информации, хищения технических средств и носителей информации; предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации и работоспособности аппаратных средств ИСПДн.

Основными задачами контроля являются:

- проверка выполнения установленных норм и требований по защите ПДн Оператором, учета требований по их защите в разрабатываемых документах;
- уточнение возможных каналов НСД к ИСПДн и программно-технических воздействий на аппаратные и программные элементы ИСПДн;
- оценка достаточности и эффективности принимаемых мер по защите ПДн;
- проверка надлежащего использования средств защиты ПДн;
- проверка выполнения требований по подсистемам СЗПДн;
- оперативное принятие мер по пресечению нарушений требований защиты ПДн в ИСПДн;
- разработка предложений по устранению (ослаблению) угроз безопасности ПДн, обрабатываемых в ИСПДн.

В ходе контроля проверяются:

- соответствие принятых мер установленным нормам и требованиям безопасности информации;
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по защите ПДн;

- полнота выявления возможных каналов НСД к ней и программно-технических воздействий на ИСПДн (ее элементы);
- эффективность применения организационных и технических мероприятий по защите ПДн;
- устранение ранее выявленных недостатков.

Контроль за соблюдением установленных требований безопасности ПДн осуществляется путем обследования ИСПДн.

Обследование ИСПДн проводится комиссией по классификации ИСПДн при участии:

- сотрудников Оператора;
- администратора безопасности;
- ответственного за обеспечение безопасности ПДн.

Обследование эксплуатируемой ИСПДн проводится не реже одного раза в год (при неизменности условий ее эксплуатации).

По результатам обследования ИСПДн издается акт. При выявлении невыполнения требований по защите информации в ИСПДн, работа в ИСПДн приостанавливается. Возобновление работы в ИСПДн разрешается только после устранения выявленных недостатков.

В ходе обследования проверяется:

- соответствие уровня защищенности ИСПДн условиям, сложившимся на момент проверки;
- выполнение условий эксплуатации и требований, изложенных в «Аттестате соответствия»;
- выполнение требований по защите ПДн от НСД;
- выполнение требований по подсистемам СЗПДн.

Периодический контроль состояния защиты ПДн в ходе обработки в ИСПДн осуществляется ответственным за обеспечение безопасности информации ИСПДн.

8. Дополнительные положения

Требования к помещению и размещению аппаратных средств ИСПДн описаны в Порядке обеспечения безопасности помещений, в которых располагаются технические средства ИСПДн.

Правила допуска сотрудников к обработке ПДн в ИСПДн отражены в Порядке оформления допуска (доступа) к обработке ПДн.

Вопросы обработки запросов субъектов ПДн рассматриваются в Порядке обработки запросов субъекта ПДн или его законного представителя, а также уполномоченного органа по защите прав субъектов ПДн.

Оператором утверждаются:

- перечень лиц, допущенных к обработке ПДн с использованием средств автоматизации;
- перечень лиц, допущенных к обработке ПДн без использования средств автоматизации;
- перечень лиц, имеющих доступ к техническому обслуживанию средств вычислительной техники ИСПДн;
- перечень лиц, имеющих доступ в помещения ИСПДн;
- перечень ПДн, разрешенных для обработки в ИСПДн;
- перечень событий безопасности, необходимых для учета;
- перечень должностей, замещение которых предусматривает осуществление обработки ПДн либо осуществления доступа к ПДн ИСПДн;
- перечень ИСПДн.

Сотрудник, получивший доступ к обработке ПДн ИСПДн, до начала обработки ПДн, должен согласиться с условиями Типового обязательства сотрудника (работника), непосредственно осуществляющего обработку ПДн в ИСПДн, в случае расторжения с ним служебного контракта или трудового договора прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных (служебных) обязанностей.