РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

УТВЕРЖДАЮ
Директор
Автономной некоммерческой
организации
дополнительного профессионального
образования «Многопрофильный
центр квалификаций «Цель»

О.В. Самоварова
«11» января 2023 г.

ПОЛОЖЕНИЕ

Об организации обработки и обеспечении безопасности персональных данных в автономной некоммерческой организации дополнительного профессионального образования «Многопрофильный центр квалификаций «Цель»

Санкт-Петербург
2023

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение предназначено для организации процесса обеспечения безопасности персональных данных (далее – ПДн), согласно требованиям действующего федерального законодательства. Положение разработано в соответствии с законодательством Российской Федерации о персональных данных и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн, в том числе при их обработке в информационных системах персональных данных (далее – ИСПДн), а также внутренними документами по информационной безопасности в автономной некоммерческой организации дополнительного профессионального образования «Многопрофильный центр квалификаций «Цель» (далее – Организации).

Для осуществления мероприятий по обеспечению и контролю безопасности персональных данных назначается сотрудник, ответственный за организацию обработки персональных данных.

Действие настоящего Положения распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению, извлечению, использованию, передаче (распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению ПДн, осуществляемые с использованием средств автоматизации и без их использования.

Положение обязательно для ознакомления и исполнения администраторами ИСПДн, Ответственным за организацию обработки персональных данных, Координатором по обращениям и запросам, и остальными работниками, которые участвуют в процессах обработки персональных данных.

Работники должны быть ознакомлены с настоящим Положением под роспись в «Листе ознакомления».

2. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

2.1. Организация обязана при обработке персональных данных принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2.2. Обеспечение безопасности персональных данных достигается, в частности:

– предоставлением доступа к персональным данным, обрабатываемым в информационных системах персональных данных, для работников, которым такой доступ необходим для выполнения их должностных обязанностей;

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, формирование на их основе модели угроз;

– определением требуемого уровня защищённости информационной системы персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– проверкой готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– установкой и вводом в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– учетом лиц, допущенных к работе с персональными данными в информационной системе;

– учетом применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

– проведением разбирательств и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контролем за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.3. Доступ к персональным данным должен предоставляться работникам исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей. Работнику запрещается работать с персональными данными, обработка которых не входит в его должностные обязанности.

2.4. В Организации ведется список работников, допущенных к обработке персональных данных.

3. ОБЯЗАТЕЛЬНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПДН

3.1. Общие требования

3.1.1. В целях обеспечения безопасности персональных данных, обрабатываемых в информационных системах Организации, создается система защиты персональных данных, включающая в себя правовые, организационные и технические меры.

3.1.2. Система защиты персональных данных должна создаваться на основании следующих основных принципов:

– *Принцип правовой защищенности.* Обеспечение безопасности персональных данных должно осуществляться в соответствии с требованиями нормативно-правовых актов Российской Федерации в области защиты персональных данных;

– *Принцип достаточности.* Система защиты персональных данных должна обеспечивать необходимый уровень безопасности персональных данных, без её чрезмерного усложнения;

– *Принцип эффективности.* Применяемые средства защиты информации не должны существенно ухудшать основные функциональные характеристики и производительность информационных систем Организации. Необходимо найти баланс между обеспечением безопасности персональных данных и удобством использования информационных систем;

– *Принцип своевременности.* Принимаемые меры по обеспечению безопасности персональных данных должны носить в первую очередь упреждающий характер и должны быть приняты до начала обработки персональных данных в информационных системах.

3.1.3. В ходе проведения работ по обеспечению безопасности персональных данных предварительно должна быть проведена инвентаризация ИСПДн.

3.1.4. Процедура инвентаризации информационных систем, посредством которых осуществляется обработка персональных данных, производится при помощи интервьюирования (опроса) или анкетирования владельцев данных информационных систем.

3.1.5. Перечень обнаруженных информационных систем, посредством которых осуществляется обработка персональных данных, должен быть документально зафиксирован и согласован.

3.1.6. Периодически необходимо производить актуализацию данного перечня информационных систем, посредством которых осуществляется обработка персональных данных.

3.1.7. Информационные системы, посредством которых осуществляется обработка персональных данных, подлежат обязательной процедуре определения необходимого уровня защищённости, с целью установления организационных и технических, необходимых для обеспечения безопасности персональных данных. Определение уровня защищённости

информационной системы производится на этапе их создания, или в ходе эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем).

3.1.8. Определение требуемого уровня защищённости информационной системы производится в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.10.2012 г. №1119. Определение уровня защищённости ИСПДн производится в следующей последовательности:

– создается Комиссия по проведению определения требуемого уровня защищённости ИСПДн;

– комиссия устанавливает требуемый уровень защищённости ИСПДн, а также определяет наличие в ИСПДн специальных категорий персональных данных, биометрических персональных данных, общедоступных персональных данных, принятия решений, порождающих юридические последствия, на основании исключительно автоматизированной обработки ПДн;

– комиссия формирует акты определения необходимого уровня защищенности для каждой ИСПДн, в которых указывается перечень обрабатываемых ПДн.

3.1.9. В Организации должны быть разработаны Модели угроз для всех ИСПДн.

3.1.10. Модель угроз разрабатывается на основании требований п.7 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных Постановлением Правительства Российской Федерации от 01.10.2012 г. №1119.

3.1.11. Модель угроз разрабатывается в соответствии с требованиями Методического документа «Методика оценки угроз безопасности информации» (утвержден руководством ФСТЭК России 5 февраля 2021 года).

3.1.12. Выбор и реализация мер защиты информации в ИСПДн осуществляются на основе Модели угроз и в зависимости от требуемого уровня защищённости ИСПДн.

3.1.13. Выбранные и реализованные меры защиты ПДн в ИСПДн должны обеспечивать нейтрализацию предполагаемых угроз безопасности ПДн при их обработке в ИСПДн в составе создаваемой системы защиты ПДн.

3.1.14. Модель угроз и требуемый уровень защищённости информационной системы могут быть пересмотрены по решению комиссии на основе проведенного анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы.

3.1.15. Для проведения работ по выбору и реализации мер защиты ПДн (включая техническое проектирование системы защиты ПДн, внедрение средств защиты ПДн, сопровождение средств защиты ПДн и т. д.) могут привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.1.16. Работы, проводимые третьими лицами (организациями) должны проводиться в присутствии работников Организации. При этом доступ к персональным данным, обрабатываемым в информационных системах персональных данных, для третьих лиц должен быть органичен.

3.1.17. Технические требования по защите ПДн в ИСПДн приведены в разделе 4.

3.2. Требования к разрабатываемым и вводимым в эксплуатацию ИСПДн

3.2.1. Разработка ИСПДн должна включать следующие стадии:

– предпроектная стадия (включает предварительный анализ целей и условий функционирования ИСПДн, а также обрабатываемых в ней ПДн, на основании которого определяется предварительный уровень защищённости ИСПДн, степень участия должностных лиц, актуализируются угрозы безопасности);

– стадия проектирования системы защиты ПДн для ИСПДн;

– стадия ввода в действие ИСПДн.

3.2.2. По результатам проведенного анализа и с учетом действующих требований федерального законодательства и регуляторов должны быть разработаны:

– модель угроз безопасности персональных данных при их обработке в ИСПДн;

– требования к защите персональных данных при их обработке в ИСПДн;

– акт определения необходимого уровня защищенности ИСПДн;

– частное техническое задание на создание системы защиты ПДн для ИСПДн.

3.2.3. Проектирование системы защиты ПДн для вводимой в эксплуатацию ИСПДн должно производиться с учетом уже построенной в Организации системы защиты ПДн, включающей комплекс организационных и технических мер.

3.2.4. На стадии ввода в эксплуатацию ИСПДн должны быть проведены, как минимум, следующие мероприятия:

– установка пакета прикладных программ ИСПДн совместно со средствами защиты информации (встроенными и наложенными);

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

– приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

3.2.5. В случае внедрения дополнительных средств защиты должны быть составлены Акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний.

3.2.6. Перед вводом новой ИСПДн в опытную эксплуатацию должен быть составлен Акт о вводе в опытную эксплуатацию ИСПДн, а также Акт определения необходимого уровня защищенности ИСПДн.

3.2.7. В случае успешного функционирования ИСПДн на стадии опытной эксплуатации и принятия решения о переводе ее в промышленную эксплуатацию должен быть составлен Акт о вводе в промышленную эксплуатацию новой ИСПДн.

3.3. Требования к выводу ИСПДн из эксплуатации

3.3.1. В случае принятия решения о выводе ИСПДн из промышленной эксплуатации должен быть подписан Акт о выводе ИСПДн из промышленной эксплуатации.

3.3.2. При выводе ИСПДн из промышленной эксплуатации с целью обеспечения справочной поддержки, доступ к ней должен быть ограничен только определенным составом лиц с правами только на чтение.

3.3.3. После подписания Акта о выводе ИСПДн из промышленной эксплуатации ИСПДн должна быть переведена в архивный фонд (в соответствии с ч. 2 ст. 13 ФЗ «Об архивном деле»), при этом должны быть выполнены следующие требования:

– Доступ к архивной ИСПДн и хранимым в ней документам должен обеспечиваться на основании соответствующей заявки на имя руководителя Организации, по согласованию с отделом информационных технологий и владельцем ИСПДн.

– ПДн, хранящиеся в архиве, могут быть использованы и переданы третьим лицам только в целях исполнения законодательства Российской Федерации.

– Должны быть обеспечены финансовые, материально-технические и иные условия, необходимые для комплектования, хранения, учета и использования ИСПДн, включая специальное помещение, отвечающее нормативным условиям труда сотрудников архива.

– Доступ в помещения, где предполагается хранение выводимой из эксплуатации ИСПДн, должен быть ограничен.

– Должен быть регламентирован перечень лиц, допущенных к работе с ИСПДн, переданной в архив.

– Все внешние запоминающие устройства (ленты с резервными копиями, дискеты, CD-диски, флеш-накопители и т. п.), относящиеся к архивной ИСПДн, должны храниться в сейфах.

– Должно быть разработано описание ИСПДн, переведенной в архивный фонд.

4. ОБЕСПЕЧЕНИЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ПДН

4.1. Общие требования

4.1.1. Обеспечение безопасности ПДн при их обработке в ИСПДн должно осуществляться на всех стадиях жизненного цикла ИСПДн и состоять из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности ПДн в ИСПДн, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и нормального функционирования ИСПДн в случае реализации угроз.

4.1.2. В целях защиты ПДн от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому обеспечению безопасности ПДн для каждой ИСПДн должны включать:

– определение требуемого уровня защищённости информационной системы производится в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.10.2012 г. № 1119;

– выявление и закрытие технических каналов утечки ПДн на основе анализа и актуализации модели угроз безопасности ПДн;

– выбор и реализацию мер защиты информации в информационной системе на основе модели угроз безопасности ПДн и в зависимости от уровня защищённости информационной системы;

– установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных средств защиты информации;

– разработку дополнений к трудовым договорам (или должностных инструкций) по обеспечению безопасности ПДн при их обработке в ИСПДн для персонала, задействованного в эксплуатации данной ИСПДн.

4.1.3. Используемые средства вычислительной техники, удовлетворяют требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

4.1.4. Защита ПДн при их обработке в ИСПДн от несанкционированного доступа и иных неправомерных действий должна осуществляться в следующими мерами:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности персональных данных;

– обеспечение целостности информационной системы и персональных данных;

– обеспечение доступности персональных данных;

– защита среды виртуализации;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

– управление конфигурацией информационной системы и системы защиты персональных данных.

4.1.5. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных могут применяться следующие меры:

– проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

– тестирование информационной системы на проникновения;

– использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

4.1.6. В Организации также могут разрабатываться и применяться другие меры защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности ПДн.

4.1.7. Конкретные методы и средства защиты ПДн в ИСПДн должны определяться на основании нормативно-методических документов ФСТЭК России и ФСБ России исходя из требуемого уровня защищённости и актуальных угроз безопасности ПДн.

4.1.8. Выполнение функций обеспечения безопасности персональных данных в ИСПДн обеспечивается средствами защиты информации, прошедшими в установленном порядке процедуру

оценки соответствия, а также комплексом встроенных механизмов защиты электронных вычислительных машин, операционных систем, систем управления базами данных, прикладного программного обеспечения.

4.1.9. Все технические средства защиты информации должны быть снабжены инструкциями по эксплуатации (рекомендациями по использованию).

4.1.10. Должен вестись учет технических средств защиты информации.

4.1.11. Ответственность за ведение учета технических средств защиты информации возлагается на ответственного за организацию обработки ПДн.

4.2. Тестирование функций системы защиты ПДн

4.2.1. В соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» должно проводиться периодическое тестирование функций системы защиты ПДн.

4.2.2. Тестирование функций системы защиты производится на основании Регламента (Плана) о порядке контроля защищенности персональных данных.

4.2.3. Ответственность за тестирование функций системы защиты ПДн возлагается на ответственного за организацию обработки ПДн.

4.3. Учет отчуждаемых электронных носителей ПДн

4.3.1. В Организации должен проводиться учет отчуждаемых защищаемых носителей ПДн. К защищаемым носителям ПДн относятся следующие:

- съемные носители информации серверов;
- съемные носители информации АРМ;
- ленты с резервными копиями;
- внешние запоминающие устройства (дискеты, флеш-накопители и т. п.), содержащие ПДн.

4.3.2. Ответственность за учет отчуждаемых защищаемых электронных носителей ПДн возлагается на ответственного за организацию обработки ПДн.

5. ОБЯЗАННОСТИ АДМИНИСТРАТОРОВ ИСПДН, ОТВЕТСВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПДН

5.1. Ответственность за обеспечение безопасности персональных данных при их автоматизированной обработке, соблюдение установленных в Организации требований к защите персональных данных при их автоматизированной обработке, в том числе требований настоящего Положения, в структурных подразделениях Организации возлагается на их руководителей.

5.2. Каждый работник, имеющий доступ к информационным системам персональных данных, необходимый ему для выполнения своих должностных обязанностей, несет персональную ответственность за свои действия.

5.3. Должностные инструкции администраторов ИСПДн и ответственного за организацию обработки ПДн должны быть расширены с учетом специфики обработки и защиты ПДн. Работники, назначенные на данные роли, должны быть ознакомлены под подпись со своими должностными инструкциями.

5.4. В обязанности администраторов ИСПДн входит:

– управление учетными записями пользователей комплекса ИСПДн;

– поддержание штатной работы комплекса ИСПДн;

– предоставление и прекращение доступа пользователей к ПДн в ИСПДн в соответствии с утвержденным Перечнем должностей сотрудников, допущенных к работе с ПДн или с утвержденными заявками на доступ к ПДн;

– установка и конфигурирование аппаратного и программного обеспечения комплекса ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн;

– уточнение ПДн в случаях, определенных настоящим Положением и Положением о порядке обработки обращений субъектов персональных данных;

– блокирование ПДн в случаях, определенных настоящим Положением и Положением о порядке обработки обращений субъектов персональных данных;

– уничтожение ПДн в случаях, определенных настоящим Положением и Положением о порядке обработки обращений субъектов персональных данных;

5.5. В обязанности ответственного за организацию обработки ПДн входит:

– осуществление внутреннего контроля за соблюдением Организации и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доведение до сведения работников Организации положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– осуществлять контроль за приемом и обработкой обращений и запросов субъектов ПДн или их представителей;

– тестирование системы защиты ПДн;

– предоставление сведений о ПДн в рамках проведения учета защищаемых носителей и проведения инвентаризации;

– установка, конфигурирование и администрирование аппаратных и программных СЗИ комплекса ИСПДн;

– учет и хранение отчуждаемых носителей ПДн;

– учет технических средств защиты информации;

– периодические проверки журналов безопасности;

– анализ защищенности ИСПДн;

– организация процесса обучения работников по направлению обеспечения безопасности ПДн;

– мониторинг порядка обработки ПДн;

– участие в проведении внутреннего контроля и служебных расследований фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

5.6. Ответственный за организацию обработки ПДн обладает следующими полномочиями:

– проводить плановые и внеплановые контрольные мероприятия в целях контроля, изучения и оценки фактического состояния защищенности ПДн;

– запрашивать необходимую информацию у очевидцев и подозреваемых лиц при проведении разбирательств по фактам нарушения установленного порядка обработки и обеспечения безопасности ПДн;

– запрашивать необходимую информацию у администраторов ИСПДн;

– давать администраторам ИСПДн распоряжения касательно блокирования, уточнения, уничтожения ПДн;

– оценивать правомерность полученных запросов уполномоченного органа по защите прав субъектов ПДн;

– созывать комиссию для решения вопросов по возражениям субъектов ПДн против принятия решений на основании исключительно автоматизированной обработки персональных данных.

5.7. В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения критичных для безопасности ПДн полномочий у одного лица запрещается совмещать роли администратора ИСПДн и роль ответственного за организацию обработки ПДн в лице одного сотрудника.

6. ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ И НАДЗОР ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Государственный контроль и надзор за соблюдением требований законодательства Российской Федерации в области персональных данных осуществляет федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности (ФСБ России), а также федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России).

6.2. Государственный контроль и надзор за соблюдением требований законодательства Российской Федерации в области персональных данных осуществляется в соответствии с требованиями Федерального закона от 26.12.2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

6.3. Организацию работ по прохождению государственного контроля и надзора осуществляет Ответственный за организацию обработки ПДн.

7. ОРГАНИЗАЦИЯ ВНУТРЕННЕГО КОНТРОЛЯ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Цели организации внутреннего контроля

7.1.1. Организация внутреннего контроля процесса обработки ПДн в Организации осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

7.1.2. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

– обеспечение соблюдения сотрудниками требований настоящего Положения и нормативных правовых актов, регулирующих защиту ПДн;

– оценка компетентности персонала, задействованного в обработке ПДн;

– обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн;

– выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений;

– принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн;

– разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий;

– осуществление контроля за исполнением рекомендаций и указаний по устранению нарушений.

7.2. Проведение контрольных мероприятий

7.2.1. Ответственный за организацию обработки ПДн на периодической основе организует проведение внутреннего контроля соблюдения порядка обработки и обеспечения безопасности ПДн.

7.2.2. Проведение контрольных мероприятий по обеспечению безопасности ПДн должно включать:

– проведение проверок деятельности работников, допущенных к работе с ПДн в ИСПДн, на соответствие порядку обработки и обеспечения безопасности ПДн, установленному настоящим Положением, ФЗ «О персональных данных» и другими нормативными правовыми актами;

– проведение проверок состояния защищенности ПДн, обрабатываемых в ИСПДн, включая проверку доступов пользователей к ПДн, выполнение требований по защите каждой конкретной ИСПДн, корректности работы системы защиты ПДн и т. д.

7.2.3. Все результаты проверок должны быть предоставлены в виде Актов для проведения анализов результатов и подготовки соответствующего Отчета о проведении внутреннего контроля обработки и обеспечения безопасности персональных данных.

7.2.4. При необходимости должны быть предложены меры по минимизации последствий выявленных угроз ИБ

ЛИСТ ОЗНАКОМЛЕНИЯ

с Положением об организации обработки и обеспечении безопасности персональных данных

№ п/п	Ф.И.О.	Подпись	Дата