ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
МИКРОКРЕДИТНАЯ КОМПАНИЯ
«АГАР»

ПРИКАЗ № 24

г. Чернушка 01 марта 2021 года

« Об утверждении «Положения об организации и проведении работ по обеспечению безопасности персональных данных»

Во исполнение требований Федерального закона № 152-ФЗ «О персональных данных» от 27 июля 2006 года, Федерального закона № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» от 30 декабря 2020 года, а также прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ

1. Утвердить «Положение об организации и проведении работ по обеспечению безопасности персональных данных в ООО МКК «АГАР» (Приложение 1).
2. Контроль исполнения настоящего приказа оставляю за собой.

Генеральный директор С.Е. Ладочкин

УТВЕРЖДАЮ

_____ С.Е. Ладонкин

Приложение № 1к приказу
ООО МКК «АГАР»
от «01» марта 2021 г. № 24

ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО МКК «АГАР»

1. Общие положения

Данное «Положение об организации и проведению работ по обеспечению безопасности персональных данных в ООО МКК «АГАР» (далее - Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» от 30 декабря 2020 года, требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн).

Настоящее Положение определяет цели, задачи и основные мероприятия по обеспечению безопасности персональных данных в ООО МКК «АГАР» (далее по тексту - Организация, Оператор) от несанкционированного доступа и неправомерного их использования или утраты.

Положение является основой для разработки локальных нормативных актов Организации по обеспечению безопасности ПДн.

Положение распространяется на всех клиентов и работников Организации, включая сотрудников, работающих по договору подряда, а также на сотрудников сторонних организаций, взаимодействующих с Организацией на основании соответствующих нормативных, правовых и организационно-распорядительных документов.

2. Цели обработки ПДн

Целью обработки персональных данных является:
- выполнение обязательств в отношении работников, согласно Трудового Кодекса РФ;
- рассмотрения заявки на предоставление кредита.

3. Принципы обработки ПДн

В целях реализации прав субъекта ПДн Оператор (ООО МКК «АГАР») и его представители обязаны соблюдать следующие принципы:
- обработка персональных данных должна осуществляться на законной и справедливой основе;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;

- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Все меры конфиденциальности при сборе, обработке и хранении ПДн работника, клиента распространяются как на бумажные, так и на электронные носители информации.

4. Способы обработки ПДн

Субъектами ПДн, обрабатываемые в Организации, являются клиенты и работники Организации. Все ПДн, обрабатываемые в информационных системах Организации представлены в документе «Перечень персональных данных, обрабатываемых в ООО МКК «АГАР».

К допустимым действиям с ПДн относятся:
- сбор;
- запись;
- систематизация;
- накопление;
- хранение;
- уточнение;
- предоставление;
- доступ;
- обезличивание;
- блокирование;
- удаление;
-уничтожение.

5. Порядок получения ПДн работников Организации

Все персональные данные работника Организации следует получать у него лично.

В случае, если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомление необходимо указать цели получения персональных данных работника у иного лица, предполагаемые источники информации,

способы получения данных. Работодатель должен сообщить работнику о последствиях отказа работника дать письменное согласие на их получение.
Работники так же передают работодателю сведения специальной категории (результаты прохождения медосмотра). Сведения данной категории должны обосабливаться от сведений иных категорий, путем фиксации на отдельных материальных носителях.
Согласие на обработку специальной категории ПДн не требуется, т.к. обработка ПДн данной категории осуществляется в соответствие с трудовым законодательством.
Обработка специальной категории ПДн должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.
С целью информирования клиентов о компетенциях сотрудников Организации, работнику должно быть предложено подписать «Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения» следующих его персональных данных:
- ФИО;
- должность;
- стаж;
- сведения об образовании.

Сведения о субъекте ПДн должны быть в любое время исключены из доступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных органов.

«Согласие на обработку ПДн работника» должно содержать следующие данные:
- фамилию, имя, отчество;
- пол, возраст;
- дата и место рождения;
- адрес регистрации по месту жительства и адрес фактического проживания;
- паспортные данные;
- номер телефона (домашний, мобильный);
- СНИЛС, ИНН;
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для представления льгот работнику, предусмотренных трудовым и налоговым законодательством;
- отношение к воинской обязанности;
- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности работника;
- наименование или ФИО и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки;
- перечень данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки;
- срок, в течение которого действует согласие, а также порядок его отзыва.

«Согласие на распространение ПДн работника» должно содержать следующие данные:
- фамилия, имя, отчество;
- дата рождения;
- место рождения;

- почтовый адрес;
- состояние здоровья (специальная категория персональных данных);
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации.
- наименование или Ф.И.О. и адрес оператора, получившего согласие;
- цель обработки персональных данных;
- категории и перечень персональных данных, на обработку которых дается согласие или обработка которых запрещена;
- условия разрешения и запрета обработки персональных данных;
- срок, в течение которого действует согласие;
- сведения об информационных ресурсах оператора, посредством которых они будут представлены неограниченному кругу лиц (например: адрес сайта).

6. Порядок получения ПДн клиентов Организации

Все персональные данные клиента Организации могут быть получены как у клиента лично, так и у его представителя.

В случае получения ПДн у представителя субъекта ПДн, необходимо убедиться в законности представления интересов субъекта ПДн данным лицом.

Если персональные данные получены не от субъекта персональных данных, то до начала обработки таких персональных данных необходимо предоставить субъекту персональных данных следующую информацию:
- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- права субъекта персональных данных;
- источник получения персональных данных.

Представитель Организации должен проверить достоверность полученных от субъекта сведений, сверяя данные, предоставленные субъектом ПДн, с имеющимися у субъекта документами.

Субъект ПДн должен быть информирован о целях, объеме обрабатываемых ПДн, возможных фактах передачи его ПДн третьим лицам (при этом требуется взять письменное «Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения»). Факт согласия субъекта ПДн обработку его ПДн должен быть закреплен письменно (получение согласия на обработку).

«Согласие на обработку ПДн клиента» должно содержать следующие данные:
- фамилию, имя, отчество;
- пол, возраст;
- дата и место рождения;
- адрес регистрации по месту жительства и адрес фактического проживания;
- паспортные данные;
- номер телефона (домашний, мобильный);
- СНИЛС, ИНН;
- наименование или ФИО и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки;
- перечень данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки;
- срок, в течение которого действует согласие, а также порядок его отзыва.

«Согласие на распространение ПДн клиента» должно содержать следующие данные:

- Ф.И.О. субъекта персональных данных;
- дата рождения;
- место рождения;
- почтовый адрес;
- наименование или Ф.И.О. и адрес оператора, получившего согласие;
- цель обработки персональных данных;
- категории и перечень персональных данных, на обработку которых дается согласие или обработка которых запрещена;
- условия разрешения и запрета обработки персональных данных;
- срок, в течение которого действует согласие;
- сведения об информационных ресурсах оператора, посредством которых они будут представлены неограниченному кругу лиц (например: адрес сайта).

Работник, клиент вправе обратиться за уточнением процесса обработки своих персональных данных. Процедура обработки обращений субъектов ПДн описана в Инструкций по обработке запросов субъектов персональных данных.

Порядок работы персонала в части обеспечения безопасности ПДн при их обработке в ИСПДн.

Настоящий порядок определяет действия персонала Организации в части обеспечения безопасности ПДн при их обработке в ИСПДн.

Все работники, работающие в ИСПДн Организации должны быть под роспись ознакомлены с внутренними документами Организации в области защиты ПДн.

Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:
- соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- выполнять требования Инструкций по организации антивирусной и парольной защиты в полном объеме;
- для хранения информации, содержащей ПДн, использовать только машинные носители информации, учтенные в Журнале учета носителей ПДн;
- немедленно известить ответственного за организацию обработки ПДн и (или) системного администратора при подозрении компрометации личных паролей, а также при обнаружении:
- о нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках средств вычислительной техники (далее - СВТ) или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным защищаемым СВТ; о несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн; о отклонениях в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения; о некорректного функционирования установленных на компьютеры технических средств защиты; о непредусмотренных отводов кабелей и подключенных устройств.

Пользователю ИСПДн категорически запрещается:
- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно- программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные

средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных носителях информации;
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие ПДн;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;
- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации;
- передавать сведения, содержащие персональные данные, по незащищённым каналам связи.

7. Правила работы с персональными данными работников при их неавтоматизированной обработке

Неавтоматизированной обработкой называется обработка без использования средств автоматизации. Неавтоматизированная обработка ПДн работников используются при ведении следующих видов документов:
- личные дела работников;
- финансовые документы работников;
- трудовые книжки работников.

Целью ведения данной документации является выполнение обязательств согласно Трудового Кодекса Российской Федерации.

Перечень сотрудников, имеющих доступ к ПДн, обрабатываемых без средств автоматизации, а так же объем обрабатываемых ПДн, утверждается приказом Директора Организации. Все сотрудники, осуществляющие обработку персональных данных без использования средств автоматизации, информируются под роспись о следующем:
- о факте обработки ими персональных данных, без использования средств автоматизации;
- о категориях обрабатываемых персональных данных;
- о правилах осуществления такой обработки.

Доступ посторонних лиц к носителям персональных данных не допускается.

В рабочее время документы, содержащие ПДн, не должны находиться на столах сотрудников дольше времени, нежели необходимо на их обработку. Во время обработки документы, содержащие ПДн, должны размещаться таким образом, чтобы исключить возможность подсматривания.

Все носители ПДн, подлежащие неавтоматизированной обработке, должны храниться в фиксированных местах:
- личные дела работников, финансовые документы подлежат хранению в шкафах оснащенных запирающими устройствами;
- трудовые книжки подлежат хранению в сейфе.

8. Правила работы с персональными данными клиентов при их неавтоматизированной обработке

Неавтоматизированной обработкой называется обработка без использования средств автоматизации. Неавтоматизированная обработка ПДн клиентов используются при ведении следующих видов документов:

- акты выполненных работ.

Все сотрудники, осуществляющие обработку персональных данных без использования средств автоматизации, информируются под роспись о следующем:
- о факте обработки ими персональных данных, без использования средств автоматизации;
- о категориях обрабатываемых персональных данных;
- о правилах осуществления такой обработки.

Доступ посторонних лиц к носителям персональных данных не допускается.

В рабочее время документы, содержащие ПДн клиентов, не должны находиться на столах сотрудников Организации дольше времени, нежели необходимо на их обработку. Во время обработки документы, содержащие ПДн клиентов, должны размещаться таким образом, чтобы исключить возможность подсматривания.

9. Правила работы с типовыми формами

Типовые формы или связанные с ними документы должны содержать:
- сведения о цели обработки персональных данных;
- наименование и адрес оператора;
- фамилию, имя, отчество и адрес субъекта персональных данных;
- источник получения персональных данных;
- сроки обработки персональных данных;
- перечень действий с персональными данными, которые будут совершаться в процессе их обработки.

Для ведения личных карт работников данная информация содержится в папках хранения личных дел.

В случае необходимости типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации.

Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

10. Передача ПДн работников третьим лицам

Передача ПДн работников возможна только с письменного Согласия на распространение ПДн субъекта.

При передаче персональных данных между Организацией и получающей стороной заключается соглашение о защите персональных данных, включающее в себя объем передаваемых ПДн, цель обработки ПДн, объем допустимых действий с ПДн, а также требования к защите обрабатываемых персональных данных, в соответствие с законодательством в области защиты ПДн.

При передаче персональных данных работника работодатель должен соблюдать следующие требования:
- не сообщать персональные данные работника третьей стороне без письменного Согласия на распространение ПДн работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

Лица, получившие доступ до ПДн работника, обязаны:
- не раскрывать третьим лицам и не распространять ПДн без письменного Согласия на распространение ПДн субъекта, если иное не предусмотрено законом;
- 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;
- осуществлять обработку ПДн исключительно в целях, заявленных в соглашении о защите персональных данных;
- соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и иными нормативными документами в области защиты ПДн;
- разрешать доступ к ПДн только тем сотрудникам, которым такие данные необходимы в рамках их трудовой деятельности.

Передача персональных данных работников третьим лицам без письменного Согласия на распространение ПДн работников возможна в следующих случаях (передача персональных данных государственным структурам):
- передача ПДн работников в пенсионный фонд в соответствие со статей 22 Трудового кодекса Российской Федерации;
- передача ПДн работников в Федеральный Фонд Обязательного Медицинского Страхования в соответствие со статей 22 Трудового кодекса Российской федерации;
- передача ПДн работников в Федеральную налоговую службу в соответствие с п.3.4 Ст.4 Налогового кодекса Российской Федерации;
- передача ПДн работников в кредитно-финансовую организацию для целей зачисления заработной платы на основании заявления сотрудника в соответствие со статей 136 Трудового кодекса Российской Федерации. Финансовые документы, необходимые для начисления заработной платы сотрудникам, должны передаваться только на бумажных носителях и только лично сотрудникам кредитного учреждения, ответственным за выполнение данных обязательств;
- передача ПДн работников в полицию, следственные органы, военкомат.

11. Передача ПДн клиентов третьим лицам

Оператор вправе поручить обработку персональных данных другому лицу с письменного согласия субъекта на распространение персональных данных, если иное не предусмотрено федеральным законом.

При передаче персональных данных между Организацией и получающей стороной заключается соглашение о защите персональных данных, включающее в себя объем передаваемых ПДн, цель обработки ПДн, объем допустимых действий с ПДн, а также требования к защите обрабатываемых персональных данных, в соответствие с законодательством в области защиты ПДн.

Лица, получившие доступ к ПДн клиента, обязаны:
- не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законом;
- 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;
- осуществлять обработку ПДн исключительно в целях, заявленных в соглашении;

- соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и иными нормативными документами в области защиты ПДн;
- разрешать доступ к ПДн клиента только тем сотрудникам, которым такие данные необходимы в рамках их трудовой деятельности.

При передаче персональных данных клиентов Организация должна предупредить лиц, получающих персональные данные клиента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

Передача персональных данных клиентов страховым компаниям осуществляется только на бумажных носителях. Бумажные носители, содержащие ПДн клиентов, должны передаваться лично в руки сотрудникам страховой компании, ответственным за взаимодействие с Организацией.

12. Правила работы с персональными данными уволенных работников

По прекращению трудовых отношений между Организацией и работником, Работодатель вправе обрабатывать персональные данные уволенного работника в случаях и в сроки, предусмотренные федеральным законодательством. К таким случаям относится:
- обязанность работодателя в течение 5 лет обеспечивать сохранность документов, необходимых для исчисления, удержания и перечисления налога в соответствие с подпунктами 5 и 3 ст. 24 Налогового кодекса Российской Федерации;
- обязанность работодателя хранить бухгалтерскую документацию в течение сроков, устанавливаемых в соответствии с правилами организации государственного архивного дела, но при этом минимальный срок хранения не может быть менее пяти лет в соответствие со ст. 17 Федерального закона от 21 ноября 1996 г. № 129-ФЗ «О бухгалтерском учете».

По истечении сроков, определенных законодательством Российской Федерации, личные дела работников и иные документы передаются на архивное хранение на срок 75 лет. Личные дела уволенных работников позже 01 января 2003 года - хранятся в течение 50 лет.

Персональные данные уволенных работников должны храниться обособленно от ПДн остальных работников.

На работу с персональными данными уволенных работников распространяются все правила работы с персональными данными работников.

Порядок обучения персонала практике работы в части обеспечения безопасности персональных данных:
- перед началом работы с ПДн пользователи должны ознакомиться с настоящим Положением и прослушать инструктаж по работе с программными и техническими средствами защиты информации под роспись;
- пользователи должны продемонстрировать ответственному за организацию обработки персональных данных наличие необходимых знаний и умений для выполнения требований настоящего Положения;
- пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего Положения, к работе с ПДн не допускаются.

13. Порядок контроля защиты ПДн

С целью контроля выполнения необходимых мероприятий по обеспечению безопасности ПДн руководителем Организации назначается ответственный за организацию обработки персональных данных.
Ответственный за организацию обработки персональных данных имеет право:

- требовать от работников соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
- осуществлять внутренний контроль и аудит соответствия обработки персональных данных законодательству в области защиты ПДн, и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам Оператора.

Контроль защиты ПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

Основными задачами контроля являются:
- проверка организации выполнения мероприятий по защите информации в подразделениях Организации, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- выявление демаскирующих признаков объектов ИСПДн;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно - технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;
- проверка выполнения требований законодательство и локальных нормативных актов Организации по защите ПДн при их неавтоматизированной обработке;
- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации;
- актуализация оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства в области зашиты ПДн.

В ходе контроля состояния защищенности ПДн проверяются:
- достаточность принятых мер по обеспечению безопасности персональных данных (далее - ОБ ПДн);
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;

- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- эффективность применения организационных и технических мероприятий по защите информации;
- устранение ранее выявленных недостатков.

Полученные в ходе контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации рассматривается вопрос о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения.

Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов Организации проводятся, как правило, ответственным за организацию обработки персональных данных, в соответствии с утвержденным планом или по согласованию с Директором.

14. Правила технического обслуживания ИСПДн

Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ИСПДн предоставляется системному администратору.

Самостоятельное изменение конфигурации аппаратно-программных средств ИСПДн сотрудниками запрещено.

Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

После установки (обновления) ПО, системный администратор должен произвести требуемые настройки средств управления доступом к компонентам компьютера, проверить работоспособность ПО, правильность их настройки, произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн».

При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за организацию обработки персональных данных. В данном случае системный администратор обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Отметка о данном мероприятии вносится в «Журнал учета нештатных ситуаций ИСПДн».

С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») запрещено.

Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется непосредственным руководителем данного сотрудника.

Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное (-ые) значение (-ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему.

15. Порядок охраны и допуска посторонних лиц в защищаемые помещения

Настоящее Положение устанавливает порядок охраны (сдачи под охрану) защищаемых помещений ИСПДн.

Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

При закрытии помещений сотрудники проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убираются для хранения в запираемые шкафы или сейф.

В соответствие с требованиями данного Положения при обработке ПДн необходимо исключить не контролируемое пребывание посторонних лиц в пределах помещениях, где ведется обработка.

При обнаружении повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и (или) ответственному за организацию обработки персональных данных.

Одновременно принимаются меры по охране места происшествия, и до прибытия должностных лиц в помещение никто не допускается.

Директор Организации, сотрудник, ответственный за организацию обработки персональных данных и ответственный за ИСПДн организуют проверку помещений на предмет несанкционированного доступа к конфиденциальной информации, наличие документов и машинных носителей информации.

16. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации

Сроки хранения сведений, содержащих ПДн клиентов, работников:

- договора на оказание услуг хранятся в течение трех лет;
- ПДн работников хранятся в течение 75 лет с момента расторжения трудового договора, уволенных позже 01 января 2003 года – 50 лет.

При автоматизированной обработке по истечению срока хранения ПДн должны быть удалены из ИСПДн. При неавтоматизированной обработке по истечению срока хранения носители ПДн должны быть уничтожены.

В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн.

Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

Бумажные и прочие сгораемые носители уничтожают путем сжигания или с помощью любых бумагорезательных машин.

Уничтожение материальных носителей производится комиссией. Состав комиссии определяется приказом Директора Организации. Комиссии предлагается произвести экспертную оценку и выделить материальные носители, подлежащие уничтожению. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

17. Заключительные положения

Требования настоящего Положения обязательны для всех работников Организации обрабатывающих конфиденциальную информацию (персональные данные).

Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Используемы сокращения и определения

Таблица 1 - Сокращения

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	Базы данных
ИСПДн	Информационная система персональных данных
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
СЗИ	Система защиты информации
СКЗИ	Средства криптографической защиты информации
ФСТЭК	Федеральная служба по техническому и экспортному контролю

Таблица 2 - Определения

Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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

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; Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники
Субъект персональных данных	Физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных
Распространение ПДн	Действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Предоставление ПДн	Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
Блокирование ПДн	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Уничтожение ПДн	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных
Обезличивание ПДн	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Трансграничная передача персональных данных	передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу