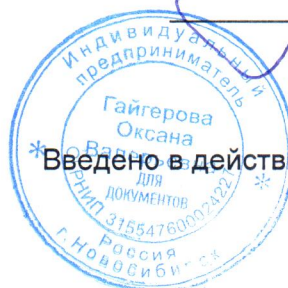


УТВЕРЖДЕНО

Индивидуальный предприниматель

Гайгерова Оксана Валерьевна



Введено в действие с 01.02.2021

ПОЛОЖЕНИЕ

«О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ»

Оглавление

АННОТАЦИЯ	3
1. Перечень сокращений, используемых в документе	3
2. Общие положения	4
3. Мероприятия по обеспечению безопасности персональных данных	5
4. Порядок защиты персональных данных.....	7
4.1. Общие требования	7
4.2. Мероприятия по защите ПДн в ИСПДн.....	8
5. Контроль за выполнением требований настоящего Положения	9
6. Ответственность за нарушения настоящего Положения	10

АННОТАЦИЯ

Настоящее Положение разработано в соответствии с требованиями Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», Постановления Правительства РФ от 17.11.2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативно-методических документов ФСТЭК России и иных документов в области персональных данных.

Обеспечение безопасности персональных данных осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы (подсистемы) защиты персональных данных.

1. Перечень сокращений, используемых в документе

- ПДн	- Персональные данные
- ИСПДн	- Информационная система персональных данных
- УК РФ	- Уголовный Кодекс Российской Федерации
- Компания	- ИП Гайгерова О.В.
- РФ	- Российская Федерация
- ФЗ	- Федеральный закон

2. Общие положения

Положение «О защите персональных данных» устанавливает общие требования по обеспечению безопасности персональных данных при их обработке.

Целью Положения является защита персональных данных, обрабатываемых в Компании, от несанкционированного доступа, неправомерного их использования, утраты, других угроз персональным данным.

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Действие настоящего документа распространяется в отношении Компании и ее обособленных подразделений (филиалов, представительств и т.д.) и охватывает все категории субъектов персональных данных, обрабатываемых Компанией.

Положение разработано на основании статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, Федерального закона «О персональных данных», а также Федерального закона «Об информации, информатизации и защите информации».

Цели и способы обработки персональных данных определяются в документе «Политика конфиденциальности».

Настоящий документ является внутренним нормативным актом Компании и вступает в силу с момента его утверждения ИП Гайгеровой О.В.

3. Мероприятия по обеспечению безопасности персональных данных

3.1. Общие положения

Работы по обеспечению безопасности (защите) персональных данных осуществляются в соответствии с требованиями нормативно-методических документов, регламентирующих порядок защиты ПДн.

Защита персональных данных представляет собой жестко регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

Организация работ по обеспечению безопасности персональных данных осуществляется руководством Компании.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах Компании, приказом ИП Гайгерова О.В. может назначаться структурное подразделение или должностное лицо, ответственные за обеспечение безопасности персональных данных.

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных может осуществляться также сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.

Ответственные лица по работе с персональными данными назначаются в соответствии с Приказами, Индивидуальным предпринимателем Гайгеровой О.В. в отношении соответствующих обособленных подразделений.

Лица, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании утвержденного списка.

3.2. Внутренний нарушитель.

Основным источником угроз несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

Для обеспечения защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

- строгое избирательное и обоснованное распределение документов и информации между работниками;

- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения.

3.3. Внешний нарушитель.

Под внешним нарушителем понимается любое лицо, не имеющее непосредственного отношения к деятельности Компании, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов.

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и т.д..

Для обеспечения защиты персональных данных от внешнего нарушителя необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

3.4. Дополнительные меры защиты

Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

По возможности персональные данные обезличиваются.

4. Порядок защиты персональных данных

4.1. Общие требования

При обеспечении безопасности персональных данных осуществляются следующие мероприятия по:

- выявлению и закрытию технических каналов утечки ПДн в ИСПДн;
- защите ПДн от несанкционированного доступа и неправомерных действий;
- установке, настройке и применению средств защиты.

Мероприятия по защите ПДн при их обработке в ИСПДн от несанкционированного доступа и неправомерных действий включают:

- управление доступом;

регистрацию и учет;
обеспечение целостности;
антивирусную защиту;
обеспечение безопасного межсетевого взаимодействия ИСПДн;
анализ защищенности;
обнаружение вторжений.

4.2. Мероприятия по защите ПДн в ИСПДн

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- описание системы защиты персональных данных;
- проведение оценки соответствия ИСПДн требованиям по безопасности.
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.3. Порядок защиты ПДн при их неавтоматизированной обработке

Мероприятия по обеспечению безопасности персональных данных при их неавтоматизированной обработке включают в себя:

- определение мест хранения персональных данных (материальных носителей);
- определение перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- обеспечение сохранности материальных носителей персональных данных и исключение несанкционированный к ним доступ при их хранении;
- информирование лиц, осуществляющих обработку персональных данных без использования средств автоматизации о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

5. Контроль за выполнением требований настоящего Положения

За выполнением требований настоящего Положения осуществляется контроль.

5.1. Структурные подразделения и сотрудники Компании, ответственные за обеспечение безопасности персональных данных, а также ответственные лица по работе с персональными данными назначаются в соответствии с Приказом «О назначении ответственных за обеспечение безопасности персональных данных и

ответственных лиц по работе с персональными данными», подписанным директором Компании в отношении соответствующих обособленных подразделений.

6. Ответственность за нарушения настоящего Положения

Лица, виновные в нарушении требований настоящего Положения, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

6.1. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке