

УТВЕРЖДАЮ  
Генеральный директор  
ООО «СоюзДонСтрой»  
С.М. Борцов



**ПОЛОЖЕНИЕ**  
**информационной безопасности об организации и обеспечении**  
**безопасности персональных данных**  
**в обществе с ограниченной ответственностью**  
**«СоюзДонСтрой»**

## СОДЕРЖАНИЕ

Содержание .....	2
Определения .....	3
Обозначения и сокращения.....	6
Введение .....	7
1 Общие положения .....	8
2 Задачи СЗПДн .....	11
3 Объекты защиты .....	12
Перечень информационных систем .....	12
Перечень объектов защиты .....	12
4 Классификация пользователей ИСПДн.....	13
5 Меры, методы и средства обеспечения требуемого уровня защищенности... 14	
Законодательные (правовые) меры защиты .....	14
Организационные (административные) меры защиты .....	14
Физические меры защиты .....	15
Аппаратно-программные средства защиты ПДн .....	15
6 Контроль эффективности СЗПДн.....	17
7 Сферы ответственности за безопасность ПДн .....	18
8 Модель нарушителя безопасности.....	19
9 Модель угроз безопасности.....	20
10 Порядок работы с персональными данными сотрудников.....	21
11 Порядок работы с персональными данными контрагентов... ..	23
12 Особенности обработки персональных данных без использования средств автоматизации.....	25
13 Список использованных источников.....	27

## ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**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.

**Биометрические персональные данные** – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

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

**Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**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.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**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.

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор (персональных данных)** – 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.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи,

звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

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

## ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

ИБ – информационная безопасность

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУИ – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

## ВВЕДЕНИЕ

Настоящее Положение информационной безопасности в обществе с ограниченной ответственностью «СоюзДонСтрой» (далее по тексту – ООО «СоюзДонСтрой»), определяет политику в отношении обработки персональных данных в ООО «СоюзДонСтрой» и является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности ООО «СоюзДонСтрой».

Настоящее Положение определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) ООО «СоюзДонСтрой». Положение определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Положение разработано в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Положение служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ООО «СоюзДонСтрой», а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Положение является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ООО «СоюзДонСтрой»;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса, согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;
- координации деятельности структурных подразделений ООО «СоюзДонСтрой» при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн ООО «СоюзДонСтрой».

Правовой базой для разработки настоящего положения служат требования действующих в Российской Федерации законодательных и нормативных документов по обеспечению безопасности персональных данных (ПДн).

## 1 Общие положения

Обработка ПДн в ООО «СоюзДонСтрой» ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

Цели обработки ПДн происходят в том числе из анализа правовых актов, регламентирующих деятельность ООО «СоюзДонСтрой», целей фактически осуществляемой ООО «СоюзДонСтрой» деятельности, а также деятельности, которая предусмотрена учредительными документами ООО «СоюзДонСтрой», и конкретных бизнес-процессов в конкретных ИСПДн.

К целям обработки ПДн в ООО «СоюзДонСтрой» относятся:

- заключение, исполнение и прекращение гражданско-правовых договоров;
- организация кадрового учета организации, обеспечение соблюдения законов, заключение и исполнение обязательств по трудовым и гражданско-правовым договорам;
- ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, пользовании льготами;
- исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц, взносов во внебюджетные фонды и страховых взносов во внебюджетные фонды, пенсионного законодательства при формировании и передаче в ПФР персонализированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование;
- заполнение первичной статистической документации в соответствии с трудовым, налоговым законодательством и иными федеральными законами.
- организация контрольно-пропускного режима.

Под обработкой ПДн в ООО «СоюзДонСтрой» подразумевается любое действие (операция) или совокупность действий (операций) с ПДн, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

Безопасность персональных данных достигается путем исключения 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.

Структура, состав и основные функции технических и организационных мероприятий СЗПДн определяются исходя из уровня защищенности (класса) ИСПДн, установленного в соответствии с требованиями Постановления Правительства № 1119 от 1 ноября 2012 г., приказа ФСТЭК России № 17 от 11 февраля 2013 г., приказа ФСТЭК России № 21 от 18 февраля 2013 г., а также в соответствии с требованиями Постановления Правительства Российской Федерации № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);
- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации мер защиты СЗПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия СЗПДн требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИСПДн следующих организационно-распорядительных документов:

- План мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;
- План мероприятий по контролю обеспечения защиты ПДн;
- Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;
- Должностная инструкция администратора ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
- Должностная инструкция администратора безопасности ИСПДн;

- Должностная инструкция пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
- Инструкция на случай возникновения внештатной ситуации;
- Инструкция по размещению, оборудованию и охране помещений, где хранятся персональные данные, по хранению персональных данных на бумажных носителях и порядку работы исполнителей с персональными данными на бумажных носителях информации.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн ООО «СоюзДонСтрой».

## 2 Задачи СЗПДн

Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

Для достижения основной цели система безопасности ПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования ИСПДн и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:
- к информации, циркулирующей в ИСПДн;
- средствам вычислительной техники ИСПДн;
- аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;
- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн;
- оборудование и охрана помещений, где хранятся персональные данные;
- соблюдение порядка хранения персональных данных на бумажных носителях;
- соблюдение порядка хранения ключей от помещений где хранятся ПДн на бумажных носителях;
- соблюдение порядка работы исполнителей с персональными данными на бумажных носителях информации.

### **3 Объекты защиты**

#### **Перечень информационных систем**

В ООО «СоюзДонСтрой» производится обработка персональных данных в информационной системе обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется в процессе работы комиссии, по итогам работ которой составляется акт классификации ИСПДн.

#### **Перечень объектов защиты**

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Список персональных данных, подлежащие защите, определен в Перечне персональных данных, подлежащих защите в ИСПДн.

Объекты защиты включают:

- Обрабатываемая информация.
- Технологическая информация.
- Программно-технические средства обработки.
- Средства защиты ПДн.
- Каналы информационного обмена и телекоммуникации.
- Объекты и помещения, в которых размещены компоненты ИСПДн.

#### 4 Классификация пользователей ИСПДн

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник ООО «СоюзДонСтрой», имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями. Пользователи ИСПДн делятся на три основные категории:

##### Администратор информационной безопасности.

Сотрудники ООО «СоюзДонСтрой», которые занимаются настройкой, внедрением и сопровождением систем безопасности. Администратор ИБ обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- не обладает правами конфигурирования и административной настройки технических средств ИСПДн.

##### Администратор ИСПДн.

Сотрудники ООО «СоюзДонСтрой», которые занимаются сопровождением программного обеспечения.

Администратор ИСПДн обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

##### Оператор ИСПДн.

Сотрудники подразделений ООО «СоюзДонСтрой» участвующих в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

## 5 Меры, методы и средства обеспечения требуемого уровня защищенности

### Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

### Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер – сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности ПДн в ИСПДн состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;
- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

- регламента доступа в помещения ИСПДн;
- порядка допуска сотрудников к использованию ресурсов ИСПДн ООО «СоюзДонСтрой»;
- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;
- инструкций пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора ИСПДн);
- инструкции пользователя при возникновении внештатных ситуаций.
- инструкции по размещению, оборудованию и охране помещений, где хранятся персональные данные, по хранению персональных данных на бумажных носителях и порядку работы исполнителей с персональными данными на бумажных носителях информации.

#### **Физические меры защиты**

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключая нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

#### **Аппаратно-программные средства защиты ПДн**

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн ООО «СоюзДонСтрой»;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонентов ИСПДн;
- каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им

своих функциональных обязанностей полномочия по доступу к ресурсам системы;

- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства ООО «СоюзДонСтрой»;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);
- специалистами ООО «СоюзДонСтрой» осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

## **6 Контроль эффективности СЗПДн**

Контроль эффективности СЗПДн должен осуществляться на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

## 7 Сферы ответственности за безопасность ПДн

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководство ООО «СоюзДонСтрой». Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.

Сфера ответственности руководителя включает следующие направления обеспечения безопасности ПДн:

- Планирование и реализация мер по обеспечению безопасности ПДн;
- Анализ угроз безопасности ПДн;
- Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;
- Обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;
- Предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 3), с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн». Подготовка типовых вариантов этих соглашений осуществляется юристами ООО «СоюзДонСтрой».

## 8 Модель нарушителя безопасности

Под нарушителем в ООО «СоюзДонСтрой» понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн, а также хранятся ПДн на бумажных носителях;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн, а также хранятся ПДн на бумажных носителях.
- Классификация нарушителей представлена в Модели угроз безопасности персональных данных.

## 9 Модель угроз безопасности

Для ИСПДн ООО «СоюзДонСтрой» выделяются следующие основные категории угроз безопасности персональных данных:

- Угрозы от утечки по техническим каналам.
- Угрозы несанкционированного доступа к информации.
- Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.
- Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).
- Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.
- Угрозы преднамеренных действий внутренних нарушителей.
- Угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в «Модели угроз безопасности персональных данных в ИСПДн».

## **10 Порядок работы с персональными данными сотрудников Обязанности работодателя**

В целях исполнения требований законодательства Российской Федерации при обработке персональных данных, все работники ООО «СоюзДонСтрой» должны исполнять установленный порядок работы:

Работа с персональными данными работников должна не нарушать требований законодательства Российской Федерации, локальных нормативных актов организации, и должна быть непосредственно связана с осуществлением ими своих трудовых функций.

При сборе и обработке персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

Персональные данные работников должны быть получены только непосредственно у него. Если для обработки его данных или их получения привлекается третья лица, то работник должен дать предварительное письменное согласие на это. Одновременно работник должен быть уведомлен о целях сбора информации, источниках ее получения, а также о последствиях отказа от предоставления письменного согласия на сбор информации.

Персональные данные работника о его политических, религиозных и иных убеждениях, частной жизни, а также членстве в общественных и профсоюзных организациях не подлежат сбору организацией, если иное не предусмотрено законодательством.

Защита персональных данных работника должна обеспечиваться полностью за счет работодателя.

Учреждение при приеме на работу, а также при любых изменениях правил работы с персональными данными обязано письменно знакомить с ними всех работников.

Учреждение не имеет право принуждать работников к отказу от своих прав на защиту персональных данных.

### **Обязанности работника**

Работник обязан:

Передать работодателю все персональные данные, указанные в соответствующих документах.

В установленный правилами срок сообщать работодателю об изменении своих персональных данных.

### **Передача персональных данных**

Для организации передачи (распространения) персональных данных соблюдаются следующие условия:

- Берется письменное согласие работника на обработку персональных данных, разрешенных для распространения, оформляется отдельно от других согласий на обработку его персональных данных. При этом соблюдаются условия, предусмотренные, в частности, ст. 10.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных". Требования к содержанию такого согласия устанавливаются уполномоченным органом по защите прав субъектов персональных данных.
- Письменное согласие на обработку персональных данных, разрешенных для распространения, работник предоставляет Работодателю лично.

- Работодатель обязан не позднее трех рабочих дней с момента получения указанного согласия опубликовать информацию об условиях обработки, о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных для распространения.
- Согласие на обработку персональных данных, разрешенных для распространения, прекращает свое действие с момента поступления Работодателю требования.

При осуществлении передачи персональных данных работников третьим лицам работодатель обязан:

- не сообщать персональные данные без полученного письменного согласия работника, кроме случаев, когда такие обязанности установлены законодательством;
- не передавать персональные данные работника для использования в коммерческих целях;
- требовать от третьих лиц соблюдения правил работы с персональными данными, а также предоставления письменного подтверждения использования персональных данных в порядке, предусмотренных настоящим положением о защите персональных данных;
- давать доступ к персональным данным только лицам, имеющим соответствующий допуск и использующих их только для выполнения конкретных полномочий;
- не истребовать информацию о состоянии здоровья работника, за исключением данных, которые могут повлиять на исполнение работником своих трудовых обязанностей.

### **Защита персональных данных работника**

В рамках реализации пунктов настоящего Положения о защите персональных данных работников, руководитель учреждения издает приказ о назначении лица, ответственного за соблюдение порядка работы с персональными данными работников, на котором лежат все обязанности по обеспечению конфиденциальности полученных данных, а также организации работы с ними.

Передача информации происходит только в письменном виде. Запрос должен быть сделан в письменном виде с указанием всех реквизитов лица, запрашивающего информацию. Ответ должен быть сделан на фирменном бланке учреждения и отправлен либо курьерской службой, либо заказным письмом.

Все полученные персональные данные должны храниться в месте, исключаящем несанкционированных доступ третьих лиц.

Электронные носители информации, должны быть защищены криптографическими средствами защиты информации.

### **Ответственность за разглашение информации, связанной с персональными данными работника**

Лица, признанные виновными в нарушении требований настоящего Положения о защите персональных данных работником, привлекаются к дисциплинарной, административной, гражданско-правовой и уголовной ответственности, в порядке, предусмотренном законодательством РФ и локальными нормативными актами.

## **11 Порядок работы с персональными данными контрагентов**

### **Порядок получения и обработки персональных данных контрагентов**

Под обработкой ПДн понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных контрагентов.

Работа с персональными данными контрагентов должна не нарушать требований законодательства РФ и локальных нормативных актов организации.

Использование персональных данных возможно только в соответствии с целями, определившими их получение. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

Порядок обработки персональных данных на бумажных материальных носителях регламентирован «Инструкцией по хранению персональных данных на бумажных носителях и порядку работы исполнителей с персональными данными на бумажных носителях информации», утвержденной руководителем.

Обработка персональных данных в автоматизированных информационных системах осуществляется на основании ряда утвержденных руководителем инструкций, регламентирующих обработку персональных данных в ИСПДн.

### **Доступ к персональным данным**

Внутренний доступ (доступ внутри организации) определяется перечнем лиц, имеющих доступ к персональным данным контрагентов, определяется приказом руководителя.

Внешний доступ:

К числу массовых потребителей персональных данных вне организации можно отнести государственные функциональные структуры: налоговые инспекции, правоохранительные органы, органы статистики, военкоматы, органы социального страхования, пенсионные фонды, подразделения муниципальных органов управления;

Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

### **Права обязанности и ответственность субъекта персональных данных**

Закрепление прав субъектов персональных данных, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

В целях защиты персональных данных контрагенты (законные представители) имеют право:

- требовать исключения или исправления неверных, или неполных персональных данных, свободный бесплатный доступ к своим персональным данным, включая право на получение копии новой записи, содержащей персональные данные;

- определять своих представителей для защиты своих персональных данных на сохранение и защиту своей личной тайны.

### **Права обязанности и ответственность оператора персональных данных**

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 документу, содержащему персональные сведения контрагентов, несет персональную ответственность за данное разрешение.

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

Допуск к персональным данным контрагентов других сотрудников работодателя, не имеющих надлежащим образом оформленного доступа, запрещается.

Передача (обмен и т.д.) персональных данных между подразделениями осуществляется только между сотрудниками, имеющими доступ к персональным данным контрагентов.

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 РФ дисциплинарные взыскания.

## 12 Особенности обработки персональных данных без использования средств автоматизации

При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

Документы (носители информации), содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах).

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на

том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ. Хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях должно быть отдельным.

### 13 Список использованных источников

**Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:**

Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утверждены Постановлением Правительства РФ от 01.11.2012 г. № 1119.

«Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.

Постановление Правительства № 211 от 21 марта 2012 года «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

«Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.

Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г.

Методика оценки угроз безопасности информации, утвержденная ФСТЭК России 5 февраля 2021 года.

Приказ ФСТЭК России № 21 от 18 февраля 2013 года «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

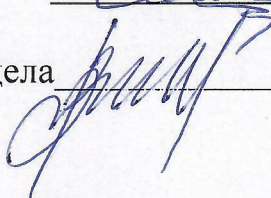
Согласовано:

Исполнительный директор



Сабадырева Н.В.

Начальник Юридического отдела



Царькова В.В.