

**Муниципальное бюджетное учреждение  
Дополнительного образования «Центр детского творчества «Ирбис» г.о. Самара**

**ПРИНЯТО**  
Общим собранием работников  
МБУ ДО ЦДТ «Ирбис»  
г. о. Самара

Протокол от 25.05.2023 № 3

**УТВЕРЖДЕНО**  
Приказом МБУ ДО ЦДТ  
«Ирбис» г. о. Самара  
от 16.06.2023 № 281

Директор Сенников

П.В. Сенников



**Концепция информационной безопасности  
МБУ ДО «Центра детского творчества «Ирбис»  
г. о. Самара**

2023

# **КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ информационной системы персональных данных**

## **1. Общие положения**

1.1. Настоящая Концепция информационной безопасности информационной системы персональных данных (далее – ИСПДн) муниципального бюджетного учреждения дополнительного образования «Центра детского творчества «Ирбис» г.о. Самара (далее – образовательная организация или ЦДТ «Ирбис»), является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности образовательной организации.

1.1.1. Разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ (с изменениями) "Об информации, информационных технологиях и о защите информации";
- Федеральным Законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (с изменениями);
- Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановлением Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации";
- Постановлением Правительства РФ от 06.07.2008 № 512 (с изменениями) "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";
- Приказом ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г. (ДСП);
- Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. зам. директора ФСТЭК России 15.02.2008 г. (ДСП).

1.1.2. Определяет:

- основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) образовательной организацией;
- основные требования и базовые подходы к реализации задач, для достижения требуемого уровня безопасности информации.

1.1.3. Служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности образовательной организации, 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.

1.1.4. Является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн образовательной организации;
- 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 образовательной организации 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 образовательной организации.

1.2. Является локальным нормативным актом, регламентирующим деятельность образовательной организации.

1.3. Принимается общим собранием работников образовательной организации и утверждается приказом образовательной организации.

1.4. Принимается на неопределенный срок.

### **Используемые определения**

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

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

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

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

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной 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.

**Закладочное устройство** – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**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.

**Информативный сигнал** – электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базе данных персональных данных и обеспечивающих их обработку с помощью информационных технологий и технических средств.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**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.

**Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и / или выходящей из информационной системы.

**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.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**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.

**Образовательная организация** – МБУ ДО «Центр детского творчества «Ирбис» г.о. Самара.

**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) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и 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 (оператор)** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и / или осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому, на основании такой информации, физическому лицу (субъекту персональных данных).

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**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.

**Программная закладка** – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных, и / или блокировать аппаратные средства.

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Программное (программно-математическое) воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляющееся с использованием вредоносных программ.

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

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** – персональные данные, касающиеся расовой и 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.

**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.

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

**Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**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.

**Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

## **2. Цели и задачи Концепции**

Концепция разработана 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 в обрабатывающей их инфраструктуре от несанкционированного, в том числе

случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре.

**Целью** СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

**Задачи ИСПДн:**

- защита от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС 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;
- регистрация 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;
- защита от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защита системы от внедрения несанкционированных программ;
- защита ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защита 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.

### **3. Условия, обеспечивающие защиту персональных данных**

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. 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 ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн 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;
- Рекомендации по использованию программных и аппаратных средств защиты 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 образовательной организации.

## **4. Объекты защиты**

### **4.1 Перечень информационных систем**

В образовательной организации производится обработка персональных данных в информационных системах обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется на основании Отчета по результатам внутренней проверки.

#### **4.2 Перечень объектов защиты**

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

Объекты защиты включают:

- обрабатываемую информацию;
- технологическую информацию;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

### **5. Классификация пользователей ИСПДн**

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник образовательной организации, 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:

- 1) Администратор ИСПДн. Сотрудники образовательной организации, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИСПДн 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;
  - обладает правами конфигурирования и административной настройки технических средств ИСПДн.
- 2) Программист-разработчик ИСПДн. Сотрудники образовательной организации или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик 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.
- 3) Оператор ИСПДн. Сотрудники образовательной организации участвующие 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.

Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей, определенными в Политике информационной безопасности.

Все выявленные группы пользователей отражаются в Отчете по результатам внутренней проверки. На основании Отчета определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Матрице доступа в Положении о разграничении прав доступа к обрабатываемым персональным данным.

## **6. Основные принципы построения системы комплексной защиты информации**

Построение системы обеспечения безопасности ПДн ИСПДн образовательной организации и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

|                      |   |
|----------------------|---|
| <b>Законность</b>    | <p>Предполагает осуществление защитных мероприятий и разработку СЗПДн образовательной организации в соответствии с действующим законодательством в области защиты ПДн и другими нормативными правовыми актами по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.</p> <p>Пользователи и обслуживающий персонал ПДн ИСПДн образовательной организации должны быть осведомлены о порядке работы с защищаемой информацией, и об ответственности за защиту ПДн.</p>  |
| <b>Системность</b>   | <p>Системный подход к построению СЗПДн образовательной организации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн образовательной организации.</p> <p>При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.</p> |
| <b>Комплексность</b> | <p>Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.</p> <p>Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их</p>   |

|  |  |
|--|--|
|  | <p>преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.</p> <p>Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.</p>  |
| <b>Непрерывность защиты ПДн</b>            | <p>Задача ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.</p> <p>ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.</p> <p>Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок", и других средств преодоления системы защиты после восстановления ее функционирования.</p> |
| <b>Своевременность</b>                     | <p>Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн, в целом, и ее системы защиты информации, в частности.</p> <p>Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании информационной архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.</p>  |
| <b>Преемственность и совершенствование</b> | <p>Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.</p>   |
| <b>Персональная ответственность</b>        | <p>Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим</p>   |

|   |  |
|---|--|
|   | принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.  |
| <b>Принцип минимизации полномочий</b>                     | <p>Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».</p> <p>Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.</p>  |
| <b>Взаимодействие и сотрудничество</b>                    | <p>Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн образовательной организации, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.</p> <p>В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.</p>   |
| <b>Гибкость системы защиты ПДн</b>                        | Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.  |
| <b>Открытость алгоритмов и механизмов защиты</b>          | Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.  |
| <b>Простота применения средств защиты</b>                 | Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.). Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн. |
| <b>Научная обоснованность и техническая реализуемость</b> | Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации, должны  |

|  |   |
|--|---|
|  | <p>соответствовать установленным нормам и требованиям по безопасности ПДн.</p> <p>СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.</p>   |
| <b>Специализация и профессионализм</b> | <p>Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами образовательной организации.</p>   |
| <b>Обязательность контроля</b>         | <p>Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.</p> <p>Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.</p> |

## 7. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

|                                       |  |
|---------------------------------------|--|
| <b>Правовые меры защиты</b>           | <p>К правовым мерам защиты относятся действующие в стране законы и иные нормативные правовые 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.</p> <p>Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.</p> |
| <b>Морально-этические меры защиты</b> | <p>К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их</p>  |

|   |   |
|---|---|
|   | <p>несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписанные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.</p> <p>Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.</p>  |
| <b>Организационные (административные) меры защиты</b> | <p>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.</p> <p>Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы, и контролируя состояние дел.</p> <p>Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.</p> <p>К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:</p> <ul style="list-style-type: none"> <li>– принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;</li> <li>– формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;</li> <li>– принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне (краткое наименование оператора) в целом;</li> <li>– обеспечение нормативно - правовой базы вопросов безопасности и т.п.</li> </ul> <p>Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.</p> <p>На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:</p> <ul style="list-style-type: none"> <li>– какова область применения политики безопасности ПДн;</li> </ul> |

|                               |   |
|-------------------------------|---|
|                               | <ul style="list-style-type: none"> <li>– каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а также установить их ответственность;</li> <li>– кто имеет права доступа к ПДн;</li> <li>– какими мерами и средствами обеспечивается защита ПДн;</li> <li>– какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.</li> </ul> <p>Организационные меры должны:</p> <ul style="list-style-type: none"> <li>– предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;</li> <li>– определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;</li> <li>– определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты, криптозащиты, и других защитных механизмов;</li> <li>– организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.</li> </ul> <p>Организационные меры должны состоять из:</p> <ul style="list-style-type: none"> <li>– регламента доступа в помещения ИСПДн;</li> <li>– порядок допуска сотрудников к использованию ресурсов ИСПДн образовательной организации;</li> <li>– регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;</li> <li>– регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;</li> <li>– инструкций пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора ИСПДн);</li> <li>– инструкции пользователя при возникновении внештатных ситуаций.</li> </ul> |
| <b>Физические меры защиты</b> | <p>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.</p> <p>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,</p>  |

|  |  |
|--|--|
|  | <p>проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки (видеокамер, подслушивающих устройств).</p> <p>Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.</p>  |
| <b>Аппаратно-программные средства защиты ПДн</b> | <p>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.).</p> <p>С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:</p> <ul style="list-style-type: none"> <li>– средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;</li> <li>– средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн (краткое наименование оператора);</li> <li>– средства обеспечения и контроля целостности программных и информационных ресурсов;</li> <li>– средства оперативного контроля и регистрации событий безопасности;</li> <li>– криптографические средства защиты ПДн.</li> </ul> <p>Успешное применение технических средств защиты на основании принципов (раздел 5) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:</p> <ul style="list-style-type: none"> <li>– обеспечена физическая целостность всех компонент ИСПДн;</li> <li>– 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;</li> <li>– в ИСПДн образовательной организации разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;</li> <li>– все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства образовательной организации;</li> </ul> |

|  |  |
|--|--|
|  | <ul style="list-style-type: none"> <li>– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещений, шкафах, и т.п.).</li> <li>– специалистами образовательной организации осуществляется непрерывное управление и административная поддержка функционирования средств защиты.</li> </ul> |
|--|--|

## **8. Контроль эффективности системы защиты ИСПДн учреждения**

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.

## **9. Сфера ответственности за безопасность ПДн**

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководитель образовательной организации. 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 политики, руководств, концепции, 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, с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн».

## **10. Модель нарушителя безопасности**

Под нарушителем в образовательной организации понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

## **11. Модель угроз безопасности**

Для ИСПДн образовательной организации 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 непреднамеренных 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 каждой ИСПДн.

## **12. Механизм реализации концепции**

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- нормативно-правовых актов Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России;
- потребностей ИСПДн в средствах обеспечения безопасности информации.

### **13. Ожидаемый эффект от реализации концепции**

Реализация Концепции безопасности ПДн в ИСПДн позволит:

- оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
- разработать распорядительные и нормативно-методические документы применительно к ИСПДн;
- провести классификацию и сертификацию ИСПДн;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;
- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для ее дальнейшего совершенствования.

### **14. Заключительные положения**

11.1. Изменения и дополнения к Концепции вносятся общим собранием работников образовательной организации, принимаются на его заседании и утверждаются приказом образовательной организации.

11.2. После принятия новой редакции Концепции предыдущая редакция утрачивает силу.