

Принято:

Управляющим советом

МДОУ «ЦРР-детский сад «Улыбка»

Протокол № 2 от « 15 » 03 2016г

Утверждаю:

Заведующий МДОУ

«ЦРР-детский сад «Улыбка»

Н.И. Куликова

Приказ № 38 от « 18 » 03 2016г.



**Концепция информационной безопасности
информационных систем персональных данных
МДОУ «Центр развития ребенка – детский сад «Улыбка»**

ОГЛАВЛЕНИЕ

Определения.....	3
Обозначения и сокращения	7
Введение.....	8
1 Общие положения	9
2 Задачи СЗПДн.....	10
3 Объекты защиты.....	11
3.1 Перечень информационных систем.....	11
3.2 Перечень объектов защиты.....	11
4 Классификация пользователей ИСПДн.....	12
5 Основные принципы построения системы комплексной защиты информации	13
5.1 Законность.....	13
5.2 Системность	13
5.3 Комплексность.....	13
5.4 Непрерывность защиты ПДн.....	14
5.5 Своевременность	14
5.6 Преимущество и совершенствование.....	14
5.7 Персональная ответственность	14
5.8 Принцип минимизации полномочий	14
5.9 Взаимодействие и сотрудничество	14
5.10 Гибкость системы защиты ПДн	15
5.11 Открытость алгоритмов и механизмов защиты.....	15
5.12 Простота применения средств защиты.....	15
5.13 Научная обоснованность и техническая реализуемость.....	15
5.14 Специализация и профессионализм	15
5.15 Обязательность контроля.....	15
6 Меры, методы и средства обеспечения требуемого уровня защищенности	16
6.1 Законодательные (правовые) меры защиты.....	16
6.2 Морально-этические меры защиты.....	16
6.3 Организационные (административные) меры защиты	16
6.4 Физические меры защиты.....	17
6.5 Аппаратно-программные средства защиты ПДн	18
7 Контроль эффективности системы защиты ИСПДн ДОУ	19
8 Сферы ответственности за безопасность ПДн	19
9 Модель нарушителя безопасности.....	20
10 Модель угроз безопасности.....	20
11 Механизм реализации Концепции.....	21
12 Ожидаемый эффект от реализации Концепции.....	21
13 Список использованных источников.....	22

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.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся 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 сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

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.

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.

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 – электрические сигналы, 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) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств, используемая в образовательном учреждении.

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 распространения 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.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, 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, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

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, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

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

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

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

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 оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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 невозможно восстановить содержание персональных данных в информационной системе персональных данных 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).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства

АС – автоматизированная система

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ОУ – образовательное учреждение.

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

ТС – технические средства

УБПДн – угрозы безопасности персональных данных

АИБ – администратор информационной безопасности

ВВЕДЕНИЕ

Настоящая Концепция информационной безопасности ИСПДн, используемая в МДОУ «ЦРР – детский сад «Улыбка» (далее - ДОУ), является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности ДОУ.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗ ПДн) ДОУ. Концепция определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации.

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 и обрабатывающей их инфраструктуры 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.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ДОУ, 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.

Концепция является методологической основой для:

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

Область применения Концепции распространяется на все структурные подразделения ДОУ, эксплуатирующие технические и программные средства ИСПДн, в которых осуществляется автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

Правовой базой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных (ПДн).

1. Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) ДОУ, в соответствии с Перечнем ИСПДн ДОУ. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

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 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;
- Должностная инструкция пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
- Инструкция пользователя на случай возникновения внештатной ситуации;

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

Перечень необходимых мер защиты информации определен по результатам внутренней проверки безопасности ИСПДн ОУ.

2. Задачи системы защиты персональных данных (СЗПДн)

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

Для достижения основной цели система безопасности ПДн ИСПДн обеспечивает эффективное решение следующих задач:

- защиту 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:
 - а) к информации, циркулирующей в ИСПДн;
 - б) к средствам вычислительной техники ИСПДн;
 - в) к 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.

3. Объекты защиты

3.1. Перечень информационных систем

В ДОУ производится обработка персональных данных с помощью следующих ИСПДн:

- Е-услуги. Образование;
- Парус-бюджет;
- Контур-Экстерн;
- ПРО-ГОСЗАКУПКИ.РУ;
- Комплексная автоматизированная система ИРО.

3.2. Перечень объектов защиты

Объектами защиты является информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Персональные данные, подлежащие защите, определены в Перечне персональных данных, подлежащих защите в ИСПДн.

Объекты защиты включают следующие компоненты:

- 1) Обрабатываемая информация.
- 2) Технологическая информация.
- 3) Программно-технические средства обработки.
- 4) Средства защиты ПДн.
- 5) Каналы информационного обмена и телекоммуникации.
- 6) 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. В ДОУ пользователем ИСПДн является ответственный сотрудник, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Пользователи ИСПДн в ДОУ относятся к категории оператор ИСПДн и обладают следующими уровнями доступа:

- обладают всеми необходимыми атрибутами (логином, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагают конфиденциальными данными, к которым имеют доступ.

Категория пользователей определена для каждой ИСПДн. 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 определены права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Матрице доступа пользователей к ПДн.

5. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности ПДн в ИСПДн ДОУ и ее функционирование осуществляются в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

5.1. Законность

Защитные мероприятия СЗПДн ДОУ разработаны в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи ПДн в ИСПДн осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение защиты ПДн.

5.2. Системность

Учтены все взаимосвязанные, взаимодействующие и изменяющиеся во времени элементы, условия и факторы, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн в ИСПДн ДОУ.

5.3. Комплексность

Комплексное использование методов и средств защиты согласовано с применением разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита построена эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности существует несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита обеспечивается физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывает особенности предметной области, представляет внутренний рубеж защиты.

5.4. Непрерывность защиты ПДн

Защита ПДн – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

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.

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.

5.5. Своевременность

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.

Разработка системы защиты ведется параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

5.6. Преимущество и совершенствование

Постоянное совершенствование мер и средств защиты информации на основе преимущественности 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.

5.7. Персональная ответственность

Возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.8. Принцип минимизации полномочий

Предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью.

Доступ к ПДн предоставляется только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

5.9. Взаимодействие и сотрудничество

Создание благоприятной атмосферы в коллективах подразделений, обеспечивающих функционирование ИСПДн ДОУ, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке сотрудники осознанно соблюдают установленные правила и оказывают содействие в деятельности подразделений защиты информации.

5.10. Гибкость системы защиты ПДн

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, обеспечивают как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты обладают определенной гибкостью.

5.11. Открытость алгоритмов и механизмов защиты

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.

5.12. Простота применения средств защиты

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.

5.13. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации реализуются на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и соответствуют установленным нормам и требованиям по безопасности ПДн.

СЗПДн ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

5.14. Специализация и профессионализм

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 ДОУ.

5.15. Обязательность контроля

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.

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.

6. Меры, методы и средства обеспечения требуемого уровня защищенности

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

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражен в Плане мероприятий по обеспечению защиты персональных данных.

6.1. 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.

6.2. Морально-этические меры защиты

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 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 писанные, то есть оформленные в некоторый свод (устав) правил или предписаний.

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.

6.3. 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, 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.

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. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне ДООУ в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

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.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

- какова область применения политики безопасности ПДн;
- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а также их установить ответственность;
- кто имеет права доступа к ПДн;
- какими мерами и средствами обеспечивается защита ПДн;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры:

- предусматривают регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определяют коалиционные и иерархические принципы и методы разграничения доступа к ПДн;
- определяют порядок работы с программно-математическими и техническими (аппаратными) средствами защиты и криптозащиты и других защитных механизмов;
- организуют меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.
- Организационные меры состоят из:
 - Порядка допуска сотрудников к использованию ресурсов ИСПДн ОУ (Разрешительная система доступа к ПДн);
 - Инструкций пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора ИСПДн);
 - Инструкции пользователя при возникновении внештатных ситуаций.

6.4. 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, исключаящими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

6.5. 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 включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн ДОУ;
- 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 на основании принципов (раздел 5) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый сотрудник (пользователь ИСПДн) имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- в ИСПДн ДОУ разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;
- сетевое оборудование (концентраторы, коммутаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

7. Контроль эффективности системы защиты ИСПДн ДОУ

Контроль эффективности СЗПДн осуществляется 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.), прогнозирование атак и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль проводится администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн) 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.

8. Сферы ответственности за безопасность ПДн

Ответственными за разработку мер и контроль над обеспечением безопасности персональных данных являются операторы, назначаемые приказом заведующего ДОУ.

Сфера ответственности операторов включает следующие направления обеспечения 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.
- Не реже одного раза в квартал (а при наличии необходимости и чаще) информирование руководства ДОУ о состоянии информационной безопасности.

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.

9. Модель нарушителя безопасности

Под нарушителем в ДООУ понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел 3).

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 ИСПДн.

10. Модель угроз безопасности

Для ИСПДн ДООУ выделяются следующие основные категории угроз безопасности персональных данных:

- 1) Угрозы от утечки по техническим каналам.
- 2) 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.) характеров.
 - Угрозы преднамеренных действий внутренних нарушителей.
 - Угрозы несанкционированного доступа по каналам связи.

11. Механизм реализации Концепции

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

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

12. 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 обеспечивает создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для ее дальнейшего совершенствования.

13. Список использованных источников

1 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.

2 Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

3 «Порядок проведения классификации информационных систем персональных данных», утвержденный совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи РФ № 20 от 13.02.2008 г.

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

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

6 Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

7 Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

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

9 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

**Лист ознакомления
с Концепцией информационной безопасности информационных систем
персональных данных МДОУ «ЦРР – детский сад «Улыбка»**

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления с Инструкцией	Подпись ра- ботника
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			