**Концепция информационной безопасности**

**персональных данных**

**муниципального автономного дошкольного образовательного учреждения**

**Киселевского городского округа «Детский сад № 2 «Лучики» комбинированного вида»**

**г. Киселёвск**

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

2

**ОПРЕДЕЛЕНИЯ**

* настоящем документе используются следующие термины и их определения. **Автоматизированная система** –система,состоящая из персонала и комплекса

средств автоматизации его деятельности, реализующая информационную технологию выпол-нения установленных функций.

**Аутентификация отправителя данных** –подтверждение того,что отправитель по-лученных данных соответствует заявленному.

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

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

**Блокирование персональных данных** –временное прекращение сбора,системати-зации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** –исполняемый программный код или ин-терпретируемый набор инструкций, обладающий свойствами несанкционированного распро-странения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и са-мовоспроизведению.

**Вредоносная программа** –программа,предназначенная для осуществления несанк-ционированного доступа и (или) воздействия на персональные данные или ресурсы информа-ционной системы персональных данных.

**Вспомогательные технические средства и системы** –технические средства и систе-мы, не предназначенные для передачи, обработки и хранения персональных данных, устанав-ливаемые совместно с техническими средствами и системами, предназначенными для обра-ботки персональных данных или в помещениях, в которых установлены информационные систе-мы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персо-нальных 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(за-

кладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, кон-струкцию, оборудование, предметы интерьера, транспортные средства, а также в технические сред-ства и системы обработки информации).

**Защищаемая информация** –информация,являющаяся предметом собственности и под-лежащая защите в соответствии с требованиями правовых документов или требованиями, устанавли-ваемыми собственником информации.

**Идентификация** –присвоение субъектам и объектам доступа идентификатора и(или)сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** –электрические сигналы,акустические,электромагнитные идругие физические поля, по параметрам которых может быть раскрыта конфиденциальная информа-ция (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** –информационнаясистема, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуще-ствлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

3

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

**Использование персональных данных** –действия(операции)с персональными дан-ными, 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 объектили физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** –пространство(территория,здание,часть здания,помещение),в ко-тором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, техниче-ских и иных материальных средств.

**Конфиденциальность персональных данных** –обязательное для соблюдения операто-ром или иным получившим доступ к персональным данным лицом требование не допускать их рас-пространение без согласия субъекта персональных данных или наличия иного законного основания.

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

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

**Неавтоматизированная обработка персональных данных** –обработка персональ-ных данных, содержащихся в информационной системе персональных данных либо извле-ченных из такой системы, считается осуществленной без использования средств автоматиза-ции (неавтоматизированной), если такие действия с персональными данными, как использо-вание, уточнение, распространение, уничтожение персональных данных в отношении каждо-го из субъектов персональных данных, осуществляются при непосредственном участии че-ловека.

**Недекларированные возможности** –функциональные возможности средств вычисли-тельной техники, не описанные или не соответствующие описанным в документации, при использо-вании которых возможно нарушение конфиденциальности, доступности или целостности обрабаты-ваемой информации.

**Несанкционированный доступ (несанкционированные действия)** –доступ к ин-формации или действия с информацией, нарушающие правила разграничения доступа с использова-нием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** –физическое лицо или материальный объект,в том числе физиче-ское поле, в котором информация находит свое отражение в виде символов, образов, сигналов, техни-ческих решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** –действия,в результате которых невозмож-но определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** –действия(операции)с персональными данными,включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), исполь-зование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение пер-сональных данных.

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

4

**Оператор (персональных данных)** –государственный орган,муниципальный орган,юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональ-ных данных, а также определяющие цели и содержание обработки персональных данных.

**Технические средства информационной системы персональных данных** –средствавычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроиз-ведения, переговорные и телевизионные устройства, средства изготовления, тиражирования доку-ментов 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.

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

**Персональные данные** –любая информация,относящаяся к определенному или оп-ределяемому 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 излучениятехнических средств обработки защищаемой информации, возникающие как побочное явле-ние и вызванные электрическими сигналами, действующими в их электрических и магнит-ных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, кон-струкции и цепи питания.

**Политика «чистого стола»** –комплекс организационных мероприятий,контроли-рующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паро-лей) и хранения их вблизи объектов доступа.

**Пользователь информационной системы персональных данных** –лицо,участ-вующее в функционировании информационной системы персональных данных или исполь-зующее результаты ее функционирования.

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

**Программная закладка** –код программы,преднамеренно внесенный в программу сцелью осуществить утечку, изменить, блокировать, уничтожить информацию или уничто-жить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

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

**Раскрытие персональных данных** –умышленное или случайное нарушение конфи-денциальности персональных данных.

**Распространение персональных данных** –действия,направленные на передачуперсональных данных определенному кругу лиц (передача персональных данных) или на оз-накомление с персональными данными неограниченного круга лиц, в том числе обнародова-ние персональных данных в средствах массовой информации, размещение в информацион-но-телекоммуникационных сетях или предоставление доступа к персональным данным ка-ким-либо иным способом.

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

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

5

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

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

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

**Трансграничная передача персональных данных** –передача персональных данныхоператором через Государственную границу Российской Федерации органу власти ино-странного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** –совокупность условий и факторов,соз-дающих опасность несанкционированного, в том числе случайного, доступа к персональным дан-ным, результатом которого может стать уничтожение, изменение, блокирование, копирование, рас-пространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** –действия,в результате которых невозможно вос-становить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** –неконтролируемоераспространение информации от носителя защищаемой информации через физическую среду до тех-нического средства, осуществляющего перехват информации.

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

**Целостность информации** –способность средства вычислительной техники или автома-тизированной системы обеспечивать неизменность информации в условиях случайного и/или пред-намеренного искажения (разрушения).

6

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

АВС – антивирусные средства

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

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных СОВ – система обнаружения вторжений ТКУИ – технические каналы утечки информации УБПДн – угрозы безопасности персональных данных

7

**ВВЕДЕНИЕ**

Настоящая Концепция информационной безопасности ИСПДн муниципального автономного дошкольного образовательного учреждения Киселевского городского округа «Детский сад № 2 «Лучики» комбинированного вида» (далее – МАДОУ №2 «Лучики») является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности МАДОУ №2и «Лучики». Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в МАДОУ №2 «Лучики», при обработке информации вообще, и персональных данных в частности. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) МАДОУ №2 «Лучики». Концепция определяет основные требования и базовые подходы 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 инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также

* прогнозированию и предотвращению таких воздействий. Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информацион-ной безопасности ОИВ (ОМСУ), а также нормативных и методических документов, обеспе-чивающих 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 МАДОУ №2 «Лучики»;

-принятия управленческих решений и разработки практических мер по воплощению полити-

ки 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 МАДОУ №2 «Лучики» 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 МАДОУ №2 «Лучики».

Область применения Концепции распространяется на все эксплуатирующие техниче-ские и программные средства ИСПДн МАДОУ №2 «Лучики», в которых осуществляется автоматизированная обработка ПДн.

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

8

1. **ОБЩИЕ ПОЛОЖЕНИЯ**

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) МАДОУ №2 «Лучики», в соответствии с Перечнем ИСПДн. 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 несанкциониро-ванного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персо-нальных данных, а также иных несанкционированных действий. Структура, состав и основ-ные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организаци-онные меры и технические средства защиты информации, средства предотвращения несанк-ционированного 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 защищен-ность от разрушения и несанкционированного изменения);
* доступность информации (возможность за приемлемое время получить требуемую инфор-мационную услугу).

Стадии создания СЗПДн включают:

* предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку тех-нического (частного технического) задания на ее создание;
* стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разра-ботку 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 базыбезопасности ПДн и разработку (введение в действие) предусмотренных Политикой инфор-мационной безопасности ИСПДн следующих организационно-распорядительных докумен-тов:

* 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 ОИВ (ОМСУ).

9

1. **ЗАДАЧИ СЗПДн**

Основной целью СЗПДн является минимизация ущерба от возможной реализации уг-роз безопасности ПДн.

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

* + **защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только за-регистрированные установленным порядком пользователи);**
  + **разграничение доступа зарегистрированных пользователей к аппаратным, про-граммным 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 защи-ту от несанкционированного доступа:**

а) к информации, циркулирующей в ИСПДн; б) средствам вычислительной техники ИСПДн;

в) аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

* + **регистрацию действий пользователей при использовании защищаемых ресур-сов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;**
  + **контроль целостности (обеспечение неизменности) среды исполнения программ**
* **ее восстановление в случае нарушения;**
  + **защиту от несанкционированной модификации и контроль целостности ис-пользуемых в ИСПДн программных средств, а также защиту системы от внедрения не-санкционированных 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 усло-вий, способствующих нанесению ущерба субъектам ПДн, создание механизма опера-тивного реагирования на угрозы безопасности ПДн и негативные тенденции;**
  + **создание условий для минимизации и локализации наносимого ущерба непра-вомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.**
  1. **ОБЪЕКТЫ ЗАЩИТЫ Перечень информационных систем**
* МАДОУ №2 «Лучики» производится обработка персональных данных в ин-формационных системах обработки персональных данных (ИСПДн). Перечень ИСПДн оп-ределяется на основании Отчета по результатам внутренней проверки.

**Перечень объектов защиты**

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

Объекты защиты включают:

* Обрабатываемая информация.
* Технологическая информация.
* Программно-технические средства обработки.

10

* Средства защиты ПДн.
* Каналы информационного обмена и телекоммуникации.
* Объекты и помещения, в которых размещены компоненты ИСПДн.

1. **КЛАССИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИСПДн**

Пользователем ИСПДн является лицо, участвующее в функционировании информа-ционной системы персональных данных или использующее результаты ее функционирова-ния. Пользователем ИСПДн является любой сотрудник МАДОУ №2 «Лучики», 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 ОИВ (ОМСУ), которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уров-нем 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). Администратор ТЗ ИСПДн, это сотрудник управления образования Киселевского городского округа 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, программ-ных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее раз-работки, 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 МАДОУ №2 «Лучики», участвующих в процессе экс-плуатации 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 внутрен-ней 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.

1. **ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

Построение системы обеспечения безопасности ПДн ИСПДн МАДОУ №2 «Лучики» и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

* **законность;**
* **системность;**

11

* **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**

Предполагает осуществление защитных мероприятий и разработку СЗПДн МАДОУ №2 «Лучики» 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 и обслуживающий персонал ИСПДн МАДОУ №2 «Лучики» должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиты ПДн.

**5.2. Системность**

Системный подход к построению СЗПДн МАДОУ №2 «Лучики» предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн МАДОУ №2 «Лучики».

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 ин-формации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

**5.3. Комплексность**

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрываю-щей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Соз-дание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенци-альному злоумышленнику требовались профессиональные навыки в нескольких невзаимо-связанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационны-ми 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.

12

**5.4. Непрерывность защиты ПДн**

Защита ПДн – не разовое мероприятие и не простая совокупность проведенных меро-приятий и установленных средств защиты, а непрерывный целенаправленный процесс, пред-полагающий 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 не-допущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполне-ния своих функций необходима постоянная техническая и организационная (административ-ная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в рабо-те средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закла-док" и других средств преодоления системы защиты после восстановления ее функциониро-вания.

**5.5. Своевременность**

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть по-становку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в ча-стности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектиро-вании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресур-сов, так и по стойкости) защищенные системы.

**5.6. Преемственность и совершенствование**

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, ана-лиза функционирования ИСПДн и ее системы защиты с учетом изменений в методах и сред-ствах перехвата информации, нормативных требований по защите, достигнутого отечествен-ного и зарубежного опыта в этой области.

**5.7. Персональная ответственность**

Предполагает возложение ответственности за обеспечение безопасности ПДн и сис-темы 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 мини-муму.

**5.8. Принцип минимизации полномочий**

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запреще-но».

Доступ к ПДн должен предоставляться только в том случае и объеме, если это необ-ходимо сотруднику для выполнения его должностных обязанностей.

**5.9. Взаимодействие и сотрудничество**

Предполагает создание благоприятной атмосферы в МАДОУ №2 «Лучики», для снижения вероятности возникновения негативных действий связанных с человеческим фак-тором.

* + такой обстановке сотрудники должны осознанно соблюдать установленные правила
* оказывать содействие в деятельности подразделений технической защиты информации.

13

**5.10. Гибкость системы защиты ПДн**

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 систе-му, не нарушая процесса ее нормального функционирования.

**5.11. Открытость алгоритмов и механизмов защиты**

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что за-щита не должна обеспечиваться только за счет секретности структурной организации и алго-ритмов 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 обыч-ной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод не-скольких 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 должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности ин-формации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и ме-ры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

**5.14. Специализация и профессионализм**

Предполагает привлечение к разработке средств и реализации мер защиты информа-ции специализированных организаций, наиболее подготовленных к конкретному виду дея-тельности по обеспечению безопасности ПДн, имеющих опыт практической работы и госу-дарственную лицензию на право оказания услуг в этой области. Реализация административ-ных мер и эксплуатация средств защиты должна осуществляться профессионально подготов-ленными специалистами ОИВ (ОМСУ).

**5.15. Обязательность контроля**

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.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отно-шении любого объекта защиты должен осуществляться на основе применения средств опера-тивного контроля и регистрации и должен охватывать как несанкционированные, так и санк-ционированные действия пользователей.

14

1. **МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЁННОСТИ**

Обеспечение требуемого уровня защищенности должности достигаться с использова-нием 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 отражается в Плане мероприятий по обеспечению защиты персональных данных.

**6.1. Законодательные (правовые) меры защиты**

* + правовым мерам защиты относятся действующие в стране законы, указы и норма-тивные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязан-ности 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 потенци-альных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер

* требуют постоянной разъяснительной работы с пользователями и обслуживающим персо-налом системы.

**6.2. Морально-этические меры защиты**

* + морально-этическим мерам относятся нормы поведения, которые традиционно сло-жились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные норматив-ные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные
* некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоян-ной работы по созданию здорового морального климата в коллективах подразделений. Мо-рально-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 ресур-сов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или ис-ключить 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 подхо-ды к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

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

15

* + административному уровню относятся решения руководства, затрагивающие дея-тельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безо-пасности. 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 деятель-ности в области безопасности ПДн;**
* **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, персо-нал) 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 по-литики безопасности ПДн, а так же их установить ответственность;**
* **кто имеет права доступа к ПДн;**
* **какими мерами и средствами обеспечивается защита ПДн;**
* **какими мерами и средствами обеспечивается контроль за соблюдением введен-ного режима безопасности.**

Организационные меры должны:

* **предусматривать регламент информационных отношений, исключающих воз-можность несанкционированных действий в отношении объектов защиты;**
* **определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;**
* **определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;**
* **организовать меры противодействия НСД пользователями на этапах аутенти-фикации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.**
  + организационные меры должны состоять из:
* **регламента доступа в помещения ИСПДн;**
* **порядок допуска сотрудников к использованию ресурсов ИСПДн МАДОУ №2 «Лучики»;**
* **регламента процессов ведения баз данных и осуществления модификации ин-формационных ресурсов;**
* **регламента процессов обслуживания и осуществления модификации аппарат-ных и программных ресурсов ИСПДн;**
* **инструкций пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора ИСПДн);**
* **инструкция пользователя при возникновении внештатных ситуаций.**

**6.4. Физические меры защиты**

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

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью техниче-ских средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информа-

16

ционных носителей, самих средств информатизации, исключающими 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, реги-страцию событий, криптографическое закрытие информации и т.д.).

* + учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:
* **средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;**
* **средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн МАДОУ №2 «Лучики»;**
* **средства обеспечения и контроля целостности программных и информацион-ных ресурсов;**
* **средства оперативного контроля и регистрации событий безопасности;**
* **криптографические средства защиты ПДн.**

Успешное применение технических средств защиты на основании принципов (раздел

1. предполагает, что выполнение перечисленных ниже требований обеспечено организаци-онными (административными) мерами и используемыми физическими средствами защиты:
   * **обеспечена физическая целостность всех компонент ИСПДн;**
   * **каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;**
   * **все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства управления образования Киселевского городского округа;**
   * **сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);**
   * **специалистами управления образования Киселевского городского округа осуществляется непрерывное управление и административная поддержка функциони-рования средств защиты.**

**7. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИСПДн**

Контроль эффективности СЗПДн должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкциониро-ванное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирова-ние на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн (опера-тивный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекае-мыми для этой цели компетентными организациями, имеющими лицензию на этот вид дея-тельности, 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.

17

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

1. **СФЕРЫ ОТВЕТСТВЕННОСТИ ЗА БЕЗОПАСНОСТЬ ПДн**

Ответственным за разработку мер и контроль над обеспечением безопасности персо-нальных данных является заведующий МАДОУ №2 «Лучики». Заведующий может деле-гировать 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 со-стоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;**
* **Контроль защищенности ИТ инфраструктуры МАДОУ №2 «Лучики»**  **от угроз ИБ путем;**
* **Обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;**
* **Предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.**

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 3), с этими организа-циями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн».

1. **МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ**

Под нарушителем в ОИВ (ОМСУ) понимается лицо, которое в результате умышлен-ных или неумышленных действий может нанести ущерб объектам защиты (раздел 3).

Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушите-ли делятся на две группы:

* **внешние нарушители** – физические лица, не имеющие права пребывания натерритории контролируемой зоны, в пределах которой размещается оборудо-вание ИСПДн;
* **внутренние нарушители** – физические лица, имеющие право пребывания натерритории контролируемой зоны, в пределах которой размещается оборудо-

вание ИСПДн.

Классификация нарушителей представлена в Модели угроз безопасности персональ-ных данных каждой ИСПДн.

1. **МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

Для ИСПДн МАДОУ №2 «Лучики» - 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 про-граммных средств (в том числе программно-математических воздействий).

18

- Угрозы не преднамеренных действий пользователей и нарушений безопасности функцио-нирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропи-тания) 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.

1. **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;**
* **постановлений Правительства Российской Федерации;**
* **руководящих, организационно-распорядительных и методических документов ФСТЭК России;**
* **потребностей ИСПДн в средствах обеспечения безопасности информации.**

1. **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 приме-нительно к ИСПДн;**
* **провести классификацию и сертификацию ИСПДн;**
* **провести организационно-режимные и технические мероприятия по обеспече-нию безопасности ПДн в ИСПДн;**
* **обеспечить необходимый уровень безопасности объектов защиты.**

Осуществление этих мероприятий обеспечит создание единой, целостной и скоорди-

нированной системы информационной безопасности ИСПДн и создаст условия для ее даль-нейшего совершенствования.

1. **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

Основными нормативно-правовыми и методическими документами, на которых бази-руется настоящая Концепция являются:

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 «Положение об обеспечении безопасности персональных данных при их обработке

* информационных системах персональных данных», утвержденное Постановлением Прави-тельства РФ от 17.11.2007 г. № 781.

3 «Порядок проведения классификации информационных систем персональных дан-ных», утвержденный совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Ми-нинформсвязи 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.

19

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

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

7 Рекомендации по обеспечению безопасности персональных данных при их обработ-ке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

8 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)

9 Базовая модель угроз безопасности персональных данных при их обработке в ин-формационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

10 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)

20