Приложение
к приказу заведующего МБДОУ
«ЦРР – д/с №34 «Рябинушка»
от 01.09.2016г. № 130/10

Отчет о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных, используемых в муниципальном бюджетном дошкольном образовательном учреждении «Центр развития ребенка – детский сад №34 «Рябинушка» муниципального образования город-курорт Геленджик

г-к Геленджик, 2016

Определения

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

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

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.

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

Доступ к информации – возможность получения информации и ее использования.

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

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

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

Информационная система персональных данных (ИСПДн) – 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.

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

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

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

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

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

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

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

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

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующими 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 и уничтожение персональных данных.

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

Оператор (персональных данных) – 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 и 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 записи ключей и атрибутов доступа (паролей) на бумажные носители 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, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и / или блокировать 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.

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

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

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео - и буквенно-цифровой информации), программные средства

(операционные системы, системы управления базами данных и т. п.), средства защиты информации, применяемые в информационных системах.

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

Трансграничная передача персональных данных – передача персональных данных 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.

Учреждение – Государственное образовательное учреждение города Москвы.

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).

1) 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
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю

Введение

Внутренняя проверка (далее – Проверка) произведена на основании приказа заведующего от 01.09.2016г. №_____

Проверка проводилась с 15.09.2016г. по 17.09.2016г. на территории МБДОУ «ЦРР – д/с №34 «Рябинушка» по адресу мкн. Парус, 21

В ходе проверки были выявлены следующие ИСПДн:

- **информационная система персональных данных работников;**
- **информационная система персональных данных воспитанников и их родителей.**

В ходе проверки для каждой ИСПДн определялось:

- состав и структура объектов защиты;
- конфигурация и структура ИСПДн;
- режим обработки ПДн;
- перечень лиц участвующих в обработке ПДн;
- права доступа лиц, допущенных к обработке ПДн;
- угрозы безопасности персональных данных. Оценивалась вероятность их реализации, реализуемость, опасность и актуальность;
- существующие меры защиты ПДн;
- список необходимых мер защиты ПДн.

Данные Проверки служат основой для других нормативно-организационных и распорядительных документов.

Данные о составе и структуре объектов защиты отражаются в Перечне персональных данных.

Данные о составе и структуре обрабатываемых персональных данных, конфигурации ИСПДн и режиме обработке являются основой для составления Акта классификации информационной системы персональных данных.

Данные о лицах, допущенных к обработке ПДн, и уровне их доступа отражаются в Положении о разграничении прав доступа к обрабатываемым персональным данным.

Данные о существующих и необходимых мерах защиты ПДн служат основной для составления Плана мероприятий по обеспечению защиты ПДн.

1. ИСПДн работников.

1.1. Структура ИСПДн

Таблица 1 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Автоматизированное рабочее место
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительная информация	К персональным данным предъявляется требование целостности и доступности

1.2. Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:

- ФИО;
- дата рождения;
- адрес прописки;
- адрес фактического проживания;
- паспортные данные;
- информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- телефонный номер (домашний, рабочий, мобильный);
- семейное положение и состав семьи (муж/жена, дети);
- данные о трудовом договоре (номер трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день,

обязанности работника, дополнительные социальные льготы и гарантии, номер и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);

- информация о приеме на работу, перемещении по должности, увольнении;
- информация о трудовой деятельности до приема на работу;
- информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- размер оклада;
- сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- данные об аттестации работников;
- данные о повышении квалификации;
- данные о наградах, медалях, поощрениях, почетных званиях;
- и другие данные.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **2 категории персональных данных,** т. е. к данным, позволяющим идентифицировать субъекта персональных данных и получить о нем дополнительную информацию.

Объем обрабатываемых персональных данных, **не превышает 1000 записей** о субъектах персональных данных.

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 01.01.01г. № 55/86/20, на основании категории и объема обрабатываемых персональных данных – **ИСПДн работников классифицируется, как ИСПДн класса К3.**

Так же в ИСПДн существуют следующие объекты защиты:

- технологическая информация:

§ управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

§ технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

§ информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

§ информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;

§ информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

§ служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки

Обрабатываемой информации.

- технические средства обработки:

§ общее программное обеспечение, участвующее в обработке ПДн (операционные системы, СУБД, клиент-серверные приложения и другие);

§ резервные копии общесистемного программного обеспечения;

§ инструментальные средства и утилиты систем управления ресурсами ИСПДн;

§ аппаратные средства обработки ПДн (АРМ и сервера);

§ сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т. п.).

- средства защиты ПДн:

§ средства управления и разграничения доступа пользователей;

§ средства обеспечения регистрации и учета действий с информацией;

§ средства, обеспечивающие целостность данных;

§ средства антивирусной защиты;

§ средства анализа защищенности;

§ средства обнаружения вторжений.

Каналы информационного обмена и телекоммуникации.

Объекты и помещения, в которых размещены компоненты ИСПДн.

1.3. Конфигурация ИСПДн

При составлении конфигурации используются следующие условные обозначения:

– Группа пользователей ИСПДн (операторы, администраторы).

– АРМ пользователей ИСПДн.

– Сервер баз данных.

– Направление информационного взаимодействия.

На рисунке 1 представлена конфигурация элементов ИСПДн работников.

Рисунок 1

Администраторы
Операторы

1.4. Структура обработки ПДн

В ИСПДн работников обработка персональных данных происходит следующим образом:

1) Пользователь (оператор, администратор) авторизуется на своем рабочем месте в ОС Windows 7.

2) Входит в ИСПДн работников.

3) Вносит необходимые данные на работника.

4) Сохраняет внесенные данные на работника.

3) Данные хранятся на сервере.

1.5. Режим обработки ПДн

В ИСПДн работников обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в таблице.

Таблица 2 – Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники
Администраторы ИСПДн	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.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Прибыткова А.А.
Администратор безопасности	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов	- сбор - систематизация - накопление - хранение - уточнение	Прибыткова А.А.

	ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	- использование - уничтожение	
Оператор ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Болтова В.И. Федоренко Н.Ф.

В ИСПДн работников осуществляют работу следующие сотрудники:

Таблица 3 – Перечень сотрудников

№	Роль	ФИО сотрудника	Подразделение
1.	Администратор ИСПДн	Прибыткова А.А.	ДОУ
2.	Администратор безопасности ИСПДн	Прибыткова А.А.	ДОУ
3.	Оператор	Федоренко Н.Ф.	ДОУ
4.	Оператор	Болтова В.И.	ДОУ
5.	Оператор	Иванова А.А.	ДОУ

1.6. Угрозы безопасности ПДн

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

- угрозы от утечки по техническим каналам:

§ Угрозы утечки акустической информации.

§ Угрозы утечки видовой информации.

§ Угрозы утечки информации по каналам ПЭМИН.

- Угрозы несанкционированного доступа к информации;

- Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн:

§ Кража ПЭВМ;

§ Кража носителей информации;

§ Кража ключей и атрибутов доступа;

§ Кражи, модификации, уничтожения информации;

§ Вывод из строя узлов ПЭВМ, каналов связи;

§ Несанкционированное отключение средств защиты.

- 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):

§ Действия вредоносных программ (вирусов);

§ Недекларированные возможности системного ПО и ПО для обработки персональных данных;

§ Установка ПО не связанного с исполнением служебных обязанностей.

- угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неатропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т. п.) характера:

§ утрата ключей и атрибутов доступа;

§ непреднамеренная модификация (уничтожение) информации сотрудниками;

§ непреднамеренное отключение средств защиты;

§ выход из строя аппаратно-программных средств;

§ сбой системы электроснабжения;

§ стихийное бедствие.

- угрозы преднамеренных действий внутренних нарушителей;

- доступ к информации, модификация, уничтожение, лицами, не допущенными к ее обработке;

- разглашение информации, модификация, уничтожение, сотрудниками допущенными к ее обработке;

- угрозы несанкционированного доступа по каналам связи:

§ Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

§ Перехват за переделами с контролируемой зоны;

§ Перехват в пределах контролируемой зоны внешними нарушителями;

§ Перехват в пределах контролируемой зоны внутренними нарушителями;

§ Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

§ Угрозы выявления паролей по сети;

§ Угрозы навязывание ложного маршрута сети;

§ Угрозы подмены доверенного объекта в сети;

§ Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

§ Угрозы типа «Отказ в обслуживании»;

§ Угрозы удаленного запуска приложений;

§ Угрозы внедрения по сети вредоносных программ;

1.7. Существующие меры защиты

Существующие в ИСПДн технические меры защиты представлены в таблице ниже.

Таблица 4 – Меры защиты

Элемент ИСПДн	Программное средство обработки ПДн	Установленные средства защиты
АРМ оператора	ОС Windows 7 Браузер	Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией. Антивирус *Kaspersky* - регистрацию и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.
АРМ администратора	ОС Windows 7 Клиент приложения	Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией. Антивирус *Kaspersky* - регистрацию и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.

Сервер		Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией; - обеспечение целостности данных. Антивирус *Kaspersky* - регистрацию и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.

В ИСПДн введены следующие организационные меры защиты:

- осуществляется контроль доступа в контролируемую зону, двери закрываются на замок;
- существует ответственный сотрудник за обеспечение безопасности ПДн – администратор безопасности;
- проводятся периодические внутренние проверки режима безопасности ПДн;
- введена парольная политика, устанавливающая сложность ключей и атрибутов доступа (паролей), а так же их периодическую смену;
- пользователи осведомлены и проинструктированы о порядке работы и защиты персональных данных;
- осуществляется резервное копирование защищаемой информации.

1.8. Необходимые меры защиты

Для достижения требуемого уровня защиты рекомендуется осуществить следующие мероприятия:

1. Организационные мероприятия:

· Первичная внутренняя проверка;

· Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц, не допущенных к обработке ПДн;

· Организация режима доступа в помещения, в которых установлены аппаратные средства ИСПДн;

· Организация порядка резервного копирования защищаемой информации на твердые носители;

· Организация порядка восстановления работоспособности технических средств, ПО, баз данных.

2. Физические мероприятия:

· Установка замков на дверях в помещениях с аппаратными средствами ИСПДн;

· Установка жалюзи на окнах (план ноябрь 2017г.);

· Установка систем кондиционирования в помещениях, где расположены аппаратные средства ИСПДн (план ноябрь 2017г.);

· Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн.

3. Технические (аппаратные и программные) мероприятия

· Внедрение единого хранилища зарегистрированных действий пользователей с ПДн;

· Внедрение межсетевого экранирования.

4. Контролирующие мероприятия

· Создание журнала внутренних проверок и поддержание его в актуальном состоянии;

· Контроль над соблюдением режима обработки ПДн;

· Контроль над соблюдением режима защиты;

· Контроль над выполнением антивирусной защиты;

· Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена;

· Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн;

· Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн;

· Контроль за обеспечением резервного копирования;

· Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз.

2. ИСПДн воспитанников и их родителей.

2.1. Структура ИСПДн

Таблица 5 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Автоматизированное рабочее место
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничением доступа

Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительная информация	К персональным данным предъявляется требование целостности и доступности

2.2. Состав и структура персональных данных

В ИСПДн воспитанников и их родителей обрабатываются следующие персональные данные:

Данные родителя (законного представителя):

· фамилия, имя, отчество;

· год рождения;

· месяц рождения;

· дата рождения;

· место рождения;

· адрес (регистрации и фактического проживания);

· паспортные данные;

· пол, гражданство;

· место работы;

- СНИЛС;

- номер лицевого счета;

- свидетельство о браке;

- свидетельство о расторжении брака;

- справки на льготу;

· номер контактного телефона.

Данные о детях:

· фамилия, имя, отчество;

· год рождения;

· месяц рождения;

· дата рождения;

· место рождения;

· адрес (регистрации и фактического проживания);

· национальность;

· пол, гражданство;

· СНИЛС;

- медицинский полис;

- справка об инвалидности (при наличии);

- выписка ПМПК (при наличии);

- медицинская карта;

- справки о состоянии здоровья.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **2 категории персональных данных,** т. е. к данным, позволяющим идентифицировать субъекта персональных данных и получить о нем дополнительную информацию.

Объем обрабатываемых персональных данных, **от 1000 до 100 000 записей** о субъектах персональных данных.

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 01.01.01 г. № 55/86/20, на основании категории и объема обрабатываемых персональных данных – **ИСПДн воспитанников и их родителей классифицируется, как ИСПДн класса К2.**

Так же в ИСПДн существуют следующие объекты защиты:

- технологическая информация:

§ управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

§ технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

§ информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

§ информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;

§ информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

§ служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

- технические средства обработки:

§ общее программное обеспечение, участвующее в обработке ПДн (операционные системы, СУБД, клиент-серверные приложения и другие);

§ резервные копии общесистемного программного обеспечения;

§ инструментальные средства и утилиты систем управления ресурсами ИСПДн;

§ аппаратные средства обработки ПДн (АРМ и сервера);

§ сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т. п.).

- средства защиты ПДн:

§ средства управления и разграничения доступа пользователей;

§ средства обеспечения регистрации и учета действий с информацией;

§ средства, обеспечивающие целостность данных;

§ средства антивирусной защиты;

§ средства анализа защищенности;

§ средства обнаружения вторжений.

Каналы информационного обмена и телекоммуникации.

Объекты и помещения, в которых размещены компоненты ИСПДн.

2.3. Конфигурация ИСПДн

При составлении конфигурации используются следующие условные обозначения:

– Группа пользователей ИСПДн (операторы, администраторы).

– АРМ пользователей ИСПДн.

– Сервер баз данных.

– Направление информационного взаимодействия.

На рисунке 3 представлена конфигурация элементов ИСПДн воспитанников и их родителей.

Рисунок 3

Администраторы
Операторы

2.4. Структура обработки ПДн

В ИСПДн воспитанников и их родителей обработка персональных данных происходит следующим образом:

1) Пользователь (оператор, администратор) авторизуется на своем рабочем месте в ОС Windows 7.

2) Входит в ИСПДн воспитанников и их родителей (законных представителей).

3) Вносит необходимые данные.

4) Сохраняет внесенные данные.

3) Данные хранятся на сервере.

2.4. Режим обработки ПДн

В ИСПДн воспитанников обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в таблице.

Таблица 6 – Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники
Администраторы ИСПДн	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.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Прибыткова А.А.
Администратор безопасности	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Прибыткова А.А.

	(инспекционных).		
Оператор ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Болтова В.И. Федоренко Н.Ф.
Пользователи ИСПДН	Обладает правом доступа к ПДн воспитанников.	- сбор - накопление - хранение - уточнение - использование	Иванова А.А.

В ИСПДн осуществляют работу следующие сотрудники:

Таблица 7 – Перечень сотрудников

№	Роль	ФИО сотрудника	Подразделение
1.	Администратор ИСПДн	Прибыткова А.А.	ДОУ
2.	Администратор безопасности ИСПДн	Прибыткова А.А.	ДОУ

5.	Оператор	Федоренко Н.Ф.	ДОУ
6.	Пользователи	Иванова А.А.	ДОУ

2.5. Угрозы безопасности ПДн

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

- угрозы от утечки по техническим каналам:

§ Угрозы утечки акустической информации.

§ Угрозы утечки видовой информации.

§ Угрозы утечки информации по каналам ПЭМИН.

- Угрозы несанкционированного доступа к информации;

- Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн:

§ Кража ПЭВМ;

§ Кража носителей информации;

§ Кража ключей и атрибутов доступа;

§ Кражи, модификации, уничтожения информации;

§ Вывод из строя узлов ПЭВМ, каналов связи;

§ Несанкционированное отключение средств защиты.

- 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):

§ Действия вредоносных программ (вирусов);

§ Недекларированные возможности системного ПО и ПО для обработки персональных данных;

§ Установка ПО не связанного с исполнением служебных обязанностей.

- угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неатропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т. п.) характера:

§ утрата ключей и атрибутов доступа;

§ непреднамеренная модификация (уничтожение) информации сотрудниками;

§ непреднамеренное отключение средств защиты;

§ выход из строя аппаратно-программных средств;

§ сбой системы электроснабжения;

§ стихийное бедствие.

- угрозы преднамеренных действий внутренних нарушителей;

- доступ к информации, модификация, уничтожение, лицами, не допущенными к ее обработке;

- разглашение информации, модификация, уничтожение, сотрудниками допущенными к ее обработке;

- угрозы несанкционированного доступа по каналам связи:

§ Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

§ Перехват за переделами с контролируемой зоны;

§ Перехват в пределах контролируемой зоны внешними нарушителями;

§ Перехват в пределах контролируемой зоны внутренними нарушителями;

§ Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

§ Угрозы выявления паролей по сети;

§ Угрозы навязывание ложного маршрута сети;

§ Угрозы подмены доверенного объекта в сети;

§ Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

§ Угрозы типа «Отказ в обслуживании»;

§ Угрозы удаленного запуска приложений;

§ Угрозы внедрения по сети вредоносных программ;

2.6. Существующие меры защиты

Существующие в ИСПДн технические меры защиты представлены в таблице ниже.

Таблица 8 – Меры защиты

Элемент ИСПДн	Программное средство обработки ПДн	Установленные средства защиты
АРМ оператора	ОС Windows 7 Браузер	Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией. Антивирус *Kaspersky* - регистрацию и учет действий с информацией;

		- обеспечение целостности данных; - обнаружение вторжений.
АРМ администратора	ОС Windows 7 Клиент приложения	Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией. Антивирус *Kaspersky* - регистрацию и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.
АРМ пользователя	ОС Windows 7 Браузер	Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией. Антивирус *Kaspersky* - регистрацию и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.
Сервер		Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией; - обеспечение целостности данных. Антивирус *Kaspersky* - регистрацию и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.

В ИСПДн введены следующие организационные меры защиты:

- осуществляется контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания;
- существует ответственный сотрудник за обеспечение безопасности ПДн – администратор безопасности;
- проводятся периодические внутренние проверки режима безопасности ПДн;
- введена парольная политика, устанавливающая сложность ключей и атрибутов доступа (паролей), а так же их периодическую смену;

- пользователи осведомлены и проинструктированы о порядке работы и защиты персональных данных;
- осуществляется резервное копирование защищаемой информации;
- в помещениях, где расположены элементы ИСПДн, установлена пожарная сигнализация.

2.7. Необходимые меры защиты

Для достижения требуемого уровня защиты рекомендуется осуществить следующие мероприятия:

1. Организационные мероприятия:

· Первичная внутренняя проверка;

· Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц, не допущенных к обработке ПДн;

· Организация режима и контроля доступа в помещения, в которых установлены аппаратные средства ИСПДн;

· Организация порядка резервного копирования защищаемой информации на твердые носители;

· Организация порядка восстановления работоспособности технических средств, ПО, баз данных.

2. Физические мероприятия:

· Установка замков на дверях в помещениях с аппаратными средствами ИСПДн;

· Установка жалюзи на окнах;

· Установка систем кондиционирования в помещениях, где расположены аппаратные средства ИСПДн;

· Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн.

3. Технические (аппаратные и программные) мероприятия

· Внедрение единого хранилища зарегистрированных действий пользователей с ПДн;

· Внедрение межсетевого экранирования.

4. Контролирующие мероприятия

· Создание журнала внутренних проверок и поддержание его в актуальном состоянии;

· Контроль над соблюдением режима обработки ПДн;

· Контроль над соблюдением режима защиты;

· Контроль над выполнением антивирусной защиты;

· Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена;

· Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн;

· Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн;

· Контроль за обеспечением резервного копирования;

· Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз.