**УТВЕРЖДАЮ:**
директор детского дома
_____ Ю.Г. Коровкин
«_21_» _мая_ 20_17_ г

**ЗАКЛЮЧЕНИЕ**
**о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных, используемых в государственном казенном учреждении для детей-сирот и детей, оставшихся без попечения родителей, «Детский дом (смешанный) № 30»**

г. Георгиевск 20.05.2017г

В настоящем заключении используются следующие термины и их определения.

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

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

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

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

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

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

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

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

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

Доступ к информации – возможность получения информации и ее использования.

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

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

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

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

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

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

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

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

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

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс),

реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

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

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

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

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

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

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

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

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.

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

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

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

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

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

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

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, 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, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

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

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

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

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 пер-сональных 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 – учреждения здравоохранения, социальной сферы, труда и занятости. Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

## ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства
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
ТКУ И – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

В соответствии с приказом директора ГКУ «Детский дом (смешанный) № 30» (далее – детский дом) от 20.04.2017г № 17/1-од «О проведении плановой внутренней проверки соответствия обработки персональных данных требованиям к защите персональных данных» комиссией детского дома в составе:

| | |
|---|---|
| председатель комиссии: | Демчук И.В., председатель профсоюзного комитета; |
| члены комиссии: | Сапрыкина Ж.М., медицинская сестра по питанию; |
| | Пакулева Е.Н., заведующий библиотекой, |
| | Иваненко Е.Н., педагог дополнительного образования |

в период с 20.04.2017 года по 20.05.2017 года была проведена плановая внутренняя проверка соответствия обработки персональных данных требованиям к защите персональных данных (далее - проверка). Проверка проводилась на территории детского дома, по адресу г. Георгиевск, ул. Воровского, д.2.

Проверка проводилась в соответствии со следующими законодательными, нормативными и методическими актами:
- Федеральный закон N 152-ФЗ от 27 июля 2006 года "О персональных данных" (далее – Федеральный закон "О персональных данных");
- Федеральный закон от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Постановление Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных детского дома, утв. приказом детского дома от 28.02.2017г № 9/1-од.

В ходе проведения проверки решались следующие задачи:

- определение перечня информационных систем, осуществляющих обработку персональных данных в детском доме;
- определение границ информационных систем персональных данных;
- установление мест и форматов хранения персональных данных;
- проведение изучения существующего порядка обработки и защиты персональных данных в информационных системах персональных данных;
- составление перечня персональных данных, обрабатываемых в информационных системах персональных данных в детском доме;
- оценка степени участия сотрудников в обработке персональных данных;
- определения перечня используемого оборудования и ПО;

- определение состава используемых средств защиты персональных данных;
- установление способов обработки персональных данных;
- выявление нарушений требований к защите персональных данных.

В ходе проверки для каждой информационной системы персональных данных определялось:

- состав и структура объектов защиты;
- конфигурация и структура информационной системы;
- режим обработки информационной системы;
- перечень лиц, участвующих в обработке персональных данных;
- права доступа лиц, допущенных к обработке персональных данных;
- существующие меры защиты персональных данных;
- необходимые меры защиты персональных данных.

Данные Проверки служат информационной основой для других нормативно-организационных документов. Данные о составе и структуре объектов защиты отражаются в Перечне персональных данных, подлежащих защите. 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 об угрозах безопасности ПДн служат основной для составления Модели угроз безопасности персональных данных. Данные о существующих и необходимых мерах защиты ПДн служат основной для составления Плана мероприятий по обеспечению защиты ПДн.

## Описание структуры ИСПДн

| | |
|---|---|
| Заданные характеристики безопасности персональных данных | Типовая информационная система |
| Структура информационной системы | Автоматизированное рабочее место |
| Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена | Отсутствует (автономная система) |
| Режим обработки персональных данных | Многопользовательская система |
| Режим разграничения прав доступа пользователей | Система с разграничение доступа |
| Местонахождение технических средств информационной системы | Все технические средства находятся в пределах Российской Федерации |

## Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:

| 1. Персональные данные работников детского дома | 2. Персональные данные воспитанников детского дома |
|---|---|
| - анкетные и биографические данные;<br>- образование;<br>- сведения о трудовом и общем стаже;<br>- сведения о составе семьи;<br>- паспортные данные;<br>- сведения о воинском учете;<br>- сведения о заработной плате сотрудника;<br>- сведения о социальных льготах;<br>- специальность;<br>- наличие судимостей;<br>- адрес места жительства;<br>- домашний и мобильный телефон;<br>- место работы или учебы членов семьи и родственников;<br>- содержание трудового договора;<br>- состав декларируемых сведений о наличии материальных ценностей;<br>- содержание декларации, подаваемой в налоговую инспекцию;<br>- подлинники и копии приказов по личному составу;<br>- личные дела и трудовые книжки сотрудников;<br>- основания к приказам по личному составу;<br>- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям. | - анкетные и биографические данные;<br>- место учебы;<br>- сведения о родителях (попечителях), опекунах;<br>- паспортные данные, данные свидетельства о рождении;<br>- сведения о ближайших родственниках (братья, сестры и др.);<br>- медицинские сведения;<br>- наличие судимостей;<br>- личные дела воспитанников;<br>- основания к приказам по личному составу;<br>- алфавитная книга воспитанников. |

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к 3 и 4 категориям персональных данных. Объем обрабатываемых персональных данных составляет данные менее чем 1000 субъектов персональных данных. В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, на основании категории и объема обрабатываемых персональных данных – информационная система обработки персональных данных детского дома классифицируется как ИСПДн класса К3.

Так же в ИСПДн существуют следующие объекты защиты:

1) 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 об 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.

2). Программно-технические средства обработки:
- общесистемное 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);
- сетевое оборудование (маршрутизаторы).

3). Средства защиты ПДн:
- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты.

4). Каналы информационного обмена и телекоммуникации.

5). Объекты и помещения, в которых размещены компоненты ИСПДн.

## Режим обработки ПДн

В ИСПДн 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 ролей представлен в виде матрицы доступа в таблице:

| **Наименование источника информации, содержащий** | **Разрешенные действия** | **Должность ответственного за организацию обработки** |
|---|---|---|

| **персональные данные** | | **персональных данных работников и воспитанников детского дома (администратор)** |
|---|---|---|
| Подлинники приказов по личному составу работников | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Зам. директора по АХЧ, зам. директора по УВР |
| Основания к приказам по личному составу работников | | Зам. директора по АХЧ |
| Трудовые книжки работников | | Зам. директора по АХЧ, отв. за ведение трудовых книжек |
| Личные дела (карточки) работников | | Зам. директора по АХЧ, зам. директора по УВР |
| Медицинские книжки работников | | Старшая мед. сестра |
| Сведения о воинском учете работников | | Зам. директора по АХЧ, зам. директора по УВР |
| Сведения о заработной плате работников | | Главный бухгалтер, бухгалтер |
| Подлинники (копии) договоров гражданско-правового характера | | Бухгалтер, Юрисконсульт, специалист по закупкам, зам. директора по АХЧ., зав. складом |
| Материалы по служебным расследованиям работников | | Зам. директора по АХЧ, зам. директора по УВР |
| Медицинские сведения воспитанников | | Врач, мед. сестра, социальный педагог |
| Личные дела воспитанников | | социальный педагог |
| Личные дела выпускников из числа воспитанников | | социальный педагог |
| Подлинники приказов по личному составу воспитанников | | Секретарь руководителя |
| Основания к приказам по личному составу воспитанников | | Секретарь руководителя |
| Материалы временной передачи воспитанников в семьи граждан РФ | | Зам. директора по УВР, социальный педагог |
| Алфавитная книга воспитанников | | социальный педагог |
| Материалы психолого-педагогической диагностики воспитанников | | Педагоги-психологи |
| Материалы, касающиеся персональных данных слушателей Школы приемных родителей | | Педагоги-психологи |
| Материалы, касающиеся | | Педагоги-психологи, |

| | | |
|---|---|---|
| персональных данных сопровождаемых Службой сопровождения замещающих семей | | ответственные за работу Службы |
| Материалы, касающиеся персональных данных выпускников из числа воспитанников детского дома, сопровождаемых Клубом выпускников | | ответственный за работу Клуба, воспитатели групп |

**Угрозы безопасности ПДн**

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

1. Угрозы от утечки по техническим каналам:
1.1. Угрозы утечки акустической информации.
1.2. Угрозы утечки видовой информации.
2. Угрозы несанкционированного доступа к информации.
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.
2.1.1. Кража ПЭВМ;
2.1.2. Кража носителей информации;
2.1.3. Кража ключей и атрибутов доступа;
2.1.4. Кражи, модификации, уничтожения информации;
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи;
2.1.6. Несанкционированное отключение средств защиты.
2.2. 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).
2.2.1. Действия вредоносных программ (вирусов);
2.2.2. Установка ПО не связанного с исполнением служебных обязанностей.
3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.
3.1. Утрата ключей и атрибутов доступа;
3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками;
3.3. Непреднамеренное отключение средств защиты;
3.4. Выход из строя аппаратно-программных средств;
3.5. Сбой системы электроснабжения;
3.6. Стихийное бедствие.
4. Угрозы преднамеренных действий внутренних нарушителей.
4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;

4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.

**Существующие меры защиты.**

Существующие в ИСПДн технические меры защиты представлены в таблице ниже.

| Элемент ИСПДн | Программное средство обработки ПДн | Установленные средства защиты |
|---|---|---|
| АРМ администратора | ОС Windows XP, Windows 7 | Средства ОС:<br>- управление и разграничение доступа пользователей;<br>- регистрация и учет действий с информацией. |
| | Антивирус | - регистрация и учет действий с информацией;<br>- обеспечение целостности данных;<br>- обнаружение вторжений. |

В ИСПДн введены следующие организационные меры защиты:

Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа работниками детского дома к источникам информации, содержащей персональные данные субъектов;
- воспитательная и разъяснительная работа с сотрудниками детского дома по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- запрет выдачи документов, содержащих персональные данные субъектов на рабочие места сотрудников. В исключительных случаях данные документы могут выдаваться на рабочие места работникам с разрешения администрации детского дома.

Для обеспечения внешней защиты персональных данных работников и воспитанников используются следующие организационные и технические мероприятия:

- назначение ответственного за организацию защиты персональных данных;
- установление порядка приема, учета и контроля деятельности посетителей;
- пропускной режим;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях;
- разграничение прав доступа сотрудников к базе персональных данных;
- наличие необходимой нормативной базы документов, определяющих политику в отношении обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации;
- осуществление учета носителей информации, наличие и использование средств обеспечения безопасности: сейф, шкаф (запирающийся на ключ) для хранения носителей информации с персональными данными;
- организация процесса резервного копирования и архивирования информации;
- наличие установленного антивирусного программного обеспечения и др.

**Выводы и предложения.**

В результате проведенной проверки комиссия детского дома не установила нарушения требований к защите персональных данных.

Учитывая вышеизложенное, комиссия рекомендует в дальнейшем:
- проводить мероприятия, направленные на предотвращение несанкционированного доступа (далее НСД) к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременно обнаруживать факты НСД к персональным данным;
- не допускать воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- незамедлительно восстанавливать ПДн, модифицированные или уничтоженные вследствие несанкционированного доступа к ним; осуществлять постоянный контроль за обеспечением уровня защищенности ПДн.

20 мая 2017 года

Председатель комиссии:  И.В. Демчук