УТВЕРЖДАЮ:
Заведующий
МБДОУ «Детский сад «Колосок»
г. Заозерного»
_____ Е.Л. Новикова

# МОДЕЛЬ
# УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ МБДОУ «ДЕТСКИЙ САД «КОЛОСОК» Г.ЗАОЗЕРНОГО»

АВС - антивирусные средства;
АПКШ - аппаратно-программный комплекс шифрования;
АРМ - автоматизированное рабочие место;
АС - автоматизированная система;
ВТСС - вспомогательные технические средства и системы;
ЗИ - защита информации;
ИБ - информационная безопасность;
ИС - информационная система;
ИСПДн - информационная система персональных данных;
ИТ - информационные технологии;
КЗ - контролируемая зона;
МНИ - магнитные носители информации;
МСЭ - межсетевой экран;
НСД - несанкционированный доступ;
ОС - Операционная система;
ОТСС - основные технические средства и системы;
ПАК - программно-аппаратный комплекс;
ПДн - персональные данные;
ПО - программное обеспечение;
РД - руководящие документы;
РФ - Российская Федерация;
СВТ - средства вычислительной техники;
СЗИ - средства защиты информации;
ТКУИ - технические каналы утечки информации;
ФЗ - Федеральный закон;
ФСБ - Федеральная служба безопасности;
ФСТЭК - Федеральная служба по техническому и экспортному контролю.

## 1. ТЕРМИНЫ Т ОПРЕДЕЛНИЯ

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.

Базовые угрозы информационной безопасности - нарушение конфиденциальности, нарушение целостности и отказ в обслуживании;

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

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

Доступ к информации - возможность получения информации и ее использования.

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.

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.

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 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.

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 ис-пользованием 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.

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.

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

Ресурс - любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер). Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса.

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.

Угроза - действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

Уязвимость - это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость.

## 2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая "Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных МБДОУ «Детский сад «Колосок» г. Заозерного»" (далее - Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которое ведет к ущербу жизненно важных интересов личности, общества и государства.

Данная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных МБДОУ «Детский сад «Колосок» г. Заозерного» разработана на основании:

1) «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной 15 февраля 2008 г. заместителем директора ФСТЭК России;

2) «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России;

3) ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения».

Модель определяет угрозы безопасности персональных данных, обрабатываемых в информационной системе персональных данных МБДОУ «Детский сад «Колосок» г. Заозерного».

# 3 УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 3.1.Угрозы несанкционированного доступа к информации

3.1.1. *Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн*

3.1.1.1. Кража ПЭВМ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В здании МБДОУ «Детский сад «Колосок» г. Заозерного»» ведется круглосуточный контроль доступа в контролируемую зону, который осуществляется сторожем, двери закрываются на замок, вынос компьютерный техники за пределы здания возможен только с разрешения охраны.

Вероятность реализации угрозы - маловероятна.

3.1.1.2. Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации. Журнал

В здании МБДОУ «Детский сад «Колосок» г. Заозерного» введен контроль доступа в контролируемую зону, двери закрываются на замок, хранение носителей информации осуществляет ответственный, разработан журнал учета машинных носителей (Приложение 1), разработан журнал учета лиц СПДн (Приложение 2)

Вероятность реализации угрозы - маловероятна.

3.1.1.3. Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В здании МБДОУ «Детский сад «Колосок» г. Заозерного» введен контроль доступа в контролируемую зону, двери закрываются на замок, организовано хранение ключей и паролей у ответственного .

Вероятность реализации угрозы - маловероятна.

3.1.1.4. Кража, модификация, уничтожение информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В здании МБДОУ «Детский сад «Колосок» г. Заозерного» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы - маловероятна.

3.1.1.5. Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В здании МБДОУ «Детский сад «Колосок» г. Заозерного» введен контроль доступа в контролируемую зону, двери закрываются на замок

Вероятность реализации угрозы - маловероятна.

3.1.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ

В Учреждении техническое обслуживание ПЭВМ осуществляется сотрудниками, подписавшими соглашение о неразглашении.

Вероятность реализации угрозы - маловероятна.

3.1.1.7. Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

В здании МБДОУ «Детский сад «Колосок» г. Заозерного» введен контроль доступа в контролируемую зону, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн.(Приложение 3)

Вероятность реализации угрозы - низкая вероятность.

3.2.2. *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*

3.2.2.1. Действия вредоносных программ (вирусов)

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять такие функции как:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

На АРМ установлено антивирусное программное обеспечение, персонал проинструктирован об антивирусной защите (Приложение 4).

Вероятность реализации угрозы - низкая.

3.2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных.

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.

Вероятность реализации угрозы - маловероятна.

3.2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Вероятность реализации угрозы - высокая вероятность.

3.2.3. *Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п) характера*

3.2.3.1. Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В Учреждении введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы - низкая вероятность.

3.2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

В учреждении осуществляется резервное копирование обрабатываемых ПДн. Пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы - низкая вероятность.

3.2.3.3. Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, пользователи проинструктированы о работе с ИСПДн, разграничение доступа к настройкам режимов средств защиты не осуществляется.

Вероятность реализации угрозы - средняя вероятность.

3.2.3.4. Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В учреждении осуществляется резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы - маловероятна.

3.2.3.5. Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В учреждении осуществляется резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы - низкая вероятность.

3.2.3.6. Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы - маловероятна.

### 3.2. Угрозы преднамеренных действий внутренних нарушителей

3.2.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В здании МБДОУ «Детский сад «Колосок» г.Заозерного» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы - маловероятна.

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

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В учреждении пользователи осведомлены о порядке работы с персональными данными (приложение 5), а также подписали Соглашение о неразглашении.

Вероятность реализации угрозы - низкая вероятность.

### 3.3. Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (Базовая модель угроз безопасности персональных данных при их обработке в информационных системах

персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
- 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 навязывания ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта в ИСПДн и во внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

3.3.1. Угроза «Анализ сетевого траффика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

- изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;
- перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

В ИСПДн МБДОУ «Детский сад «Колосок» г.Заозерного» осуществляется передача информации по каналам связи с использованием криптошлюза.

Вероятность реализации угрозы - маловероятна.

3.3.2. Угроза «сканирование сети»

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза.

Вероятность реализации угрозы - маловероятна.

3.3.3. Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза.

Вероятность реализации угрозы - маловероятна.

3.3.4. Угрозы навязывания ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена

недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза.

Вероятность реализации угрозы - маловероятна.

3.3.5. Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза.

Вероятность реализации угрозы - маловероятна.

3.3.6. Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность пере-хвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом- жертвой, будет проходить через ложный объект сети.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза.

Вероятность реализации угрозы - маловероятна.

3.3.7. Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресур-сов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP- соединений (SYN-flooding), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания

каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому сер-веру (Spam);

- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;
- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза, установлена антивирусная защита.

Вероятность реализации угрозы - маловероятно.

3.3.8. Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений - серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза, установлена антивирусная защита.

Вероятность реализации угрозы - маловероятно.

3.3.9. Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
- программы, демонстрирующие уязвимости средств защиты информации;
- программы-генераторы компьютерных вирусов и др.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза, установлена антивирусная защита.

Вероятность реализации угрозы - маловероятно.

## 4. Определение актуальных угроз безопасности

Потенциальную опасность для персональных данных (далее - ПДн) при их обработке в ИСПДн представляют:

- угрозы несанкционированного доступа;
- угрозы персонала.
- угрозы утечки информации по техническим каналам;
- физические угрозы.

## 5. Определение уровня исходной защищенности ИСПДн

Уровень исходной защищенности ИСПДн определен экспертным методом в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (далее - Методика), утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России.

| Технические и эксплуатационные характеристики ИСПДн | Уровень защищенности | | |
|---|---|---|---|
| | Высокий | Средний | Низкий |
| 1. По территориальному размещению | | | |
| Локальная ИСПДн, развернутая в пределах одного здания | | | |
| 2. По наличию соединения с сетями общего пользования | | | |
| ИСПДн, имеющая одноточечный выход в сеть общего пользования | | | |
| 3. По встроенным (легальным) операциям с записями баз ПДн | | | |
| Модификация, передача | | | |
| 4. По разграничению доступа к ПДн | | | |

| | | | |
|---|---|---|---|
| ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн | | | |
| 5. По наличию соединений с другими базами ПДн иных ИСПДн | | | |
| ИСПДн, в которой используется одна база персональных данных, принадлежащая организации - владельцу данной ИСПДн | | | |
| 6. По уровню обобщения (обезличивания) ПДн | | | |
| ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации | | | |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | | | |
| ИСПДн, не предоставляющая никакой информации | | | |
| Характеристики ИСПДн | | | |

## 6. Расчет рисков важных объектов защиты

Расчет рисков важных объектов защиты МБДОУ «Детский сад «Колосок» г.Заозерного» был выполнен на основе документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК.

### 6.1. Вероятность реализации угроз безопасности персональных данных

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);
- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2= 5);
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

### 6.2. Реализуемость угроз

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20

| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность реализации |
|---|---|---|
| 1 | 2 | 3 |
| 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 | | |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | | |
| Несанкционированное отключение средств защиты | | |
| Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программноаппаратных 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 неантропогенного (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 аппаратнопрограммных средств | | |
| Сбой системы электроснабжения | | |
| Стихийное бедствие | | |
| Угрозы преднамеренных действий внутренних нарушителей | | |
| Доступ к информации, модификация, уничтожение лиц не допущенных 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 | | |
| 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 | | |

7. Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

| Тип угроз безопасности ПДн | Опасность угрозы |
|---|---|
| 1 | 2 |
| 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 | |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | |
| Несанкционированное отключение средств защиты | |
| Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программноаппаратных 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 неантропогенного (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 | |
| 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 лиц не допущенных 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: | |
| 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 | |

8. Определение актуальности угроз

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

| Возможность реализации угрозы | Показатель опасности угрозы | | |
|---|---|---|---|
| | Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Оценка актуальности угроз безопасности.

| Тип угроз безопасности ПДн | Актуальность угрозы |
|---|---|
| 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 | |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | |
| Несанкционированное отключение средств защиты | |
| Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программноаппаратных 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 неантропогенного (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 лиц не допущенных 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 | |
| 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 | |

Приложение 4
к модели угроз безопасности персональных данных
при их обработке в информационных системах персональных данных
МБДОУ «Детский сад «Колосок» г.Заозерного»

# ИНСТРУКЦИЯ
# ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

УСЛОВНЫЕ СОКРАЩЕНИЯ**:**
АВЗ - антивирусная защита;
ИСПДн - информационная система персональных данных;
ПДн - персональные данные;
ИС - информационная система;
АРМ - автоматизированное рабочее место;
ПО - программное обеспечение

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция предназначена для Ответственного за организацию обработки персональных данных, и пользователей, эксплуатирующих автоматизированную информационную систему(далее - ИС).
1.2. Инструкция устанавливает требования и ответственность пользователей ИС при организации защиты персональных данных от воздействия вредоносного программного обеспечения.
1.3. Инструкция регулирует как вопросы организации антивирусной защиты, так и требования к порядку проведения антивирусного контроля при работе в ИС

## 2. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ АНТИВИРУСНОЙ ЗАЩИТЫ

2.1. Требования к порядку организации антивирусной защиты

2.1.1. Для организации антивирусной защиты ИС допускаются к использованию только лицензионные антивирусные средства общего применения, прошедшие в установленном порядке процедуру проверки соответствия требованиям по защите информации (сертифицированные).

2.1.2. Приобретение и установка (обновление) антивирусных программных средств осуществляется в установленном порядке с учётом требований настоящей Инструкции.

2.1.3. Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется Ответственным за организацию обработки персональных данных с привлечением (при необходимости) специалистов лицензированной организации.

2.1.4. Обновление антивирусного программного обеспечения (при необходимости) и антивирусных баз на АРМ и серверах, входящих в состав ИС, должно производиться не реже одного раза в месяц. Ответственным за настройку, своевременное обновление антивирусного программного обеспечения и антивирусных баз Ответственный за организацию обработки персональных данных и пользователей.

2.1.5. Должностные лица не должны допускать использования в ИС программного обеспечения (ПО) и данных, не связанных с выполнением должностных обязанностей.

2.2.1. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вредоносного ПО. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка в присутствии и под контролем Ответственного за организацию обработки ПДн или сотрудника, им уполномоченного.

2.2.2. При загрузке компьютера должен проводиться антивирусный контроль в автоматическом режиме. Порядок и периодичность расширенного антивирусного контроля и других необходимых антивирусных проверок определяется на этапе планирования мероприятий установленным порядком (не реже одного раза в месяц и при необходимости, в случае появления подозрений в заражении вредоносным ПО).

2.2.3. Ежемесячно должна проводиться полная антивирусная проверка

2.2.4. В случае обнаружения вирусной активности или её признаков, пользователь должен оповестить ответственного за организацию обработки персональных данных.

2.2.5. Обязательному дополнительному антивирусному контролю подлежит любая информация на съёмных машинных носителях информации, поступающая для обработки в ИС. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель информации).

2.2.6. При возникновении подозрения на наличие вредоносного ПО (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Ответственный за организацию обработки персональных данных, или пользователь должен провести внеочередной антивирусный контроль своей рабочей станции для определения ими факта наличия или отсутствия вредоносного ПО.

2.2.7. В случае обнаружения при проведении антивирусной проверки заражённых вредоносным ПО файлов пользователи ИС обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения заражённых вредоносным ПО файлов руководителя, Ответственного за организацию обработки персональных данных, владельца заражённых файлов, а также других пользователей, использующих эти файлы в работе;
- совместно с владельцем заражённых вредоносным ПО файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение заражённых файлов;
- в случае обнаружения нового вредоносного ПО, не поддающегося лечению применяемыми антивирусными средствами, направить заражённый вредоносным ПО файл на съёмном носителе Ответственному за организацию обработки персональных данных для дальнейшей антивирусной поддержки;

по факту обнаружения заражённых вредоносным ПО файлам составить служебную записку Ответственному за организацию обработки персональных данных, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) заражённого файла, тип заражённого файла, характер содержащейся в файле информации, тип вредоносного ПО (если известен) и выполненные антивирусные мероприятия.

## 3. ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

3.1. Ответственность за организацию антивирусной защиты ИС и установление порядка её проведения, в соответствии с требованиями настоящей Инструкции, возлагается на Ответственного за организацию обработки персональных данных.

3.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на Ответственного за организацию обработки ПДн и пользователей (операторов) ИС.

Приложение 1
к модели угроз безопасности персональных данных
при их обработке в информационных системах персональных данных
МБДОУ «Детский сад «Колосок» г.Заозерного»

**ЖУРНАЛ**
**УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ**
**МБДОУ «Детский сад «Колосок» г. Заозерного»**
**663960,Красноярскмй край, Рыбинский район, г. Заозерный, ул. Советская, 17**

| № п/п | Дата учета | Наименование носителя | Инвентарный номер | Местонахождение носитителя | Наименование хранилища | ФИО ответственного за сейф,шкаф | дата, подпись ответственного |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Приложение 2
к модели угроз безопасности персональных данных
при их обработке в информационных системах персональных данных
МБДОУ «Детский сад «Колосок» г.Заозерного»

**ЖУРНАЛ**
**УЧЕТА ЛИЦ ИСПНДн**
**МБДОУ «Детский сад «Колосок» г. Заозерного»**
**663960,Красноярскмй край, Рыбинский район, г. Заозерный, ул. Советская, 17**

| № п/п | Сведения о допуске к персональным данным | | | Сведения о прекращении допуска к персональным данным | | |
|---|---|---|---|---|---|---|
| | Наименование ИСПДн | Основание предоставления допуска | Дата, Ф.И.О. и подпись допускаемого лица | Основание прекращения допуска к ИСПДн | Приказ об увольнении/ переводе | Дата, Ф.И.О. и подпись лица об ознакомлении с документом |
| | СБИС | Должностные обязанности | | | | |

Приложение 5
к модели угроз безопасности персональных данных
при их обработке в информационных системах персональных данных
МБДОУ «Детский сад «Колосок» г.Заозерного»

**Положение об обработке персональных данных**
**МБДОУ «Детский сад «Колосок» г. Заозерного»**

Общие положения

Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников учреждения. Под работниками подразумеваются лица, заключившие трудовой договор с МБДОУ «Детский сад «Колосок» г. Заозерного» (далее МБДОУ).

Цель Положения - защита персональных данных работников учреждения от несанкционированного доступа и разглашения. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

Основанием для разработки настоящего Положения являются Конституция РФ, Трудовой кодекс РФ, другие действующие нормативно-правовые акты РФ.

Положение и изменения к нему утверждаются заведующей МБДОУ и вводятся приказом по учреждению. Все работники учреждения должны быть ознакомлены под расписку с данным Положением и изменениями к нему.

Понятие и состав персональных данных

Под персональными данными работников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

Состав персональных данных работника:

- анкета;
- автобиография;
- образование;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- размер заработной платы;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и пере-подготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

- фотографии и иные сведения, относящиеся к ПДн работника;
- рекомендации, характеристики и т.п.

Данные документы являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

## Обязанности работодателя

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ и иными федеральными законами.

Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на ПДн работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

Работники не должны отказываться от своих прав на сохранение и защиту тайны.

## Обязанности работника

Работник обязан:

- передавать работодателю или его представителю комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом РФ;
- своевременно в разумный срок, не превышающий 5 дней, сообщать работодателю об изменении своих персональных данных.

## Права работника

Работник имеет право:

- на полную информацию о своих ПДн и обработке этих данных.

- на свободный бесплатный доступ к своим персональным данным, вклю-чая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством РФ.
- на доступ к медицинским данным с помощью медицинского специалиста по своему выбору.
- требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных трудовым законодательством. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения.
- требовать об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях.
- обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных.

## Сбор, обработка и хранение персональных данных

Обработка персональных данных работника - это получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

Работник предоставляет работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами. Предоставление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

При поступлении на работу работник заполняет анкету и автобиографию. Ан-кета представляет собой перечень вопросов о ПДн работника. Анкета заполняется работником самостоятельно. При заполнении анкеты работник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркиваний, прочерков, помарок в строгом соответствии с записями, которые содержатся в его личных документах. Автобиография - документ, содержащий описание в хронологической последовательности основных этапов жизни и деятельности принимаемого работника. Автобиография составляется в произвольной форме, без помарок и исправлений. Анкета и автобиография работника должны храниться в личном деле работника. В личном деле также хранятся иные документы персонального учета, относящиеся к персональным данным работника. Личное дело работника оформляется после издания приказа о приеме на работу. Все документы личного дела подшиваются в обложку образца, установленного в организации. На ней указываются фамилия, имя, отчество работника, номер личного дела. Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитых в личное дело, нумеруются. Личное дело ведется на протяжении всей трудовой деятельности работника. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

## Передача персональных данных

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работника в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

## Доступ к персональным данным сотрудника

Право доступа к персональным данным сотрудника имеют:
- заведующий МБДОУ;
- ответственный за обеспечение безопасности ПДн;
- сам работник, носитель данных.

К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;
- медицинские учреждения, задействованные согласно Договоров к осмотру сотрудников МБДОУ;
- другие организации (сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника);
- родственники и члены семей (персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника).

В случае развода бывшая супруга (супруг) имеет право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (согласно ТК РФ).

## Защита персональных данных работников

В целях обеспечения сохранности и конфиденциальности персональных данных работников МБДОУ все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться ответственным за обеспечение безопасности ПДн.

Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке организации и в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках организации.

Передача информации, содержащей сведения о персональных данных работников организации, по телефону, факсу, электронной почте без письменного согласия работника запрещается.

Личные дела и документы, содержащие персональные данные работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

## Ответственность за разглашение информации, связанной с персональными данными работника

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Приложение 3
к модели угроз безопасности персональных данных
при их обработке в информационных системах персональных данных
МБДОУ «Детский сад «Колосок» г.Заозерного»

**Инструкция пользователю**
**МБДОУ «Детский сад «Колосок» г. Заозерного»**

Общие положения

Инструкция разработана в соответствии нормативными документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ пользователями в АС на базе автоматизированного рабочего места МБДОУ «Детский сад «Колосок» г. Заозерного» (далее МБДОУ).

В соответствии с "Актом определения уровня защищенности" МБДОУ «Детский сад «Колосок» г. Заозерного» является автоматизированной системой уровня защищенности 4.

Субъектами доступа к ресурсам АС являются пользователи, администраторы и обслуживающий персонал (сотрудники, осуществляющие техническое обслуживание, ремонт).

Обрабатываемая в АС информация относится к сведениям, составляющим информацию ограниченного доступа, и имеет максимальный гриф конфиденциальности "для служебного пользования".

Все отчуждаемые и не отчуждаемые носители информации имеют гриф конфиденциальности, равный максимальному грифу конфиденциальности обрабатываемой информации.

Пользователи получают свои права на доступ к ресурсам АС через администратора информационной безопасности (АИБ).

Общее руководство и контроль обеспечения информационной безопасности пользователями АС и обслуживающим персоналом осуществляет администратор информационной безопасности.

Пользователи имеют право вносить предложения по изменению и дополнению данной инструкции (в письменном виде на имя заведующего). Изменения и дополнения к данной инструкции утверждаются в установленном порядке. Правом толкования положений настоящей инструкции возлагается на заведующего МБДОУ «Детский сад «Колосок» г. Заозерного».

Требования к пользователям

Пользователи, не ознакомленные с данной инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами АС не допускаются.

Пользователи обязаны выполнять требования администратора информационной безопасности (АИБ).

Пользователи обязаны немедленно ставить в известность АИБ обо всех неисправностях и нарушениях в работе технических средств (ТС), средств защиты информации (СЗИ), прикладного и системного программного обеспечения (ПО).

Доступ к ресурсам АС

Обязательными условиями получения доступа к ресурсам АС пользователей являются:

- наличие формы допуска к конфиденциальной информации (не ниже "ДСП");
- право прохода на контролируемую территорию (пропуск);
- право доступа в помещение и к автоматизированным рабочим местам (приказ «О допуске сотрудников к работе в АС»);
- знание технологии обработки информации на АРМ с учетом требований информационной безопасности (ознакомление с «Технологическим процессом обработки информации»);
- право доступа к конкретным ресурсам АС.

Идентификация пользователей в автоматизированную систему осуществляется по уникальному имени и паролю.

Длина пароля пользователей - не менее 6 буквенно-цифровых символов.

Уникальные имена пользователи получают от АИБ в установленном порядке. Пользователи обязаны помнить и соблюдать в тайне свои имена и пароли, не до-пускается их запись на каких либо носителях в целях напоминания. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами.

При утере или подозрении на утечку своих имен и паролей пользователи должны немедленно сообщить об этом АИБ.

Пользователь имеет право требовать у АИБ изменения своих идентификационных данных в АС.

## Требования к учету и обращению с машинными носителями информации

Все машинные носители информации (МНИ), задействованные в процессе обработки информации ограниченного доступа, должны быть поставлены на учет в конфиденциальном делопроизводстве в соответствии с действующими требованиями. На отчуждаемых МНИ (USB накопители) указывается инвентарный номер и гриф конфиденциальности.

Понижение грифа конфиденциальности МНИ не допускается даже в случае отсутствия на нем соответствующей информации.

Отчуждаемые МНИ используются исключительно в соответствии с утвержденным "Технологическим процессом обработки информации" (ТП). Один пользователь имеет право работать с несколькими отчуждаемыми МНИ.

Выдача МНИ из места его хранения пользователю, не имеющему доступа к нему, не допускается. Допускается передача и выдача из места его хранения любых МНИ АИБ для осуществления резервирования и восстановления информации ограниченного доступа.

Пользователь имеет право требовать у АИБ провести внеплановое резервирование информации.

По окончании рабочей смены пользователь должен сдать отчуждаемые МНИ и хранить в металлическом шкафу.

При заполнении отчуждаемого МНИ информацией, пользователь пишет заявку на выдачу дополнительного отчуждаемого МНИ. Выдача новых МНИ производится в установленном порядке.

При подозрении на неисправность МНИ пользователь ставит в известность об этом АИБ. Если неисправность подтверждается и исправить ее невозможно, МНИ подлежит уничтожению в установленном порядке.

## Порядок работы пользователя с ресурсами АС

Начало работы на ПЭВМ.

Включить ПЭВМ и дождаться завершения загрузки и готовности системы защиты информации (СЗИ) и операционной системы (ОС) к идентификации пользователя. Для получения доступа к ресурсам АС пользователь должен ввести с клавиатуры имя своей учетной записи и пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке идентификации пользователя, пользователь должен обратиться к АИБ.

Завершение работы на ПЭВМ.

По мере окончания работ пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения ПЭВМ), либо завершить работу ПЭВМ стандартным способом (при этом выключить ПЭВМ).

Общие требования к обработке информации на ПЭВМ.

При обработке на ПЭВМ информации ограниченного доступа используется необходимый и достаточный набор программных средств. Перечень программного обеспечения, устанавливаемого на ПЭВМ, утверждается в установленном порядке. Пользователям запрещается устанавливать или удалять какие-либо программные средства. Кроме того, пользователям запрещается запускать любые режимы работы и программы

(служебные программы СЗИ и ОС), выходящие за рамки установленной для них технологии обработки информации согласно ТП.

Каждый пользователь может работать только с теми ресурсами АС, к которым ему предоставлен доступ АИБ. В случае невозможности доступа к каким-либо ресурсам АС или недостаточности типа доступа (чтение, запись, удаление) для об-работки информации, а также любых других несоответствий между настройками доступа и ТП пользователь должен обратиться к АИБ.

При необходимости внесения изменений в систему доступа, сотрудник делает письменную заявку на имя заведующей МБДОУ.

При выходе из помещения пользователь обязан завершить сеанс своей работы либо заблокировать АРМ (штатными средствами ОС).

Запрещается работа пользователей на ПЭВМ в присутствии лиц, не имеющих доступа к ресурсам АС.

Пользователям запрещается изменять местоположение составных частей ПЭВМ, а также подключать к ПЭВМ какие-либо аппаратные средства.

Запрещаются любые, не утвержденные в ТП, способы копирования и переноса информации с аппаратных средств ПЭВМ (монитор, МНИ и др.) на любые МНИ.

По требованию пользователя АИБ проводит архивное копирование и восстанавливает необходимую информацию из архива.

Удаление файлов возлагается на пользователя. Восстановление файлов из корзины запрещено.

## Требования к распечатыванию информации.

Все бумажные носители информации (БН), задействованные в процессе обработки информации ограниченного доступа, должны быть поставлены на учет в конфиденциальном делопроизводстве в соответствии с действующими требованиями.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам АС, все учтенные БН должны быть недоступны для просмотра и иного их использования.

Готовые распечатанные на ПЭВМ документы учитываются и хранятся в металлическом шкафу в установленном порядке.

## Контроль

Действия пользователя (начало и окончание работы, работа с отчуждаемыми МНИ) должны регистрироваться средствами защиты информации и операционной системой. Контроль за выполнением всех вышеизложенных требований возлагается на АИБ.

## Ответственность

Пользователь несет личную ответственность за сохранность носителей информации и содержащейся на них информации (в рабочее время), а также за соблюдение требований данной инструкции и неправомерное использование ресурсов АС.