

**МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**«Арсеньевская средняя общеобразовательная школа»**

301510, п. Арсеньево, ул. Халтурина, д.11, Тел: 8 (48733) 21-4-97,

e-mail:mouasos@tularegion.org

---

**МОДЕЛЬ УГРОЗ**

**безопасности персональных данных, обрабатываемых в  
автоматизированном рабочем месте подключения к сетям  
информационного обмена в МОУ «Арсеньевская СОШ»**

**Обозначения и сокращения.**

**АРМ** - автоматизированное рабочее место

**ВИ** - видовая информация

**ВТСС** - вспомогательные технические средства и системы

**ИСПДн** - информационная система персональных данных

**КЗ** - контролируемая зона

**МЭ** - межсетевой экран

**НДВ** - недекларированные возможности

**НСД** - несанкционированный доступ

**ОБПДн** - обеспечение безопасности персональных данных

**ОС** - операционная система

**ПДн** - персональные данные

**ПМВ** - программно-математическое воздействие

**ПО** - программное обеспечение

**ПЭМИН** - побочные электромагнитные излучения и наводки

**РИ** - речевая информация

**СВТ** - средство вычислительной техники

**СЗИ** - средство защиты информации

**СПИ** - стеганографическое преобразование информации

**СЭУПИ** - специальные электронные устройства перехвата информации

**ТКУИ** - технический канал утечки информации

**ТСОИ** - технические средства обработки информации

**УБПДн** - угрозы безопасности персональных данных

**1. Термины и определения**

В настоящем документе используются следующие термины и их определения:

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

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

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

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

**Вирус (компьютерный, программный)** - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не

всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

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

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

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

**Доступ к информации** - возможность получения информации и ее использования.

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

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

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

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

**Информационная система персональных данных** - это 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.

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

**Контролируемая зона** - это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

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

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

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

**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, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

**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.

**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** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

**Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, 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.

**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** - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

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

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

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

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

**Технические средства информационной системы персональных данных** - средства вычислительной техники, информационно-вычислительные комплексы и сети,

средства и системы передачи, приема и обработки персональных данных (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.

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

**Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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

**Утечка (защищаемой) информации по техническим каналам** - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость** - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

## **2. Общие положения.**

ИСПДн подлежат классификации устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

Идентификация ИСПДн – выделение в ИТ-инфраструктуре областей учреждения (отдельных рабочих станций, узлов и сегментов сети), в которых осуществляется обработка ПДн, определение границ контролируемых зон для выделенных областей, присвоение наименований отдельным ИСПДн в составе ИТ-инфраструктуры учреждения, утверждение перечня защищаемых ИСПДн приказом руководителя учреждения.

## **3. Исходные данные по ИСПДн.**

### **3.1. Назначение и состав ИСПДн.**

ИСПДн предназначена для хранения и сбора ПДн сотрудников, учащихся и их родителей (законных представителей), а именно: ФИО, даты рождения, пола, серии и номер документа, удостоверяющего личность; сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством; персональные данные о детях, оставшихся без попечения родителей; персональные данные кандидатов в усыновители, приемные родители, опекуны.

В состав ИСПДн входят: технические средства и их программное обеспечение и информационные ресурсы.

### **3.2. Условия размещения ИСПДн.**

Территориально технические средства размещены в помещениях, находящихся в пределах контролируемой зоны МОУ «Арсеньевская СОШ».

## **4. Классификация угроз безопасности.**

Классификация ИСПДн - это присвоение каждой идентифицированной ИСПДн класса (К1, К2, К3, К4), соответствующего её индивидуальным признакам.

В соответствии с рекомендациями ФСТЭК России, класс ИСПДн определяется с учётом категорий и объёма обрабатываемых ПДн, и ей должен быть присвоен буквенно-цифровой индекс К1, К2, К3 или К4.

Типовым ИСПДн могут быть присвоены следующие классы:

- класс 1 (К1) – информационные системы, для которых нарушения могут привести к значительным негативным последствиям для субъектов персональных данных;
- класс 2 (К2) – информационные системы, для которых нарушения могут привести к негативным последствиям для субъектов персональных данных;
- класс 3 (К3) – информационные системы, для которых нарушения могут привести к незначительным негативным последствиям для субъектов персональных данных;
- класс 4 (К4) – информационные системы, для которых нарушения не приводят к негативным последствиям для субъектов персональных данных.

**Категория 1** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

Данные этой категории не обрабатываются в ИСПДн школы.

**Разъяснение:** данные о больничном или декретном отпуске, обрабатываемые в бухгалтерии – не являются ПДн 1 категории. Это не информация о состоянии здоровья и вообще не относится к персональным данным. Это информация о временной нетрудоспособности (именно так эти данные должны быть отражены в «Отчёте о внутренней нетрудоспособности» в разделе, описывающем бухгалтерскую систему).

**Категория 2** – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Это совокупность данных 3 категории с еще какими-либо данными. Например, сами по себе данные об образовании в совокупности с данными 4 категории (например, ФИО), не образуют данных 2 или 3 категории – это все так же останутся данные 4 категории. Но если данные об образовании обрабатываются вместе с данными 3 категории (ФИО и адрес прописки), то эта совокупность данных становится данными 2 категории.

**Категория 3** – персональные данные, позволяющие идентифицировать субъекта персональных данных.

Под идентификацией понимается – однозначное выделение субъекта из множества.

К персональным данным позволяющим идентифицировать человека относятся такие данные, которые позволяют установить личность человека.

**Объяснение:** обработка только фамилии, имени и отчества – не позволяет идентифицировать человека, т.к. встречаются полные однофамильцы.

Наиболее часто встречающиеся совокупности данных, позволяющих идентифицировать субъекта:

- паспортные данные (полностью);
- ФИО (полностью) + дата рождения;
- ФИО (полностью) + адрес проживания;
- ФИО (полностью) + должность (если в базе данных указано название организации);
- ФИО + фотография (качества не хуже, чем на паспорте).

**Объяснение:** совокупность данных позволяющих идентифицировать субъекта (например, ФИО + дата рождения + адрес проживания) относится к 2 категории, как к данным позволяющим идентифицировать человека и получить о нем дополнительные сведения.

**Объяснение:** обработка других данных о субъекте вместе с данными 3 категории (например, ФИО + дата рождения + данные об образовании), относит персональные данные к 2 категории.

**Объяснение:** при определении объема ПДн бухгалтерские системы имеют Хнпд равный 3.

**Категория 4** – обезличенные и / или общедоступные персональные данные.

Это данные не позволяющие идентифицировать человека. Наиболее часто встречающиеся совокупности данных, не позволяющих идентифицировать субъекта:

- фамилия и инициалы + любые другие данные;
- порядковый номер + любые другие данные.

Обезличивание данных, является одним из основных способов понижения класса ИСПДн.

В МОУ «Арсеньевская СОШ» обрабатываются следующие персональные данные: ФИО, даты рождения, пол, серии и номер документа удостоверяющего личность, домашние адреса и телефоны, семейное положение, а так же различные типы документов для участия в ГИА и ЕГЭ. Таким образом, категория ПДн (Хпд), обрабатываемых в ИСПДн может быть отнесена ко **2-й категории**, так как позволяют идентифицировать субъекта ПДн и получить о нём дополнительную информацию, за исключением ПДн, относящейся к 1-й категории (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни).

В зависимости от объёма обрабатываемых ПДн (Хнпд) может быть присвоено значение **3** (в ИСПДн школы одновременно обрабатываются данные менее чем 1000 субъектов персональных данных).

Класс ИСПДн МОУ «Арсеньевская СОШ» определяется в соответствии с таблицей №1.

Хнпд Хпд	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

По данным характеристикам обрабатываемых ПДн ИСПДн школы относится к специальной информационной системе, так как в ИСПДн кроме обеспечения конфиденциальности ПДн, требуется обеспечить защищённость от уничтожения ПДн.

МОУ «Арсеньевская СОШ» может быть присвоен **класс 3 (К3 - специальная)** – информационные системы, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПДн.

## 5. Классификация угроз безопасности персональных данных.

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения **информативных сигналов**, содержащих **защищаемую информацию**, и возможностей источников угрозы.

К характеристикам ИСПДн, обуславливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в ИСПДн персональных данных, структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы **обработки персональных данных**, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Информационные системы ПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также **информационных технологий**, применяемых при обработке ПДн.

Основными элементами ИСПДн являются:

персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;

информационные технологии, применяемые при обработке ПДн;

технические средства, осуществляющие обработку ПДн (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) (далее - технические средства ИСПДн);

программные средства (операционные системы, системы управления базами данных и т.п.);

средства защиты информации;

**вспомогательные технические средства и системы (ВТСС)** - технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях (далее - служебные помещения), в которых расположены ИСПДн, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электроснабжения).

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн.

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

- источник УБПДн - субъект, материальный объект или физическое явление, создающие УБПДн;

- среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

- носитель ПДн - физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

По способам реализации УБПДн выделяются следующие классы угроз:

- угрозы, связанные с **НСД** к ПДн (в том числе угрозы внедрения вредоносных программ);

- угрозы утечки ПДн по **техническим каналам утечки информации**;

- угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системного ПО;
- угрозы, реализуемые с использованием уязвимости прикладного ПО;
- угрозы, возникающие в результате использования уязвимости, вызванной наличием ВАС аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;
- угрозы, реализуемые с использованием уязвимостей, обуславливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых на АРМ;
- угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);
- угрозы безопасности ПДн, передаваемых по сетям связи;
- угрозы прикладным программам, с помощью которых обрабатываются ПДн;
- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

## **6. Общая характеристика результатов несанкционированного или случайного доступа**

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

Нарушение конфиденциальности может быть осуществлено в случае утечки информации:

- копирования ее на отчуждаемые носители информации;
- передачи ее по каналам передачи данных;
- при просмотре или копировании ее в ходе ремонта, модификации и утилизации программно-аппаратных средств;
- при "сборке мусора" нарушителем в процессе эксплуатации ИСПДн.

Нарушение целостности информации осуществляется за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

- микропрограммы, данные и драйвера устройств вычислительной системы;
- программы, данные и драйвера устройств, обеспечивающих загрузку операционной системы;
- программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) операционной системы;
- программы и данные прикладного программного обеспечения;
- программы и данные специального программного обеспечения;

- промежуточные (оперативные) значения программ и данных в процессе их обработки (чтения/записи, приема/передачи) средствами и устройствами вычислительной техники.

Нарушение **целостности информации** в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.

Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

- конфигурацией сети;
- адресами и маршрутизацией передачи данных в сети;
- функциональным контролем сети;
- безопасностью информации в сети.

Нарушение доступности информации обеспечивается путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных **ресурсов системы**, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:

- средств обработки информации;
- средств ввода/вывода информации;
- средств хранения информации;
- аппаратуры и каналов передачи;
- средств защиты информации.

## **7. Типовые модели угроз безопасности ПДн, обрабатываемых в АРМ, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.**

При обработке ПДн на автоматизированном рабочем месте, имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теми же условиями и факторами, что и для автоматизированного рабочего места, не имеющего подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Угрозы НСД в ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования. Угрозы из внешних сетей включают в себя:

- угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;

- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа "Отказ в обслуживании";
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

**Директор школы**



**Л.А.Петрова**