Утверждено
приказом по МБОУ СОШ № 7 г. Сальска
от 30.08.2019 г. № 289/1
директор _____ С.Ю.Лысикова

# МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ МБОУ СОШ №7 г. Сальска

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или

на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

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

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

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических 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** – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и/или блокировать аппаратные средства.

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

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** – именованный элемент системного, приклад-ного или аппаратного обеспечения функционирования информационной системы.

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

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

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

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

графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

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

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

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

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

**Учреждение** – образовательное учреждение города Москвы.

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

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

## ВВЕДЕНИЕ

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификации потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

| Группа | Уровень доступа к ПДн | Разрешенные действия |
|---|---|---|
| Администраторы ИСПДн | Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн.<br>Обладает полной информацией о технических средствах и конфигурации ИСПДн.<br>Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.<br>Обладает правами конфигурирования и административной настройки технических средств ИСПДн. | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение |
| Администратор безопасности | Обладает правами Администратора ИСПДн.<br>Обладает полной информацией об ИСПДн.<br>Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.<br>Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение |
| Операторы ИСПДн с правами записи | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение |
| Операторы ИСПДн с правами чтения | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн. | - использование |

### 1.1 КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

– внешние нарушители – физические лица, осуществляющие целенаправленное деструктивное воздействие, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

– внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:
*общая информация* – информации о назначения и общих характеристиках ИСПДн.

## 1.2 ИСХОДНЫЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ ИСПДН

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн.

**Исходный уровень защищенности**

| **Позиция** | **Технические и эксплуатационные характеристики** | **Уровень защищенности** |
|---|---|---|
| 1 | По территориальному размещению | высокий |
| 2 | По наличию соединения с сетями общего пользования | средний |
| 3 | По встроенным (легальным) операциям с записями баз персональных данных | низкий |
| 4 | По разграничению доступа к персональным данным | низкий |
| 5 | По наличию соединений с другими базами ПДн / иных ИСПДн | низкий |
| 6 | По уровню (обезличивания) ПДн | низкий |
| 7 | По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | |

Таким образом ИСПДн имеет низкий уровень исходной защищенности.

**Реализуемость УБПДн**

| **Тип угроз безопасности ПДн** | **Коэффициент реализуемости угрозы (Y)** | **Возможность реализации** |
|---|---|---|
| *1. Угрозы от утечки по техническим каналам* | | |
| 1.1. Угрозы утечки акустической информации | 0,25 | низкая |
| 1.2. Угрозы утечки видовой информации | 0,25 | низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | 0,25 | низкая |
| *2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа* | | |
| 2.1. Кража и уничтожение носителей информации | 0,25 | низкая |
| 2.2. Кража физических носителей ключей и атрибутов доступа | 0,25 | низкая |
| 2.3. Утрата носителей информации | 0,25 | низкая |
| 2.4. Утрата и компрометация ключей и атрибутов доступа | 0,35 | низкая |
| *3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств* | | |
| 3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа | 0,35 | низкая |
| 3.2. Утечка информации через порты ввода/вывода | 0,25 | низкая |
| 3.3. Воздействие вредоносных программ (вирусов) | 0,35 | низкая |
| 3.4. Установка ПО, не связанного с исполнением служебных обязанностей | 0,35 | низкая |
| 3.5. Внедрение или сокрытие не декларированных возможностей системного ПО и ПО для обработки персональных данных | 0,35 | низкая |
| 3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему | 0,25 | низкая |
| *4. Угрозы несанкционированного доступа к информации по каналам связи* | | |
| 4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны | 0,25 | низкая |
| 4.2. Угрозы сканирования, направленные на выявление | 0,25 | низкая |

| | | |
|---|---|---|
| типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | | |
| 4.3. Угрозы выявления паролей по сети | 0,25 | низкая |
| 4.4. Угрозы типа «Отказ в обслуживании» | 0,25 | низкая |
| 4.5. Угрозы внедрения по сети вредоносных программ | 0,25 | низкая |
| 4.6. Утечка информации, передаваемой с использованием протоколов беспроводного доступа | 0,25 | низкая |
| 4.7. Перехват, модификация закрытого ключа ЭЦП | 0,25 | низкая |
| 4.8. Угрозы удаленного запуска приложений | 0,25 | низкая |
| *5. Угрозы антропогенного характера* | | |
| 5.1. Разглашение информации | 0,35 | средняя |
| 5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов | 0,35 | низкая |
| 5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей | 0,25 | низкая |
| 5.4. Угроза нарушения политики предоставления и прекращения доступа | 0,25 | низкая |
| 5.5. Непреднамеренная модификация (уничтожение) информации | 0,35 | низкая |
| 5.6. Непреднамеренное отключение средств защиты | 0,25 | низкая |
| *6. Угрозы воздействия непреодолимых сил* | | |
| 6.1. Стихийное бедствие | 0,25 | низкая |
| 6.2. Выход из строя аппаратно-программных средств | 0,25 | низкая |
| 6.3. Аварии (пожар, потоп, случайное отключение электричества) | 0,25 | низкая |

**Опасность УБПДн**

| **Тип угроз безопасности ПДн** | **Опасность угрозы** |
|---|---|
| *1. Угрозы от утечки по техническим каналам.* | |
| 1.1. Угрозы утечки акустической информации | низкая |
| 1.2. Угрозы утечки видовой информации | низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | низкая |
| *2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа* | |
| 2.1. Кража и уничтожение носителей информации | низкая |
| 2.2. Кража физических носителей ключей и атрибутов доступа | низкая |
| 2.3. Утрата носителей информации | низкая |
| 2.4. Утрата и компрометация ключей и атрибутов доступа | низкая |
| *3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств* | |
| 3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа | низкая |
| 3.2. Утечка информации через порты ввода/вывода | низкая |
| 3.3. Воздействие вредоносных программ (вирусов) | низкая |
| 3.4. Установка ПО, не связанного с исполнением служебных обязанностей | низкая |
| 3.5. Внедрение или сокрытие не декларированных возможностей системного ПО и ПО для обработки персональных данных | низкая |
| 3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему | низкая |
| *4. Угрозы несанкционированного доступа к информации по каналам связи* | |

| | |
|---|---|
| 4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны | низкая |
| 4.2. 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. | низкая |
| 4.3. Угрозы выявления паролей по сети | низкая |
| 4.4. Угрозы типа «Отказ в обслуживании» | низкая |
| 4.5. Угрозы внедрения по сети вредоносных программ | низкая |
| 4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа | низкая |
| 4.7. Перехват, модификация закрытого ключа ЭЦП | низкая |
| 4.8. Угрозы удаленного запуска приложений | низкая |
| *5. Угрозы антропогенного характера* | |
| 5.1. Разглашение информации | низкая |
| 5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов | низкая |
| 5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей | низкая |
| 5.4. Угроза нарушения политики предоставления и прекращения доступа | низкая |
| 5.5. Непреднамеренная модификация (уничтожение) информации | низкая |
| 5.6. Непреднамеренное отключение средств защиты | низкая |
| *6. Угрозы воздействия непреодолимых сил* | |
| 6.1. Стихийное бедствие | низкая |
| 6.2. Выход из строя аппаратно-программных средств | низкая |
| 6.3. Аварии (пожар, потоп, случайное отключение электричества) | низкая |

**Актуальность УБПДн**

| **Тип угроз безопасности ПДн** | **Опасность угрозы** |
|---|---|
| *1. Угрозы от утечки по техническим каналам.* | |
| 1.1. Угрозы утечки акустической информации | неактуальная |
| 1.2. Угрозы утечки видовой информации | неактуальная |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | неактуальная |
| *2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа* | |
| 2.1. Кража и уничтожение носителей информации | неактуальная |
| 2.2. Кража физических носителей ключей и атрибутов доступа | актуальная |
| 2.3. Утрата носителей информации | неактуальная |
| 2.4. Утрата и компрометация ключей и атрибутов доступа | актуальная |
| *3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств* | |
| 3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа | неактуальная |
| 3.2. Утечка информации через порты ввода/вывода | актуальная |
| 3.3. Воздействие вредоносных программ (вирусов) | актуальная |
| 3.4. Установка ПО, не связанного с исполнением служебных обязанностей | актуальная |
| 3.5. Внедрение или сокрытие не декларированных возможностей системного ПО и ПО для обработки персональных данных | неактуальная |
| 3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему | неактуальная |
| *4. Угрозы несанкционированного доступа к информации по каналам связи* | |
| 4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны | неактуальная |

| | |
|---|---|
| 4.2. 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. | неактуальная |
| 4.3. Угрозы выявления паролей по сети | неактуальная |
| 4.4. Угрозы типа «Отказ в обслуживании» | неактуальная |
| 4.5. Угрозы внедрения по сети вредоносных программ | неактуальная |
| 4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа | неактуальная |
| 4.7. Перехват, модификация закрытого ключа ЭЦП | неактуальная |
| 4.8. Угрозы удаленного запуска приложений | неактуальная |
| *5. Угрозы антропогенного характера* | |
| 5.1. Разглашение информации | актуальная |
| 5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов | неактуальная |
| 5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей | неактуальная |
| 5.4. Угроза нарушения политики предоставления и прекращения доступа | неактуальная |
| 5.5. Непреднамеренная модификация (уничтожение) информации | неактуальная |
| 5.6. Непреднамеренное отключение средств защиты | неактуальная |
| *6. Угрозы воздействия непреодолимых сил* | |
| 6.1. Стихийное бедствие | неактуальная |
| 6.2. Выход из строя аппаратно-программных средств | неактуальная |
| 6.3. Аварии (пожар, потоп, случайное отключение электричества) | неактуальная |

Были выявлены следующие актуальные угрозы:

- кража физических носителей ключей и атрибутов доступа;
- утрата и компрометация ключей и атрибутов доступа;
- утечка информации через порты ввода/вывода;
- воздействие вредоносных программ (вирусов);
- установка ПО, не связанного с исполнением служебных обязанностей;
- разглашение информации.

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

- установка антивирусной защиты;
- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;
- осуществление резервирования ключевых элементов ИСПДн;
- изолирование портов ввода/вывода;
- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.