Утверждено
приказом директора
МОУ «КСОШ №7»
от 08.09.2021г. № 327

ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ МУНИЦИПАЛЬНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ «КИРИШСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №7»

I. Перечень обозначений и сокращений

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
ИР - информационный ресурс
ПТС - программно-технические средства
СКЗИ - средства криптографической защиты информации
ФСБ - Федеральная служба безопасности;
ФСО - Федеральная служба охраны;
ФСТЭК - Федеральная служба по техническому и экспертному контролю.

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

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

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

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 предназначению 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.

2.1. Частная модель угроз безопасности персональных данных в информационной системе персональных данных муниципального общеобразовательного учреждения «Киришская средняя общеобразовательная школа №7» (далее- Частная модель угроз) разработаны на основании следующих документов:

- Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» ст. 19 ч.2 п. 1;

- Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008 (далее – Базовая модель угроз);

- банка данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru, далее – Банк данных угроз);

- методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных,

утвержденной заместителем директора ФСТЭК России 14.02.2008;

- методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8-го Центра ФСБ России 31.03.2015 № 149/7/2/6-432.

2.2. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (нарушение конфиденциальности, целостности и доступности обрабатываемых персональных данных).

Для информационных систем персональных данных МОУ «КСОШ №7» (далее – ИСПДн) целью защиты информации является обеспечение конфиденциальности, целостности и доступности обрабатываемых персональных данных.

2.3. В качестве источников угроз безопасности персональных данных могут выступать субъекты (физические лица, организации) или явления (техногенные аварии, стихийные бедствия, иные природные явления). При этом источники угроз могут быть следующих типов:

- антропогенные источники (антропогенные угрозы);
- техногенные источники (техногенные угрозы);
- стихийные источники (угрозы стихийных бедствий, иных природных явлений).

Источниками антропогенных угроз безопасности персональных данных могут выступать:

лица, осуществляющие преднамеренные действия с целью доступа к персональным данным (воздействия на персональные данные), содержащимся в информационной системе, или нарушения функционирования информационной системы или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности персональных данных);

лица, имеющие доступ к информационной системе, не преднамеренные действия которых могут привести к нарушению безопасности персональных данных (непреднамеренные угрозы безопасности персональных данных).

Преднамеренные угрозы безопасности персональных данных могут быть реализованы за счет утечки персональных данных по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах информационной системы, технические каналы перехвата информации при ее передаче по каналам (линиям) связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа.

2.4. Определение угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, осуществляется образовательной организацией- оператором ИСПДн.

В образовательной организации актом руководителя утверждается перечень ИСПДн, оператором которых они являются (далее – Операторы).

Определение угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, оформляется документально в виде Частной модели угроз, которая утверждается руководителем Оператора.

2.5. В случае если Оператором в соответствии с пунктом принято решение применения СКЗИ для обеспечения безопасности персональных данных в ИСПДн, то при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в данной ИСПДн, Оператор дополнительно формирует совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для ИСПДн, если для обеспечения безопасности персональных данных принято решение применения СКЗИ.

2.6. Настоящие Актуальные угрозы подлежат пересмотру (переоценке):

- при изменении законодательства Российской Федерации в части определения угроз безопасности персональных данных при их обработке в информационных системах;

- при появлении новых угроз в источниках данных об угрозах безопасности информации, используемых в настоящих Актуальных угрозах, которые будут актуальными для рассматриваемых типов ИСПДн;

- при изменении структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования ИСПДн, следствием которых стало возникновение новых актуальных угроз безопасности персональных данных;

- при повышении возможности реализации или опасности существующих угроз безопасности персональных данных;

- при появлении сведений и фактов о новых возможностях нарушителей.

Угрозы безопасности персональных данных, актуальные при обработке

персональных данных в ИСПДн, подлежат пересмотру (переоценке) Оператором:

- при внесении изменений в настоящие Актуальные угрозы для соответствующего типа ИСПДн;

- при изменении структурно-функциональных характеристик или особенностей функционирования ИСПДн, в следствии чего изменился тип, к которому относится ИСПДн;

- при применении в ИСПДн информационных технологий, посредством которых могут формироваться новые угрозы безопасности персональных данных, исключенные из базового (предварительного) перечня угроз безопасности персональных данных для этой ИСПДн Оператором в соответствии с пунктом 4.4 настоящих Актуальных угроз;

- при повышении возможности реализации существующих угроз безопасности персональных данных;

- в иных случаях по решению Оператора.

3. Описание информационных систем персональных данных и особенностей их функционирования

3.1.В образовательной организации существуют следующие типы ИСПДн:

ИСПДн ведения бухгалтерского учета, расчета заработной платы.

ИСПДн передачи информации, в том числе ПДн, в целях исполнения Федеральных законов.

3.2. В качестве объекта информатизации Школы выступают:

Автономные автоматизированные рабочие места (АРМ).

Локальные вычислительные сети.

3.3.ИСПДн образовательного учреждения относится к первому типу:

автоматизированные рабочие места (далее – АРМ), не имеющие подключение (незащищенное, защищенное) к каким-либо сетям связи, в том числе к беспроводным сетям связи (исключение составляют беспроводные технологии, предназначенные для функционирования периферийных устройств (клавиатура, манипулятор «мышь» и другие), входящих в состав АРМ).

3.4. Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта ПДн), так и с электронных носителей информации.

3.5. ИСПДн предполагают распределенную (на АРМ) обработку и хранение ПДн.

3.6. Персональные данные субъектов ПДн могут выводиться из ИСПДн

с целью передачи персональных данных субъектов Учреждения, как в электронном, так и в бумажном виде.

3.7. Все технические средства ИСПДн образовательной организации находятся в пределах Российской Федерации. Контролируемой зоной ИСПДн является отдельное помещение Оператор. В пределах контролируемой зоны находятся рабочие места пользователей, серверное оборудование, а также сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны могут находиться линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи.

Контролируемый доступ (контролируемая зона) в помещение обеспечивается, в том числе с использованием систем видеонаблюдения. Неконтролируемый вынос за пределы административного здания технических средств ИСПДн запрещен.

3.8. Помещение, в котором ведется обработка персональных данных (далее – Помещение), оснащено входной дверью с замком. Операторами установлен порядок доступа в Помещение, препятствующий возможности неконтролируемого проникновения или пребывания в этом Помещении лиц, не имеющих права доступа в них. В рабочее время, в случае ухода лиц, имеющих право самостоятельного доступа в Помещение, а также в нерабочее время двери Помещение закрывается на ключ. Доступ посторонних лиц в Помещение допускается только в присутствии лиц, имеющих право самостоятельного доступа в данное Помещение на время, ограниченное служебной необходимостью. При этом Оператором предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным, в том числе через устройства ввода (вывода) информации, а также к носителям персональных данных.

Устройства ввода (вывода) информации, участвующие в обработке персональных данных, располагаются в Помещении таким образом, чтобы исключить случайный просмотр обрабатываемой информации посторонними лицами, вошедшими в Помещение, а также через двери и окна Помещения.

3.9. Ввод (вывод), обработка и хранение персональных данных в ИСПДн осуществляется с использованием бумажных и машинных носителей информации, в том числе съемных машинных носителей информации (магнитные и оптические диски, флеш-накопители, накопители на жестких магнитных дисках, твердотельные накопители и другие) (далее – Машинные носители персональных данных).

Оператором установлен порядок, обеспечивающий сохранность используемых Машинных носителей персональных данных, осуществляется их поэкземплярный учет. Хранятся Машинные носители персональных

данных только в Помещении в сейфе в условиях, препятствующих свободному доступу к ним посторонних лиц. Выдача Машинных носителей персональных данных осуществляется под подпись только сотрудникам, допущенным к обработке персональных данных.

3.10. В целях обеспечения целостности обрабатываемых в ИСПДн персональных данных Оператор осуществляет их резервирование в соответствии с установленным порядком с использованием Машинных носителей персональных данных. В наличии имеются комплекты восстановления на применяемое в ИСПДн системное и прикладное программное обеспечение, а также средства защиты информации.

Для ключевых элементов ИСПДн предусмотрен источник резервного электропитания, при необходимости применяются системы вентиляции и кондиционирования воздуха. Помещения оснащены средствами пожарной сигнализации.

3.11. Обеспечение антивирусного контроля в ИСПДн осуществляется в соответствии с установленным Операторами порядком с применением средств антивирусной защиты информации.

3.12. В ИСПДн обработка информации осуществляется в однопользовательском и многопользовательском режимах. Осуществляется разграничение прав доступа (набора действий, разрешенных для выполнения) пользователей. Обслуживание технических и программных средств ИСПДн, средств защиты информации, в том числе СКЗИ и среды их функционирования, включая настройку, конфигурирование и распределение носителей ключевой информации между пользователями ИСПДн, осуществляется оператором ЭВМ, ответственным за обеспечение безопасности персональных данных. Оператором назначается сотрудник, ответственный за обеспечение безопасности персональных данных в ИСПДн.

3.15. К объектам защиты в ИСПДн относятся:

- обрабатываемые персональные данные;

- технические средства, в том числе Машинные носители персональных данных, средства и системы связи и передачи данных, технические средства обработки графической, виде- и речевой информации, содержащей персональные данные;

- средства защиты информации;

- среда функционирования средств защиты информации;

- информация, относящаяся к защите персональных данных, включая ключевую, парольную информацию;

- носители ключевой, парольной информации;

- документы, в которых отражена информация о мерах и средствах защиты ИСПДн;

- помещение;

- каналы (линии) связи.

3.16. ИСПДн образовательного учреждения с учетом его структурно-функциональных характеристик и условий эксплуатации, а также применяемых информационных технологий и предпринятых мер обеспечения безопасности персональных данных, указанных в настоящем разделе, имеют средний уровень исходной защищенности.

3.17. Операторы для имеющихся ИСПДн на постоянной основе должны обеспечивать меры обеспечения безопасности персональных данных, приведенные в настоящем разделе.

4. Оценка возможностей нарушителей по реализации угроз безопасности персональных данных

4.1. Нарушителем является физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке в ИСПДн.

В зависимости от права разового или постоянного доступа в контролируемую зону и возможностей по доступу к обрабатываемым персональным данным и (или) к компонентам ИСПДн рассматриваются нарушители двух типов:

внешние нарушители – лица, не имеющие права доступа к ИСПДн или ее отдельным компонентам;

внутренние нарушители – лица, имеющие право постоянного или разового доступа к ИСПДн или ее отдельным компонентам.

4.2. С учетом состава (категории) и объема обрабатываемых персональных данных в ИСПДн, а также целей и задач их обработки в качестве возможных целей (мотивации) реализации нарушителями угроз безопасности персональных данных в ИСПДн могут быть:

- получение выгоды путем мошенничества или иным преступным путем;
- любопытство или желание самореализации;
- реализация угроз безопасности персональных данных из мести;
- реализация угроз безопасности персональных данных непреднамеренно из-за неосторожности или неквалифицированных действий.

4.3. Для ИСПДн образовательного учреждения рассматриваются следующие виды нарушителей:

- лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ, – внутренние нарушители;

- лица, обслуживающие инфраструктуру оператора (охрана, уборщики и т.д.), – внутренние нарушители;
- пользователи ИСПДн – внутренние нарушители.

4.4. Нарушители обладают следующими возможностями по реализации угроз безопасности персональных данных в ИСПДн:
- получать информацию об уязвимостях отдельных компонентов ИСПДн, опубликованную в общедоступных источниках;
- получать информацию о методах и средствах реализации угроз безопасности персональных данных (компьютерных атак), опубликованных в общедоступных источниках;
- самостоятельно осуществлять создание способов атак, подготовку и проведение атак на ИСПДн только за пределами контролируемой зоны;
- самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом и без физического доступа к ИСПДн или ее отдельным компонентам, на которых реализованы меры и средства защиты информации, в том числе СКЗИ и среда их функционирования.

4.5. С учетом имеющейся совокупности предположений о целях (мотивации) и возможностях нарушителей по реализации угроз безопасности персональных данных в ИСПДн потенциал нападения при реализации угроз безопасности персональных данных для рассматриваемых видов нарушителей будет базовый (низкий). Нарушитель с базовым (низким) потенциалом является непрофессионалом, использует стандартное оборудование, имеет ограниченные знания об ИСПДн или совсем их не имеет, возможность доступа к ИСПДн или ее отдельным компонентам ограничена и контролируется организационными мерами и средствами ИСПДн.

4.6. В ИСПДн угрозы безопасности персональных данных могут быть реализованы внешними и внутренними нарушителями с базовым (низким) потенциалом следующими способами:
- несанкционированный доступ и (или) воздействие на объекты защиты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));
- несанкционированный доступ и (или) воздействие на объекты защиты на общесистемном уровне (операционные системы, гипервизоры);
- несанкционированный доступ и (или) воздействие на объекты защиты на прикладном уровне (системы управления базами данных, браузеры, веб-приложения, иные прикладные программы общего и специального назначения);

- несанкционированный физический доступ и (или) воздействие на объекты защиты (каналы (линии) связи, технические средства, носители информации).

5.Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

5.1. Угрозы безопасности персональных данных являются актуальными для ИСПДн, если существует вероятность их реализации нарушителем с базовым (низким) потенциалом, и такая реализация приведет к неприемлемым негативным последствиям (ущербу) от нарушения конфиденциальности, целостности или доступности обрабатываемых персональных данных.

5.2. С учетом среднего уровня исходной защищенности ИСПДн, состава (категории) и объема обрабатываемых в ИСПДн персональных данных, а также особенностей их обработки для ИСПДн актуальны угрозы безопасности персональных данных третьего типа. Угрозы безопасности персональных данных третьего типа не связаны с наличием недокументированных (недекларированных) возможностей в используемом в ИСПДн системном и прикладном программном обеспечении.

5.3. Принимая во внимание природно-климатические условия, характерные для Ленинградской области в силу ее территориального положения, для ИСПДн техногенные угрозы, а также угрозы стихийных бедствий и иных природных явлений неактуальны и далее рассматриваются только антропогенные (преднамеренные, непреднамеренные) угрозы безопасности персональных данных.

С учетом особенностей функционирования, используемых структурно-функциональных характеристик, применяемых информационных технологий, характера и способов обработки персональных данных и предпринятых Операторами мер обеспечения безопасности персональных данных, а также возможных негативных последствий (ущерба) от реализации преднамеренные угрозы утечки персональных данных по техническим каналам для ИСПДн неактуальны и далее из преднамеренных угроз безопасности персональных данных рассматриваются только угрозы, реализуемые за счет несанкционированного доступа.

С учетом базового (низкого) потенциала возможных нарушителей и среднего уровня исходной защищенности ИСПДн вероятность (частота) реализации угроз безопасности персональных данных для ИСПДн оценивается не выше средней. Объективные предпосылки для реализации угроз безопасности персональных данных существуют, но принятые меры обеспечения безопасности персональных данных в ИСПДн недостаточны.

С учетом состава (категории) и объема обрабатываемых в ИСПДн персональных данных, а также уровня защищенности персональных данных в ИСПДн (необходимо обеспечение не выше чем второго уровня защищенности персональных данных) опасность угроз безопасности персональных данных для рассматриваемых типов ИСПДн оценивается не выше средней. В результате нарушения одного из свойств безопасности персональных данных (конфиденциальность, целостность, доступность) возможны умеренные негативные последствия для Оператора и субъектов персональных данных. При этом опасность угроз безопасности персональных данных, направленных на нарушение их целостности и доступности при обработке в ИСПДн оценивается как низкая. В результате нарушения одного из свойств безопасности персональных данных (целостность, доступность) возможны незначительные негативные последствия для Оператора и субъектов персональных данных.

Перечень актуальных угроз безопасности персональных данных при их обработке в ИСПДн образовательного учреждения приведен в Приложении № 1.

5.4. Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для рассматриваемых типов ИСПДн, в случае применения в них для обеспечения безопасности персональных данных СКЗИ, с учетом базового (низкого) потенциала возможных нарушителей и предпринятых Оператором мер обеспечения безопасности персональных данных, содержится в приложении № 2.

Приложение № 1
к Частной модели угроз безопасности персональных данных
в информационной системе персональных данных
МОУ «КСОШ №7»

Перечень актуальных угроз безопасности персональных данных при их обработке в ИСПДн МОУ «КСОШ №7»

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
1.	УБИ.004	Угроза аппаратного сброса пароля BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
2.	УБИ.008	Угроза восстановления аутентификационной информации	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
3.	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
4.	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
5.	УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
6.	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
7.	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
8.	УБИ.018	Угроза загрузки нештатной операционной системы	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
9.	УБИ.022	Угроза избыточного выделения оперативной памяти	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
10.	УБИ.023	Угроза изменения компонентов системы	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
11.	УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
12.	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
13.	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
14.	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
15.	УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
16.	УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
17.	УБИ.049	Угроза нарушения целостности данных кеша	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
18.	УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
19.	УБИ.053	Угроза невозможности управления правами пользователей BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
20.	УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
21.	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
22.	УБИ.071	Угроза несанкционированного восстановления удаленной защищаемой информации	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
23.	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
24.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
25.	УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
26.	УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
27.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
28.	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
29.	УБИ.088	Угроза несанкционированного копирования защищаемой информации	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
30.	УБИ.089	Угроза несанкционированного редактирования реестра	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
31.	УБИ.090	Угроза несанкционированного создания учетной записи пользователя	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
32.	УБИ.091	Угроза несанкционированного удаления защищаемой информации	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
33.	УБИ.093	Угроза несанкционированного управления буфером	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
34.	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
35.	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
36.	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
37.	УБИ.121	Угроза повреждения системного реестра	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
38.	УБИ.123	Угроза подбора пароля BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
39.	УБИ.124	Угроза подделки записей журнала регистрации событий	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
40.	УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
41.	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
42.	УБИ.144	Угроза программного сброса пароля BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
43.	УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
44.	УБИ.152	Угроза удаления аутентификационной информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
45.	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
46.	УБИ.155	Угроза утраты вычислительных ресурсов	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
47.	УБИ.156	Угроза утраты носителей информации	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность
48.	УБИ.158	Угроза форматирования носителей информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
49.	УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
50.	УБИ.177	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
51.	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
52.	УБИ.179	Угроза несанкционированной модификации защищаемой информации	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
53.	УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
54.	УБИ.182	Угроза физического устаревания аппаратных компонентов	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
55.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
56.	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
57.	УБИ.192	Угроза использования уязвимых версий программного обеспечения	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
58.	УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установлены на нем средств защиты	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
59.	УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы

Приложение № 2
к Частной модели угроз безопасности персональных данных
в информационной системе персональных данных
МОУ «КСОШ №7»

Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для ИСПДн, если для обеспечения безопасности персональных данных принято решение применения СКЗИ

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1.	Проведение атаки при нахождении в пределах контролируемой зоны	Актуально	
1.2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования; помещения, в которых находятся компоненты ИСПДн, на которых реализованы СКЗИ и среда функционирования	Неактуально	Проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн назначаются из числа доверенных лиц. Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн. Указанные помещения оснащены входными дверьми с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в них. В рабочее время, в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери этих помещений закрываются на ключ. Доступ посторонних лиц в помещения с компонентами ИСПДн допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты. Установлен порядок обеспечивающий сохранность документаций на СКЗИ, машинных носителей информации с комплектами восстановления СКЗИ, носителей ключевой, парольной и аутентифицирующей информации. Документация на СКЗИ и

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			указанные носители хранятся только в сейфах или закрываемых на ключ шкафах (ящиках) в условиях, препятствующих свободному доступу к ним посторонних лиц
1.3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы ИСПДн; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИСПДн; сведений о мерах по разграничению доступа в помещения, в которых находятся компоненты ИСПДн, на которых реализованы СКЗИ и среда функционирования	Актуально	
1.4.	Использование штатных средств ИСПДн, в которой используется СКЗИ, ограниченное реализованными в ИСПДн мерами, направленными на предотвращение и пресечение несанкционированных действий	Актуально	
2.1.	Физический доступ к компонентам ИСПДн, на которых реализованы СКЗИ и среда функционирования	Неактуально	Проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн назначаются из числа доверенных лиц. Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн. Указанные помещения оснащены входными дверьми с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в них. В рабочее время, в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери этих помещений закрываются на ключ. Доступ посторонних лиц в помещения с компонентами ИСПДн допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты
2.2.	Возможность располагать или воздействовать на аппаратные компоненты СКЗИ и среду функционирования, ограниченная	Неактуально	Базового (низкого) потенциала нарушителя недостаточно для реализации угрозы.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	мерами, реализованными в ИСПДн, в которой используется СКЗИ, направленными на предотвращение и пресечение несанкционированных действий		Проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн назначаются из числа доверенных лиц. Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн. Указанные помещения оснащены входными дверьми с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в них. В рабочее время, в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери этих помещений закрываются на ключ. Доступ посторонних лиц в помещения с компонентами ИСПДн допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты. Осуществляется разграничение, регистрация и учет доступа пользователей ИСПДн к объектам защиты с использованием организационных мер и средств ИСПДн. Правами управления (администрирования) ИСПДн обладают только привилегированные пользователи
3.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среды функционирования, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Для ИСПДн актуальны угрозы безопасности персональных данных третьего типа, не связанные с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
3.2.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в ИСПДн, в которой используется СКЗИ, направленными на предотвращение и пресечение несанкционированных действий	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
3.3.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды функционирования, в том числе с использованием исходных текстов входящего в среды функционирования прикладного программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
4.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Для ИСПДн актуальны угрозы безопасности персональных данных третьего типа, не связанные с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении
4.2.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования СКЗИ	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Отсутствует в наличии конструкторская документация на аппаратные и программные компоненты среды функционирования СКЗИ
4.3.	Возможность располагать или воздействовать на любые компоненты СКЗИ и среды функционирования	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Базового (низкого) потенциала нарушителя недостаточно для реализации угрозы