Муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад №22 «Березка» г.Кудымкара
(МБДОУ «Детский сад №22»)

УТВЕРЖДАЮ
Заведующий МБДОУ «Детский сад №22»
_____ С.С. Гагарина
23.12.2019 г.

Частная модель угроз бнзопасности персональных данных в информационной системе персональных данных в Муниципальном бюджетном дошкольном образовательном учреждении «Детский сад №22 «Березка» г.Кудымкара

Оглавление

СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место;
АС – автоматизированная система;
АВС – антивирусные средства;
ВП – выделенное помещение;
ВТСС – вспомогательные технические средства и системы;
ИСПДн – информационная система персональных данных;
КЗ – контролируемая зона;
ЛВС – локальная вычислительная сеть;
МЭ – межсетевой экран;
НДВ – не декларированные возможности;
НСД – несанкционированный доступ;
ОС – операционная система;
ПДн – персональные данные;
ПМВ – программно-математическое воздействие;
ПО – программное обеспечение;
ПЭВМ – персональная электронно-вычислительная машина;
ПЭМИН – побочные электромагнитные излучения и наводки;
САЗ – система анализа защищенности;
СВТ – средства вычислительной техники;
СЗИ – средства защиты информации;
СЗПДн – система (подсистема) защиты персональных данных:
СОВ – система обнаружения вторжений;
СУБД – система управления базами данных;
УБПДн – угрозы безопасности персональным данным.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

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 к информации - возможность получения информации и ее использования.

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

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

Информационная система персональных данных - 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 так средств.

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

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.

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

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.

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

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

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.

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.

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

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

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

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 программу с целью осуществить утечку, изменить, блокировать, уничтожать 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.

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.

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.

Уполномоченное оператором лицо - лицо, которому на основании договора оператор поручает обработку персональных данных.

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

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Частная модель угроз безопасности персональных данных (далее – Модель угроз), в информационных системах персональных данных МДОБУ «Детский сад №22 «Березка»» г. Кудымкар (далее ИСПДн), разработана на основании следующих документов:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утв. постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119);
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 15 февраля 2008 г.);

Данная Модель угроз используются при определении уровня защищенности персональных данных ПДн.

2. ИСХОДНЫЕ ДАННЫЕ ОБ ИСПДН

2.1 Перечень персональных данных, обрабатываемых в ИСПДн

В соответствии с Перечнем персональных данных обрабатываемых в МДОБУ «Детский сад №22 «Березка»» г. Кудымкар (утв. __.__.20__ г. заведующим МДОБУ Гагариной Светланой Сергеевной) в данной системе обрабатываются следующие персональные данные, подлежащие защите:

- первичные учетные данные работников;
- сведения о занимаемой должности;
- сведения о финансовом состоянии работника;
- сведения о реквизитах работника;
- дополнительные сведения о работнике;
- первичные данные детей и их родителей (законных представителей);
- сведения о реквизитах детей и их родителей (законных представителей).

2.2 Условия расположения составляющих АС, обрабатывающих персональные данные.

2.2.1 Расположение АС.

ИСПДн является локальной и состоит из 2 структурных единиц:

- АРМ №1 (619000, г. Кудымкар, пер. Детский, 36, кабинет бухгалтерии);
- АРМ №2 (619000, г. Кудымкар, пер. Детский, 36, кабинет заведующего).

2.2.2 Границы контролируемых зон.

Контролируемая зона проходит по периметру помещений, в которых расположены структурные единицы ИСПДн.

2.3 Конфигурация отдельных компонентов ИСПДн

Установленное в ИСПДн ПО приведено в таблице 1.

Таблица 1.

Элемент ИСПДн	Операционная система	Средство антивирусной защиты	ПО применяемое для обработки ПДн
АРМ №1	Microsoft Windows 7 Professional	Kaspersky Internet Security 2013 McAfee Security Scan Plus	1С Предприятие 7.7 1С:Предприятие 8.2 Microsoft Office, для дома и бизнеса 2010 Архиватор WinRAR Документы ПУ 5 Континент-АП КриптоПро CSP
АРМ №2	Microsoft Windows XP Professional	USB Disk Security 5.4.0.12	Microsoft Office Standard 2007 ABBYY FineReader 10 Professional Edition Total Commander 7.56a TrueCrypt Архиватор WinRAR

2.4 Технические средства, участвующие в обработке персональных данных в ИСПДн

В обработке персональных данных участвуют следующие технические средства:

Таблица 2.

№ п/п	Модель (тип) технического средства	Заводской (инвентарный) номер
1.	АРМ №1	
1.1	Системный блок	–
1.2	Монитор Samsung SyncMaster 940N	–

№ п/п	Модель (тип) технического средства	Заводской (инвентарный) номер
1.3	Клавиатура Genius	ZM5B27021233
1.4	Манипулятор оптический A4tech	74471226036799
2.	**АРМ №2**	
2.1	Системный блок SP	Инв. №104000638080
2.2	Монитор LG Flatron 566LE	Инв. №104000638081
2.3	Клавиатура Genius	ZM5727226776
2.4	Манипулятор оптический Genius	145138905950
2.5	Принтер Hp LaserJet 1200	Инв. №104000638084
2.6	МФУ Xerox Workcentre PE16	Инв. №104000638088

2.5 Режим и степень участия персонала в обработке персональных данных

Обработка персональных данных в компонентах ИСПДн осуществляется в однопользовательском или многопользовательском режиме без разграничения прав доступа.

2.5.1 Персонал, участвующий в обработке данных.

В процессе обработки персональных данных участвует следующий персонал:

- *Администратор безопасности* занимается обслуживанием и настройкой технических и программных средств ИСПДн;
- *Пользователь* осуществляет ввод, изменение и удаление персональных данных в ИСПДн.

2.5.2 Полномочия персонала, участвующего в обработке данных.

Персонал, участвующий в обработке персональных данных, наделен следующими полномочиями:

- *Администратор безопасности* осуществляет разграничение доступа, отвечает за настройку и бесперебойную работу сетевого оборудования. Администратор безопасности вправе проводить техническое обслуживание и настройку АРМ сотрудников, осуществлять контроль антивирусной защитой.
- *Пользователь* не имеет полномочий вносить модификации в настройки какого-либо оборудования и прикладного ПО, но уполномочен проводить все виды работ с персональными данными в рамках рассматриваемой ИСПДн.

3. КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН

Состав и содержание угроз безопасности персональных данных (далее – УБПДн) в ИСПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным (ПДн).

ИСПДн представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности. Основными элементами являются:

- персональные данные, содержащиеся в базах и файлах;
- информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;
- технические средства ИСПДн, осуществляющие обработку ПДн (средства вычислительной техники (СВТ), информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн);
- программные средства (операционные системы, СУБД);
- средства защиты информации (СЗИ);
- вспомогательные технические средства и системы (технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн, их технические средства (далее – служебные помещения) (различного рода технические средства и системы, средства вычислительной техники, средства и системы охранной и пожарной сигнализации, средства и системы кондиционирования, средства электронной оргтехники и т.п.) (далее – ВТСС).

Возможности источников УБПДн обусловлены совокупностью методов и 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 реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает необходимые условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

- источник УБПДн – субъект, материальный объект или физическое явление, создающее 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 находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Носители ПДн могут содержать информацию, представленную в следующих видах:

- видовая информация, представленная в виде текста и изображений различных устройств отображения информации СВТ ИСПДн;

- информация, обрабатываемая (циркулирующая) в ИСПДн в виде электрических, электромагнитных, оптических сигналов;
- информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, IP-протоколов, файлов и других логических структур.

Угрозы безопасности для ИСПДн МДОБУ «Детский сад №22 «Березка»» г. Кудымкар классифицируются по следующим признакам:

- по видам возможных источников УБПДн;
- по типу ИСПДн, на которые направлена реализация УБПДн;
- по способу реализации УБПДн;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
- по объекту воздействия.

По видам возможных источников УБПДн выделяются следующие классы угроз:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

По типу ИСПДн для МДОБУ «Детский сад №22 «Березка»» г. Кудымкар, на которые направлена реализация УБПДн, выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);

По виду несанкционированных действий, осуществляемых с ПДн в ИСПДн АС можно выделить следующие классы угроз:

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

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.

4. УГРОЗЫ УТЕЧКИ ПДН В ИСПДН АС ПО ТЕХНИЧЕСКИМ КАНАЛАМ

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих каналов утечки информации:

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

4.1 Угрозы утечки акустической (речевой) информации

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИСПДн.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн или акустическая система ИСПДн воспроизводящая ПДн.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя при обработке ПДн, обусловлено наличием функций голосового ввода ПДн в информационную систему или функций воспроизведения ПДн акустическими средствами информационной системы.

Вывод: В ИСПДн функции голосового ввода ПДн в ИСПДн или функции воспроизведения ПДн акустическими средствами отсутствуют, поэтому дальнейшее рассмотрение данной угрозы представляется **нецелесообразным**.

4.2 Угрозы утечки видовой информации

Источником угроз утечки видовой информации являются физические лица, не имеющие доступа к информационной системе.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Носителем ПДн являются технические средства ИСПДн, создающие физические поля, в которых информация находит свое отражение в виде символов и образов.

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения СВТ, входящих в состав ИСПДн.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Вывод: Перехват ПДн в ИСПДн МДОБУ «Детский сад №22 «Березка»» г. Кудымкар может вестись портативной носимой аппаратурой (портативные аналоговые и цифровые фото- и видеокамеры, цифровые видеокамеры, встроенные в сотовые телефоны) – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них в условиях наличия визуального контакта.

Перехват (просмотр) ПДн осуществляется посторонними лицами путем их непосредственного наблюдения в служебных помещениях либо на расстоянии прямой видимости из-за пределов ИСПДн с использованием оптических (оптикоэлектронных) средств.

4.3 Угрозы утечки информации по каналам побочных электромагнитных излучения и наводок

Источником угроз утечки информации за счет ПЭМИН являются физические лица, не имеющие доступа к ИСПДн.

Среда распространения информативного сигнала – неоднородная за счет перехода из одной среды в другую.

Носителем ПДн являются технические средства ИСПДн, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническим средствами ИСПДн.

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств ИСПДн сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИСПДн.

Вывод: рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН, избыточно, так как утечка ПДн по каналам ПЭМИН маловероятна из-за несоответствия стоимости средств съема информации и величиной ущерба для субъекта от полученной в результате регистрации ПЭМИН информации, следовательно, защита ПДн от данного вида угроз в дальнейшем **рассматриваться не будет.**

5. УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ В ИСПДН

Для ИСПДн МДОБУ «Детский сад №22 «Березка»» г. Кудымкар рассматриваются следующие типы угроз НСД с применением программных и программно-аппаратных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

- угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
- угрозы создания нештатных режимов работы программных (программно-аппаратных средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программ математического воздействия).

Кроме того, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду компьютера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств – это угрозы "Отказа в обслуживании". Реализация этих угроз обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

- содержаний служебной информации в пакетах сообщений, передаваемых по сети;
- условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);
- формат представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);
- программного обеспечения обработки данных.

В результате реализации угроз "Отказ в обслуживании" происходит переполнение буферов и блокирования процедур обработки, "заклинивание" процедур обработки и "зависание" компьютера, отбрасывание пакетов сообщений и др.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы, так как количество вредоносных программ уже несоразмерно велико по сравнению с вышеуказанными угрозами. Для осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

5.1 Источники угроз несанкционированного доступа к АС ИСПДн

Источниками угроз НСД в ИСПДн АС могут быть:

- нарушитель;
- носитель вредоносной программы;
- аппаратная закладка.

Так как ИСПДн МДОБУ «Детский сад №22 «Березка»» г. Кудымкар является локальной ИСПДн, имеющей подключение к сетям международного обмена, то целесообразно рассмотрение как внешних так и внутренних нарушителей.

Внешними нарушителями в рамках данной ИСПДн могут быть:

- недобросовестные партнеры;
- внешние субъекты (физические лица).

Притом, внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Осуществление несанкционированного доступа к каналам связи, выходящим за пределы служебных помещений **не рассматривается** вследствие несоответствия стоимости средств снятия информации с такого рода каналов связи и возможного ущерба субъекту ПДн при реализации такого рода угроз.

Осуществление несанкционированного доступа через автоматизированные рабочие места, подключенные к сетям связи **сетям международного информационного обмена не рассматривается**, т.к. все АРМ, включенные в ИСПДн МДОБУ «Детский сад №22 «Березка»», защищены межсетевым экраном, входящим в состав антивирусного средства.

Внутренними нарушителями являются лица, имеющие доступ к ИСПДн АС, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

- отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;
- встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок – видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти шин передачи данных, портов ввода-вывода;

- микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

- пакеты передаваемых по компьютерной сети сообщений;
- файлы (текстовые, графические, исполняемые и т.д.)

5.2 Характеристика уязвимостей ИСПДн

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной системы, которое может быть использовано для реализации угрозы безопасности персональным данным.

Причиной возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Преднамеренные действия по внесению уязвимостей в ходе проектирования и разработке программного (программно-аппаратного) обеспечения не рассматриваются вследствие высокой экономической затратности реализации такого рода рисков по сравнению с возможным ущербом для субъектов ПДн в рассматриваемой информационной системе.

Существуют следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

5.2.1 Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем:

- в микропрограммах, в прошивках запоминающих устройств;
- в средствах операционной системы, предназначенных для управления локальными ресурсами ИСПДн (обеспечивающих выполнение функций управления процессами,

памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.) драйверах, утилитах;

- в средствах операционной системы, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);
- в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Так как в качестве **операционных систем** в рассматриваемой ИСПДн используются операционные системы семейства **Microsoft Windows**, то в дальнейшем будут рассматриваться **уязвимости** характерные именно **для данного типа операционных систем**.

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программно реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Так как в рассматриваемой ИСПДн циркулирует трафик стека протоколов **TCP/IP**, то для сетевого взаимодействия характерны **уязвимости** связанные именно с этим протоколом, а так же **служебными протоколами**, используемыми **в сетях**, основанных **на IP-адресации**.

5.2.2 Уязвимости прикладного программного обеспечения

К прикладному программного обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

В рамках рассматриваемой ИСПДн **в качестве прикладных программ** можно отметить средства работы с базой данных **«1С: Предприятие»**, пакеты программ «**Microsoft Office**», программы **«Документы ПУ 5»** и **«ABBYY FineReader»**, средства криптографической защиты

«КриптоПро CSP» и **«Континент-АП»**, файловый менеджер **«Total Commander»**, а также средства антивирусного контроля **«Kaspersky Internet Security 2013»**, **«McAfee Security Scan Plus»** и «**USB Disk Security 5.4.0.12»**.

Специальные прикладные программы – это программы, которые разрабатываются в интересах решения конкретных прикладных задач в данном ИСПДн (в том числе программные средства защиты информации, разработанные для конкретной ИСПДн).

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн и использования штатных функций операционной системы, выполнения несанкционированного доступа без обнаружения таких изменений операционной системой;
- отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

5.3 Характеристика угроз непосредственного доступа в операционную среду АС ИСПДн

Для АС ИСПДн можно рассматривать следующие угрозы непосредственного доступа в операционную среду, которые могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн:

Угрозы, реализуемые в ходе загрузки операционной системы, направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн. Чаще всего **такие угрозы реализуются** с использованием отчуждаемых носителей информации **в условиях наличия разрешения на загрузку АРМ с такого рода носителей**.

Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);

Угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

5.4 Характеристика угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия

Для ИСПДн МДОБУ «Детский сад №22 «Березка»» г. Кудымкар можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- угроза "Анализ сетевого трафика" с перехватом передаваемой по сети информации;
- угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы внедрения ложного объекта сети;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;
- угрозы удаленного запуска приложений;
- угроза типа «Отказ в обслуживании»;
- угрозы внедрения по сети вредоносных программ.

Перечисленные угрозы возможны при существовании недобросовестных партнеров, входящих в единую информационную среду, подключение к которой имеет данная ИСПДн, либо при проникновении злоумышленника в локальную сеть организации.

5.4.1 Угроза "Анализ сетевого трафика"

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

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

Такого рода программы обнаруживаются по **аномальному поведению в сети**.

5.4.2 Угроза "сканирование сети"

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

5.4.3 Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовать угрозу с помощью целого ряда методов, таких как

простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы для перехвата пароля, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя "проход" для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Угроза такого рода может быть **отклонена при повышении временной сложности подбора пароля**, что достигается либо увеличением длины и сложности пароля, либо ограничением на количество неверных паролей введенных в единицу времени. Данный результат достигается организационными мерами.

5.4.4 Угрозы навязывания ложного маршрута сети путем несанкционированного изменении маршрутно-адресных данных

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлено недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменения в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

5.4.5 Угрозы внедрения ложного объекта сети

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

5.4.6 Угрозы типа "Отказ в обслуживании"

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

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода может служить: направленный шторм эхо-запросов по протоколу OCMP (Ping flooding),

шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускании каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICPM-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);
- явный отказ в обслуживании, вызванный нарушением логической связанности между техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;
- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа "Land", "TearDrop", "Bonk", "Nuke", "UDP-bomb") или имеющих длину, превышающую максимально допустимый размер (угроза типа "Ping Death"), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличии ошибок в программах, реализующих протоколы сетевого обмена.

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

5.4.7 Угрозы удаленного запуска приложений

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

Выделяются три подкласса данных угроз:

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

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде макрокоманд (документы Microsoft

Word, Excel и т.п.); html-документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов например, тексты JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

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

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

5.4.8 Угрозы внедрения по сети вредоносных программ

Воздействие с помощью вредоносных программ относится к программно-математическому воздействию. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

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

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

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;

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

5.4.9 Возможные последствия реализации угроз различных классов

В таблице 3 приведен перечень возможных последствий реализации угроз вышеперечисленных классов в рамках рассматриваемой ИСПДн.

Таблица 3

№№ п/п	Тип угрозы		Возможные последствия
1.	Анализ сетевого трафика		Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей. Что способно повлечь за собой выявление злоумышленником сетевых сервисов, используемых в ИСПДн, а так же некоторых их характеристик, с последующим нарушением их доступности и конфиденциальности передаваемых данных.
2.	Сканирование сети		Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей. Что способно повлечь за собой выявление злоумышленником структуры сети и направления информационных потоков.
3.	Угроза выявления пароля		Выполнение любого действия, связанного с получением несанкционированного доступа.
4.	Подмена доверенного объекта сети		Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации. Что способно повлечь за собой нарушение целостности, конфиденциальности и доступности передаваемых данных.
5.	Навязывание ложного маршрута сети		Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
6.	Внедрение ложного объекта сети		Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
7.	Отказ в обслуживании	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений. Увеличение времени обработки данных и снижение эффективности вычислительных операций.
		Полное исчерпание ресурсов	Невозможность передачи сообщений из-за

№№ п/п	Тип угрозы		Возможные последствия
			отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.п.). Возможен останов обработки ПДн в ИСПДн.
		Нарушение логической связанности между атрибутами, данными, объектами	Невозможность передачи сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
		Использование ошибок в программах	Нарушение работоспособности сетевых устройств
8.	Удаленный запуск приложений	Путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации
		Путем переполнения буфера серверного приложения	
		Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой

6. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

При обработке ПДн в ИСПДн МДОБУ «Детский сад №22 «Березка»» г. Кудымкар возможна реализация следующих УБПДн:

- угрозы утечки по техническим каналам;
- угрозы НСД к ПДн.

Угрозы утечки по техническим каналам включают в себя:

- угрозы утечки видовой информации;

Угрозы НСД к ПДн в ИСПДн АС включают в себя:

- угрозы, реализуемые в ходе загрузки операционной системы, направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
- угрозы "Анализ сетевого трафика" с перехватом передаваемой по сети информации;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;
- угрозы локального внедрения вредоносных программ;
- угрозы внедрения по сети вредоносных программ.

Угрозы НСД связаны с действиями нарушителей, рассмотренных выше, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн (внутренний нарушитель), а так же нарушителями, не имеющими непосредственного доступа к ИСПДн (внешний нарушитель).

Угрозы, связанные с не декларированными возможностями операционной системы и прикладного программного обеспечения, не рассматриваются как актуальные, так как потенциальный ущерб от их реализации незначителен.

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн МДОБУ «Детский сад №22 «Березка»» г. Кудымкар являются:

- угрозы утечки видовой информации;
- угрозы, реализуемые в ходе загрузки операционной системы;
- угрозы локального внедрения вредоносных программ;
- угрозы "Анализ сетевого трафика" с перехватом передаваемой по сети информации;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;
- угрозы внедрения по сети вредоносных программ.

Согласно вышеизложенному и постановлению Правительства РФ от 01 ноября 2012 г. № 1119, для персональных данных, обрабатываемых в МДОБУ «Детский сад №22 «Березка»» г. Кудымкар **актуальными являются угрозы 3-го типа**.