Частная модель угроз безопасности персональных данных МАОУ СШ №145

Содержание

1 Термины и определения

В настоящей модели используются следующие термины и определения:

1.1 **автоматизированная система**: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1.2 **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.

1.3 **вредоносная программа**: Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

1.4 **доступ в операционную среду 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.

1.5 **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 таких средств.

1.6 **информационные технологии**: Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

1.7 **контролируемая зона:** Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

1.8 **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.

1.9 **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 системыили средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

1.10 **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.

1.11 **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.

1.12 **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.

1.13 **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.

1.14 **пользователь информационной системы персональных данных**: Лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

1.15 **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.

1.16 **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.

1.17 **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.

1.18 **утечка (защищаемой) информации по техническим каналам**: Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

1.19 **уязвимость**: Некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

1.20 **целостность информации**: Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2 Сокращения

В настоящей модели используются следующие сокращения:

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

МЭ – межсетевой экран

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

3 Общие положения

3.1 Модель угроз безопасности персональных данных при их обработке в автоматизированной информационной системе МАОУ СШ №145 разработана во исполнение требований законодательства Российской Федерации и положений нормативно-методических документов федеральных органов исполнительной власти, регулирующих деятельность в области защиты персональных данных.

3.2 Настоящая модель угроз разработана на основании следующих документов:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.;

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г..

3.3 Настоящая модель определяет актуальные угрозы безопасности персональных данных при их обработке в АИС и должна использоваться при задании требований к системе защиты ПДн указанной информационной системы.

4 Описание информационной системы персональных данных

4.1 В соответствии с Указом Президента Российской Федерации от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» обработка персональных данных гражданского служащего осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия гражданскому служащему в прохождении государственной гражданской службы Российской Федерации, в обучении и должностном росте, обеспечения личной безопасности гражданского служащего и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества государственного органа, учета результатов исполнения им должностных обязанностей.

4.3 В АИС «___КИАСУО_____» обрабатываются следующие персональные данные о субъектах:

- фамилия, имя, отчество;
- пол;
- гражданство;
- адрес проживания;
- контактный телефон;
- дата и место рождения;
- номер паспорта;
- семейное положение;
- образование;
- ученая степень и звание;
- наличие публикаций;
- знание иностранных языков;

4.3 АИС «__КИАСУО_____» представляет собой клиент-серверное приложение *(краткое описание в нескольких словах)* с централизованным размещением информационных ресурсов и распределенным размещением АРМ пользователей.

5 Перечень угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных

5.1 В соответствии с разделом 4 настоящего документа определен тип АИС «__КИАСУО_____» (далее – ИСПДн) – распределенная ИСПДн, имеющая подключения к сетям связи общего пользования и (или) сетям международного информационного обмена.

5.2 В соответствии с положениями «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» потенциальную опасность нарушения безопасности персональных данных при их обработке в ИСПДн данного типа представляют следующие угрозы:

I Угрозы утечки информации по техническим каналам:

1) угрозы утечки акустической информации;
2) угрозы утечки видовой информации;
3) угрозы утечки информации по каналу ПЭМИН;

II Угрозы НСД к персональным данным:

1) Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):

– угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывод, перехват управления загрузкой;

– 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 текстов в текстовых файлах и т.п.);

– угрозы внедрения вредоносных программ.

2) Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (угрозы удаленного доступа):

– перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации;

– сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей;

– подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа;

– навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

– внедрение ложного объекта сети;

– сетевые атаки типа «Отказ в обслуживании»;

– удаленный запуск приложения в ИСПДн;

– внедрение по сети вредоносных программ;

3) Угрозы физического доступа к элементам ИСПДн:

– хищение элементов ИСПДн, содержащих ПДн;

– хищение отчуждаемых носителей информации, содержащих ПДн;

– вывод из строя элементов ИСПДн;

– внедрение в ИСПДн аппаратных закладок.

Так же следует рассмотреть угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн, а именно:

– утрата паролей доступа к ИСПДн;

– искажение или уничтожение информации в результате ошибок пользователя;

– выход из строя аппаратно-программных средств ИСПДн;

– сбой системы электроснабжения ИСПДн;

– уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами.

5.3 В связи с тем, что в ИСПДн не реализованы функции голосового ввода персональных данных и воспроизведения персональных данных акустическими средствами, угроза утечки акустической информации исключена из дальнейшего рассмотрения.

6. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

6.1 Определение уровня исходной защищенности информационной системы персональных данных

Уровень исходной защищенности ИСПДн определен экспертным методом в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Методика).

Результаты анализа исходной защищенности приведены в таблице 1.

Таблица 1. Анализ исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			+
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования			+
3. По встроенным (легальным) операциям с записями баз персональных данных:			
модификация, передача			+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн		+	
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу данной ИСПДн	+		
6. По уровню (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая часть ПДн		+	
Характеристики ИСПДн по уровням	**14%**	**29%**	**57%**

Таким образом, ИСПДн имеет низкий уровень исходной защищенности (У1 =10), так как не выполняются определенные Методикой условия присвоения уровня исходной защищенности ИСПДн со значением высокий и средний.

6.2 Определение вероятности реализации угроз безопасности персональных данных

Вероятность реализации угроз безопасности персональных данных определена экспертным методом в соответствии с Методикой и на основании результатов обследования ИСПДн.

Результаты определения вероятности реализации угроз приведены в таблице 2.

Таблица 2. Вероятность реализации угроз безопасности персональных данных

Угроза	Вероятность Y2
Угрозы утечки информации по техническим каналам	
Угрозы утечки видовой информации:	
Просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн	5
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн	2
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны	2
Просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн	0
Угрозы утечки информации по каналам ПЭМИН:	
Утечка информации по сетям электропитания ИСПДн	2
Перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами ИСПДн, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	2
Утечка информации из ИСПДн за счет побочного излучения технический средств	0
Преднамеренное электромагнитное воздействие на элементы ИСПДн	2
Угрозы НСД к персональным данным	
Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):	
Перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления НСД к ПДн	5
Вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн	5
Внедрение в ИСПДн вредоносных программ	5
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (угрозы удаленного доступа):	
Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации	10
Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей	5

Угроза	Вероятность Y2
формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей	
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	10
Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	10
Внедрение ложного объекта сети	10
Сетевые атаки типа «Отказ в обслуживании»	5
Удаленный запуск приложения в ИСПДн	10
Внедрение по сети вредоносных программ	5
Угрозы физического доступа к элементам ИСПДн:	
Хищение элементов ИСПДн, содержащих ПДн	5
Хищение отчуждаемых носителей информации, содержащих ПДн	5
Вывод из строя элементов ИСПДн	5
Внедрение в ИСПДн аппаратных закладок	5
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн	
Утрата паролей доступа к ИСПДн	5
Искажение или уничтожение информации в результате ошибок пользователя	5
Выход из строя аппаратно-программных средств ИСПДн	2
Сбой системы электроснабжения ИСПДн	2
Уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами	2

6.3 Определение возможности реализации угроз безопасности персональных данных

Для определения возможности реализации угроз безопасности персональных данных в соответствии с Методикой использованы следующие показатели:

– уровень исходной защищенности ИСПДн (пункт 6.1 настоящей Модели);

– вероятность реализации угроз безопасности персональных данных (пункт 6.2 настоящей Модели).

Результаты определения возможности реализации угроз приведены в таблице 3.

Таблица 3. Возможность реализации угроз безопасности персональных данных

Угроза	Вероятность Y2	Промежуточный расчет Y = (Y1+Y2)/20, где Y1=10	Возможность реализации угрозы
Угрозы утечки информации по техническим каналам			
Угрозы утечки видовой информации:			

Угроза	Вероятность Y2	Промежуточный расчет Y = (Y1+Y2)/20, где Y1=10	Возможность реализации угрозы
Просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн	5	0,75	Высокая
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн	2	0,6	Средняя
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны	2	0,6	Средняя
Просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн	0	0,5	Средняя
Угрозы утечки информации по каналам ПЭМИН:			
Утечка информации по сетям электропитания ИСПДн	2	0,6	Средняя
Перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами ИСПДн, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	2	0,6	Средняя
Утечка информации из ИСПДн за счет побочного излучения технический средств	0	0,5	Средняя
Преднамеренное электромагнитное воздействие на элементы ИСПДн	2	0,6	Средняя
Угрозы НСД к персональным данным			
Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):			
Перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления	5	0,75	Высокая

Угроза	Вероятность Y2	Промежуточный расчет Y = (Y1+Y2)/20, где Y1=10	Возможность реализации угрозы
НСД к ПДн			
Вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн	5	0,75	Высокая
Внедрение в ИСПДн вредоносных программ	5	0,75	Высокая
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (угрозы удаленного доступа):			
Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации	10	1	Очень высокая
Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей	5	0,75	Высокая
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	10	1	Очень высокая
Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	10	1	Очень высокая
Внедрение ложного объекта сети	10	1	Очень высокая
Сетевые атаки типа «Отказ в обслуживании»	5	0,75	Высокая
Удаленный запуск приложения в ИСПДн	10	1	Очень высокая
Внедрение по сети вредоносных программ	5	0,75	Высокая
Угрозы физического доступа к элементам ИСПДн:			
Хищение элементов ИСПДн, содержащих ПДн	5	0,75	Высокая
Хищение отчуждаемых носителей	5	0,75	Высокая

Угроза	Вероятность Y2	Промежуточный расчет Y = (Y1+Y2)/20, где Y1=10	Возможность реализации угрозы
информации, содержащих ПДн			
Вывод из строя элементов ИСПДн	5	0,75	Высокая
Внедрение в ИСПДн аппаратных закладок	5	0,75	Высокая
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн			
Утрата паролей доступа к ИСПДн	5	0,75	Высокая
Искажение или уничтожение информации в результате ошибок пользователя	5	0,75	Высокая
Выход из строя аппаратно-программных средств ИСПДн	2	0,6	Средняя
Сбой системы электроснабжения ИСПДн	2	0,6	Средняя
Уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами	2	0,6	Средняя

6.4 Определение опасности угроз безопасности персональных данных

Определение опасности угроз безопасности персональных данных проведено экспертным методом на основании опроса экспертов (специалистов в области защиты информации) с учетом результатов обследования ИСПДн. Результаты определения опасности угроз приведены в таблице 4.

Таблица 4. Опасность реализации угроз безопасности персональных данных

Угроза	Опасность (ущерб)
Угрозы утечки информации по техническим каналам	
Угрозы утечки видовой информации:	
Просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн	Средняя
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн	Средняя
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны	Средняя
Просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн	Средняя
Угрозы утечки информации по каналам ПЭМИН:	
Утечка информации по сетям электропитания ИСПДн	Низкая
Перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами ИСПДн, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	Низкая
Утечка информации из ИСПДн за счет побочного излучения технический средств	Низкая
Преднамеренное электромагнитное воздействие на элементы ИСПДн	Низкая
Угрозы НСД к персональным данным	
Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):	
Перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления НСД к ПДн	Высокая
Вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн	Высокая
Внедрение в ИСПДн вредоносных программ	Средняя
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (угрозы удаленного доступа):	
Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации	Высокая
Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей	Средняя
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	Высокая
Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Средняя

Угроза	Опасность (ущерб)
Внедрение ложного объекта сети	Высокая
Сетевые атаки типа «Отказ в обслуживании»	Низкая
Удаленный запуск приложения в ИСПДн	Высокая
Внедрение по сети вредоносных программ	Средняя
Угрозы физического доступа к элементам ИСПДн:	
Хищение элементов ИСПДн, содержащих ПДн	Высокая
Хищение отчуждаемых носителей информации, содержащих ПДн	Высокая
Вывод из строя элементов ИСПДн	Средняя
Внедрение в ИСПДн аппаратных закладок	Высокая
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн	
Утрата паролей доступа к ИСПДн	Средняя
Искажение или уничтожение информации в результате ошибок пользователя	Средняя
Выход из строя аппаратно-программных средств ИСПДн	Средняя
Сбой системы электроснабжения ИСПДн	Низкая
Уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами	Средняя

6.5 Определение актуальных угроз безопасности персональных данных

Определение актуальных угроз безопасности персональных данных проведено экспертным методом в соответствии с Методикой. Результаты приведены в таблице 5.

Таблица 5. Определение актуальных угроз нарушения безопасности персональных данных

Угроза	Возможность реализации угрозы	Опасность (ущерб)	Актуальность
Угрозы утечки информации по техническим каналам			
Угрозы утечки акустической информации:			
В ИСПДн не реализованы функции голосового ввода ПДн и воспроизведения ПДн акустическими средствами			Неактуальна
Угрозы утечки видовой информации:			
Просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн	Высокая	Средняя	Актуальная
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн	Средняя	Средняя	Актуальная

Угроза	Возможность реализации угрозы	Опасность (ущерб)	Актуальность
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны	Средняя	Средняя	Актуальная
Просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн	Средняя	Средняя	Актуальная
Угрозы утечки информации по каналам ПЭМИН:			
Утечка информации по сетям электропитания ИСПДн	Средняя	Низкая	Неактуальная
Перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами ИСПДн, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	Средняя	Низкая	Неактуальная
Утечка информации из ИСПДн за счет побочного излучения технический средств	Средняя	Низкая	Неактуальная
Преднамеренное электромагнитное воздействие на элементы ИСПДн	Средняя	Низкая	Неактуальная
Угрозы НСД к персональным данным			
Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):			
Перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления НСД к ПДн	Высокая	Высокая	Актуальная
Вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн	Высокая	Высокая	Актуальная
Внедрение в ИСПДн вредоносных программ	Высокая	Средняя	Актуальная

Угроза	Возможность реализации угрозы	Опасность (ущерб)	Актуальность
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (угрозы удаленного доступа):			
Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации	Очень высокая	Высокая	Актуальная
Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей	Высокая	Средняя	Актуальная
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	Очень высокая	Высокая	Актуальная
Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Очень высокая	Средняя	Актуальная
Внедрение ложного объекта сети	Очень высокая	Высокая	Актуальная
Сетевые атаки типа «Отказ в обслуживании»	Высокая	Низкая	Актуальная
Удаленный запуск приложения в ИСПДн	Очень высокая	Высокая	Актуальная
Внедрение по сети вредоносных программ	Высокая	Средняя	Актуальная
Угрозы физического доступа к элементам ИСПДн:			
Хищение элементов ИСПДн, содержащих ПДн	Высокая	Высокая	Актуальная
Хищение отчуждаемых носителей информации, содержащих ПДн	Высокая	Высокая	Актуальная
Вывод из строя элементов ИСПДн	Высокая	Средняя	Актуальная
Внедрение в ИСПДн аппаратных закладок	Высокая	Высокая	Актуальная
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн			
Утрата паролей доступа к ИСПДн	Высокая	Средняя	Актуальная

Угроза	Возможность реализации угрозы	Опасность (ущерб)	Актуальность
Искажение или уничтожение информации в результате ошибок пользователя	Высокая	Средняя	Актуальная
Выход из строя аппаратно-программных средств ИСПДн	Средняя	Средняя	Актуальная
Сбой системы электроснабжения ИСПДн	Средняя	Низкая	Неактуальная
Уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами	Высокая	Средняя	Актуальная

Таким образом, в отношении персональных данных, обрабатываемых в автоматизированной информационной системе актуальными являются следующие угрозы:

- просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн;
- просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн;
- просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны;
- просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн;
- перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления НСД к ПДн;
- вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн;
- внедрение в ИСПДн вредоносных программ;
- перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации;
- сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей;
- подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа;

- навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;
- внедрение ложного объекта сети;
- сетевые атаки типа «Отказ в обслуживании»;
- удаленный запуск приложения в ИСПДн;
- внедрение по сети вредоносных программ;
- хищение элементов ИСПДн, содержащих ПДн;
- хищение отчуждаемых носителей информации, содержащих ПДн;
- вывод из строя элементов ИСПДн;
- внедрение в ИСПДн аппаратных закладок;
- утрата паролей доступа к ИСПДн;
- искажение или уничтожение информации в результате ошибок пользователя;
- выход из строя аппаратно-программных средств ИСПДн;
- уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами.

7 Модель угроз безопасности персональных данных при их обработке в автоматизированной информационной системе персональных данных«_____»

Наименование угрозы	**Вероятность реализации угрозы (Y_2)**	**Промежуточный расчет $Y=(Y_1+Y_2)/20$, где $Y_1=10$**	**Возможность реализации угрозы (Y)**	**Опасность угрозы**	**Актуальность угрозы**	**Организационно-технические меры по защите ИСПДн от угрозы**
Угрозы от утечки по техническим каналам						
Угрозы утечки видовой информации:						
Просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн	5	0,75	высокая	средняя	актуальная	Организация пропускного режима. Автоматическая блокировка экрана при отсутствии пользователя ИСПДн на рабочем месте. Включение требования о недопустимости просмотра информации посторонними лицами в инструкцию пользователя ИСПДн.
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн	2	0,6	средняя	средняя	актуальная	Организация пропускного режима. Автоматическая блокировка экрана при отсутствии пользователя ИСПДн на рабочем месте. Контроль доступа в помещения, где ведется обработка ПДн. Включение требования о недопустимости просмотра информации посторонними лицами в инструкцию пользователя ИСПДн.

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Промежуточный расчет $Y=(Y_1+Y_2)/20$, где $Y_1=10$	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Организационно-технические меры по защите ИСПДн от угрозы
Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны	2	0,6	средняя	средняя	актуальная	Установка на окна помещений, в которых ведется обработка ПД, жалюзи или штор. Размещение помещений, содержащих ИСПДн, на удалении от границ контролируемой зоны.
Просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн	0	0,5	средняя	средняя	актуальная	Организация пропускного режима. Контроль доступа в помещения, где ведется обработка ПДн.
Угрозы несанкционированного доступа (далее - НСД) к информации						
Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):						
Перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления НСД к ПДн	5	0,75	высокая	высокая	актуальная	Запрет загрузки АРМ с отчуждаемых носителей информации. Контроль доступа в помещения, где ведется обработка ПДн.

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Промежуточный расчет $Y=(Y_1+Y_2)/20$, где $Y_1=10$	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Организационно-технические меры по защите ИСПДн от угрозы
Вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн	5	0,75	высокая	высокая	актуальная	Предоставление персоналу ИСПДн привилегий, минимально необходимых для выполнения ими своих функциональных обязанностей.
Внедрение в ИСПДн вредоносных программ	5	0,75	высокая	средняя	актуальная	Использование на серверах и АРМ, входящих в состав ИСПДн, антивирусного ПО. Выполнение регулярного обновления ПО АРМ и серверов ИСПДн. Настройка антивирусного ПО на проверку подключаемых отчуждаемых носителей информации.
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (угрозы удаленного доступа):						
Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации	10	1	очень высокая	высокая	актуальная	Сегментирование ЛВС с помощью виртуальных локальных сетей. Запрет установки ПО, не связанного с исполнением служебных обязанностей. Регулярный контроль со стороны работников, ответственных за обеспечение безопасности ПДн при их обработке в ИСПДн, прав доступа пользователей к АРМ и установленного на них ПО. Предоставление персоналу

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Промежуточный расчет $Y=(Y_1+Y_2)/20$, где $Y_1=10$	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Организационно-технические меры по защите ИСПДн от угрозы
						ИСПДн привилегий, минимально необходимых для выполнения ими своих функциональных обязанностей.
Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей	5	0,75	высокая	средняя	актуальная	Сегментирование ЛВС с помощью виртуальных локальных сетей. Использование систем обнаружения и предотвращения вторжений. Предоставление персоналу ИСПДн привилегий, минимально необходимых для выполнения ими своих функциональных обязанностей.
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	10	1	очень высокая	высокая	актуальная	Сегментирование ЛВС с помощью виртуальных локальных сетей.
Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	10	1	очень высокая	средняя	актуальная	Сегментирование ЛВС с помощью виртуальных локальных сетей.
Внедрение ложного объекта сети	10	1	очень высокая	высокая	актуальная	Сегментирование ЛВС с помощью виртуальных локальных сетей.

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Промежуточный расчет $Y=(Y_1+Y_2)/20$, где $Y_1=10$	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Организационно-технические меры по защите ИСПДн от угрозы
Сетевые атаки типа «Отказ в обслуживании»	5	0,75	высокая	низкая	актуальная	Сегментирование ЛВС с помощью виртуальных локальных сетей. Использование систем обнаружения и предотвращения вторжений.
Удаленный запуск приложения в ИСПДн	10	1	очень высокая	высокая	актуальная	Сегментирование ЛВС с помощью виртуальных локальных сетей. Выполнение регулярного обновления ПО с помощью ПО ИСПДн. Использование систем обнаружения и предотвращения вторжений.
Внедрение по сети вредоносных программ	5	0,75	высокая	средняя	актуальная	Использование на серверах и АРМ входящих в состав ИСПДн антивирусного ПО. Выполнение регулярного обновления ПО АРМ и серверов ИСПДн.
Угрозы физического доступа к элементам ИСПДн:						
Хищение элементов ИСПДн, содержащих ПДн	5	0,75	высокая	высокая	актуальная	Организация пропускного режима. Контроль доступа в помещения, где ведется обработка ПДн.
Хищение отчуждаемых носителей информации, содержащих ПДн	5	0,75	высокая	высокая	актуальная	Организация пропускного режима. Контроль доступа в помещения, где ведется обработка ПДн. Вменение персоналу ИСПДн

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Промежуточный расчет $Y=(Y_1+Y_2)/20$, где $Y_1=10$	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Организационно-технические меры по защите ИСПДн от угрозы
						обязанности обеспечения сохранности отчуждаемых носителей информации, содержащих ПДн.
Вывод из строя элементов ИСПДн	5	0,75	высокая	средняя	актуальная	Организация пропускного режима. Контроль доступа в помещения, где ведется обработка ПДн. Размещение помещений, содержащих ИСПДн, в пределах контролируемой зоны.
Внедрение в ИСПДн аппаратных закладок	5	0,75	высокая	высокая	актуальная	Организация пропускного режима. Контроль доступа в помещения, где ведется обработка ПДн. Организация выполнения работ технического обслуживания, выполняемых работниками сторонних организаций, в присутствии работников организации. Включение требования по информационной безопасности в договоры и контракты на проведение работ и оказание услуг. Выбор в качестве исполнителей работ и поставщиков услуг организаций, прошедших сертификацию. Заключение соглашений о

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Промежуточный расчет $Y=(Y_1+Y_2)/20$, где $Y_1=10$	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Организационно-технические меры по защите ИСПДн от угрозы
						конфиденциальности со сторонними организациями, выполняющими работы или оказывающими услуги.
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн:						
Утрата паролей доступа к ИСПДн	5	0,75	высокая	средняя	актуальная	Вменение персоналу ИСПДн обязанности обеспечения сохранности паролей. Определение парольной политики
Искажение или уничтожение информации в результате ошибок пользователя	5	0,75	высокая	средняя	актуальная	Контроль вводимых данных. Предоставление персоналу ИСПДн привилегий, минимально необходимых для выполнения ими своих функциональных обязанностей
Выход из строя аппаратно-программных средств ИСПДн	2	0,6	средняя	средняя	актуальная	Резервирование аппаратных ресурсов ИСПДн.
Уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами	2	0,6	средняя	средняя	актуальная	Резервное копирование данных ИСПДн. Хранение резервных копий отдельно от элементов ИСПДн, содержащих резервируемые данные. Использование в серверных помещениях средств обнаружения возгорания и систем пожаротушения.