МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ "НОВОТОРЪЯЛЬСКИЙ ЦЕНТР ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ"

Приложение № 12 к приказу
№ 273 от 08.09.2023 г.

АКТ
Результаты опроса о частоте (вероятности) реализации угрозы и опасности угрозы по видам угроз безопасности персональных данных при их обработке в ИСПДн «Кадры»

В соответствии с требованиями Постановления Правительства Российской Федерации от 1 ноября 2012г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»и методическим рекомендациями Управления ФСТЭК России по ПФО по разработке частных моделей угроз безопасности персональных данных, комиссией, назначенной приказом№ 241от 08.09.2023 г.в составе:

Председатель комиссии:
Торощина Ольга Валерьевна -директор;

Члены комиссии:
Мартынова Маргарита Анатольевна -заместитель директора по учебной работе;

Зуйкова Вероника Александровна -методист (руководитель МОЦ);

проведено изучение вероятности реализации угроз и опасности угроз по видам угроз безопасности персональных данных при их обработке в информационных системах персональных данных «Кадры»МБУДО «Новоторъяльский ЦДО»(далее − ИСПДн). Результаты по видам угроз безопасности персональных данных (далее − ПДн) для рассматриваемой ИСПДн отображены в Таблице 1.

Таблица 1.

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ			
Угрозы утечки акустической (речевой) информации			
Непосредственное прослушивание ПДн акустической речевой информации физическими лицами при посещении ими служебных помещений	Низкая	Маловероятно	Функций голосового ввода персональных данных и функций воспроизведения персональных данных акустическими средствами в данной ИСПДн нет
Перехват акустических сигналов с использованием направленных микрофонов (дальность перехвата до 200 м)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Перехват акустических сигналов с использованием ненаправленных микрофонов (дальность перехвата до 10 м)	Низкая	Маловероятно	
Перехват акустических сигналов с использованием акустооптических модуляторов (оптические микрофоны, дальность перехвата - в поле акустического сигнала)	Низкая	Маловероятно	

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Перехват вибрационных сигналов с использованием оптико-электронной аппаратуры дистанционного лазерного зондирования (лазерные микрофоны, дальность перехвата до 500 м)	Низкая	Маловероятно	
Перехват вибрационных сигналов с использованием вибродатчиков (контактные микрофоны, дальность перехвата до 10 м)	Низкая	Маловероятно	
Перехват электрических сигналов, возникающих в результате «микрофонного эффекта» в технических средствах обработки ПДн и ВТСС с использованием средств съема электрических сигналов с гальваническим подключением (дальность перехвата до 300 м)	Низкая	Маловероятно	
Перехват радиоизлучений, модулированных информативным сигналом, возникающих при ВЧ-облучении технических средств обработки ПДн и ВТСС с использованием ВЧ-генераторов и средств съема электрических сигналов с гальваническим подключением (ВЧ-навязывание, дальность перехвата до 300 м)	Низкая	Маловероятно	
Перехват радиоизлучений, модулированных информативным сигналом, возникающих при ВЧ-облучении технических средств обработки ПДн и ВТСС с использованием ВЧ-генераторов и приемников электромагнитного излучения (ВЧ-облучение, до 1000 м)	Низкая	Маловероятно	
Угрозы утечки видовой информации			
Непосредственный просмотр ПДн с экранов дисплеев и других средств отображения графической, видео- и буквенно-цифровой информации физическими лицами при посещении ими служебных помещений	Низкая	Высокая вероятность	Помещения, где расположена ИСПДн, могут посещаются сотрудниками, не допущенными к ИСПДн
Просмотр (регистрация) ПДн с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации на расстоянии прямой видимости из-за пределов служебных помещений с использованием оптических (оптикоэлектронных) средств	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Просмотр (регистрация) ПДн с помощью специальных электронных устройств съема, внедренных в служебных помещениях (видеозакладки) или скрытно используемых физическими лицами при посещении ими служебных помещений	Низкая	Маловероятно	
Угрозы утечки информации по каналу ПЭМИН			
Перехват ПДн техническими средствами побочных электромагнитных излучений информативных сигналов от технических средств и линий передачи информации с использованием портативных сканерных приемников, цифровых анализаторов спектра, селективных микровольтметров и специальных программно-аппаратных комплексов (дальность перехвата до 1000 м)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Перехват ПДн техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы служебных помещений с использованием токосъемников (дальность перехвата до 300 м)	Низкая	Маловероятно	
Перехват ПДн техническими средствами радиоизлучений, модулированных информативным сигналом, возникающих в результате работы различных генераторов в составе ИСПДн или в результате паразитной генерации в узлах (элементах) технических средств с использованием портативных сканерных приемников, цифровых анализаторов спектра, селективных микровольтметров и специальных программно-аппаратных комплексов (дальность перехвата до 1000 м)	Низкая	Маловероятно	
Перехват ПДн техническими средствами радиоизлучений, формируемых за счет высокочастотного облучения технических средств ИСПДн с использованием портативных сканерных приемников, цифровых анализаторов	Низкая	Маловероятно	
спектра, селективных микровольтметров и специальных программно-аппаратных комплексов (дальность перехвата до 1000 м)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации и высокой стоимости необходимой техники
Перехват ПДн техническими средствами оптического излучения с боковой поверхности оптического волокна в волоконно-оптической системе передачи данных	Низкая	Маловероятно	

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Перехват ПДн с применением электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн («аппаратурные закладки»)	Низкая	Маловероятно	
УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ			
Угрозы непосредственного доступа			
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой			
Получение несанкционированного доступа к настройкам конфигурации компьютера (BIOS):			
В связи с отсутствием аутентификации пользователей компьютеров до загрузки ОС (паролей BIOS или дополнительных аппаратных средств аутентификации);	Средняя	Средняя	Необходима установка паролей на BIOS АРМ ИСПДн
В связи с неумышленным разглашением паролей BIOS или дополнительных аппаратных средств аутентификации (записывание в доступном для нарушителя месте: на бумаге, клавиатуре и т.п.);	Низкая	Низкая	Регулируется организационными мерами (Инструкция администратора)
Путем подбора пароля BIOS (или дополнительных аппаратных средств аутентификации);	Низкая	Низкая	Необходима установка паролей на BIOS АРМ ИСПДн. Применение пароля условно-постоянного действия длиной не менее 6 буквенно-цифровых символов
Путем вскрытия корпуса компьютера и аппаратного сброса пароля BIOS;	Низкая	Низкая	Опечатывание корпуса, применение технических средств защиты от несанкционированного вскрытия системного блока
Путем использования технологического пароля BIOS;	Низкая	Низкая	Установка специализированного ПО от производителя BIOS для смены технологического пароля, обновление версии BIOS
Путем внедрения аппаратного "клавиатурного шпиона"	Низкая	Низкая	Вскрытие клавиатуры и ее проверка на предмет наличия посторонних электронных узлов с последующим пломбированием корпуса клавиатуры при помощи пломбира или стикера, проверка на наличие посторонних устройств, включенных в разрыв кабеля клавиатуры, расположенных рядом с ним или непосредственно на нем.
Загрузка сторонней ОС с внешнего носителя (для обхода средств защиты и разграничения доступа к ресурсам компьютера, реализованного на уровне ОС)	Низкая	Средняя	Необходимо установить запрет загрузки с внешних носителей в BIOS
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, с применением специальных программ для осуществления НСД			
Предоставление пользователям прав доступа (в том числе по видам доступа) к ПДн и другим ресурсам ИСПДн сверх необходимого для работы	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Неумышленное (случайное) копирование доступных ПДн на неучтённые (в том числе отчуждаемые) носители, в том числе печать неучтённых копий документов с ПДн	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения. Необходимо вести учет носителей ПДн.
Преднамеренное копирование доступных ПДн на неучтённые (в том числе отчуждаемые) носители в том числе печать неучтённых копий документов с ПДн на принтерах	Низкая	Низкая	Регулируется организационными мерами (Положение о защите персональных данных). Необходимо вести учет носителей ПДн.
Неумышленная (случайная) отправка ПДн по электронной почте	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения.
Преднамеренная отправка ПДн по электронной почте	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения.
Неумышленная (случайная) модификация (искажение) доступных ПДн	Низкая	Низкая	Осуществляется резервное копирование базы данных ИСПДн
Преднамеренная модификация (искажение) доступных ПДн	Низкая	Высокая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения. Необходимо осуществлять резервное копирование базы данных ИСПДн
Неумышленное (случайное) добавление (фальсификация) ПДн	Низкая	Низкая	Осуществляется резервное копирование базы данных ИСПДн
Преднамеренное добавление (фальсификация) ПДн	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения. Необходимо осуществлять резервное копирование базы данных ИСПДн
Неумышленное (случайное) уничтожение доступных ПДн (записей, файлов, форматирование диска)	Низкая	Низкая	Осуществляется резервное копирование базы данных ИСПДн
Преднамеренное уничтожение доступных ПДн (записей, файлов, форматирование диска)	Низкая	Низкая	Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения. Необходимо осуществлять резервное копирование базы данных ИСПДн
Разглашение (например, при разговорах, записывание на бумаге и т.п.) пользовательских имён и паролей	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Использование для входа в систему чужих идентификаторов и паролей	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Использование оборудования, оставленного без присмотра, незаблокированных рабочих станций	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Запуск сторонних программ (технологических, инструментальных и т.п.)	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Изменение настроек и режимов работы ПО, модификация ПО (удаление, искажение или подмена программных компонентов ИСПДн или СЗИ) (преднамеренное или случайное)	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Подключение к ИСПДн стороннего оборудования (компьютеров, КПК, смартфонов, телефонов, фотоаппаратов, видеокамер, USB-дисков, флэш-дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи)	Низкая	Средняя	Рекомендуется приобретение, установка и настройка лицензионного антивирусного ПО на все АРМ, необходимо постоянное обновление вирусных баз, регулируется организационно-контрольными мерами. Требуется установка СЗИ от НСД
Нарушение работоспособности технических средств	Низкая	Низкая	Осуществляется резервное копирование базы данных ИСПДн
Вмешательство в работу (нарушение правил использования) средств защиты	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Несанкционированное изменение конфигурационных файлов ПО (настроек экрана, сети, прикладных программ)	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Установка программных "клавиатурных шпионов"	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Применение специально созданных для повышения своих прав и привилегий и выполнения НСД программ	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Использование нетрадиционных каналов (стеганографии) инсайдером для передачи ПДн	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации в связи с необходимостью целенаправленного привлечения квалифицированных специалистов в области стеганографии
Удаление или искажение регистрационных данных СЗИ (преднамеренное или случайное)	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Несанкционированный доступ к ПДн в бумажном виде	Низкая	Низкая	Регулируется организационными мерами (Инструкция пользователя)
Ошибки при разработке программного обеспечения ИСПДн (в том числе СЗИ)	Низкая	Маловероятно	Используется только лицензионное ПО

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Осуществление неавторизованных действий в серверном помещении	Низкая	Низкая	Выделенное серверное помещение отсутствует. Но доступ в помещение, где расположены сервера ИСПДн, осуществляется только в присутствии администратора ИСПДн
Ошибки при обслуживании серверного оборудования и проведении операций по обслуживанию прикладных систем, либо при проведении установочных работ	Низкая	Низкая	Имеется договора с квалифицированным системным администратором
Ошибки при доработке программного обеспечения ИСПДн (в том числе СЗИ)	Низкая	Маловероятно	Используется только лицензионное ПО.
Хищение, утрата резервных копий носителей ПДн	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция администратора).
Нарушение порядка резервного копирования ПДн	Средняя	Низкая	
Утеря или кража оборудования распределённой ИСПДн (в том числе резервных носителей информации) при транспортировке	Низкая	Маловероятно	ИСПДн не является распределенной
Доступ к информации ИСПДн, выходящей за пределы контролируемой зоны вследствие списания (утилизации) носителей информации, содержащих ПДн	Низкая	Низкая	Регулируется организационно-контрольными мерами (Положение о защите персональных данных)
Угрозы внедрения вредоносных программ (локально)			
Запись кода вредоносного ПО в код других программ с целью получения управления при запуске зараженных файлов, создание файлов-двойников для легального ПО (классические вирусы)	Средняя	Средняя	Используется лицензионное антивирусное ПО. Необходимо постоянное обновление вирусных баз. Требуется использование сертифицированных межсетевых экранов
Передача вредоносной программой своего кода на удаленный сервер или рабочую станцию (сетевые черви)	Средняя	Средняя	
Перебор паролей, демонстрация использования недекларированных возможностей программного и аппаратно-программного обеспечения ИСПДн, демонстрация уязвимостей ИСПДн (другие вредоносные программы, предназначенные для осуществления НСД)	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Преднамеренное внесение вредоносных кодов в программы при их разработке (программные закладки)	Низкая	Маловероятно	Используется только лицензионное ПО. При построении СЗПДн необходимо использовать только сертифицированные СЗИ
Преднамеренное внедрение вредоносной программы	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя). Пользователи ИСПДн официально предупреждены о необходимости соблюдения конфиденциальности ПДн и об ответственности за допущенные нарушения

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Проникновение на рабочую станцию вредоносной программы из локальной сети вследствие отключения пользователями средств антивирусной защиты	Средняя	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя) и локальной политикой безопасности АРМ
Угрозы удаленного доступа			
Анализ сетевого трафика с перехватом информации, передаваемой по локальной сети, а также во внешние сети и принимаемой из внешних сетей с помощью анализаторов пакетов ("сниффферы")			
Перехват идентификаторов и паролей пользователей для последующего осуществления несанкционированного доступа к объектам сети	Средняя	Маловероятно	Требуется использование сертифицированных межсетевых экранов
Перехват конфиденциальной информации, передаваемой по сети в открытом или слабо защищённом виде	Низкая	Низкая	Используются сертифицированные СКЗИ. Рекомендуется разработать порядок применения СКЗИ в ИСПДн
Сканирование сети с целью сбора информации об объектах сети, выявления используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов	Низкая	Низкая	Требуется использование сертифицированных межсетевых экранов
Выявление паролей			
Подбор пароля путем перебора с помощью специального программного обеспечения	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации. Политика формирования и смены паролей определена Инструкцией администратора
Перехват пароля с помощью специального программного обеспечения	Низкая	Маловероятно	
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	Низкая	Маловероятно	
Навязывание ложного маршрута сети путем несанкционированного использования протоколов маршрутизации			
Атаки на DNS	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации в связи с необходимостью целенаправленного привлечения высококвалифицированных специалистов в области сетевых информационных технологий
Атаки на ARP	Низкая	Маловероятно	
Атака "человек посередине"	Низкая	Маловероятно	
Внедрение ложного объекта сети путем использования недостатков алгоритмов удаленного поиска			
Перехват нарушителем поискового запроса и выдача на него ложного ответа, использование которого приведет к требуемому изменению маршрута	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации в связи с необходимостью целенаправленного привлечения высококвалифицированных специалистов в области сетевых информационных технологий
Внедрение ложного ARP сервера	Низкая	Маловероятно	
Внедрение ложного DNS сервера	Низкая	Маловероятно	

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Реализация отказа в обслуживании			
Привлечение части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов в целях реализации скрытого отказа в обслуживании	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за сложности ее реализации в связи с необходимостью целенаправленного привлечения высококвалифицированных специалистов в области сетевых информационных технологий
Исчерпание ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание) в целях реализации явного отказа в обслуживании	Низкая	Маловероятно	
Нарушение логической связности между атрибутами, данными, объектами путем передачи нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации с целью реализации явного отказа в обслуживании	Низкая	Маловероятно	
Передача пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер с целью реализации явного отказа в обслуживании	Низкая	Маловероятно	
Удалённый запуск приложений			
Активизация распространяемых злоумышленниками файлов, содержащих несанкционированный исполняемый код, при случайном обращении к ним пользователя ("спам" - при использовании электронной почты, "фишинг" - при использовании Интернета)	Средняя	Низкая	Используется лицензионное антивирусное ПО. Необходимо постоянное обновление вирусных баз.
Переполнение буфера приложений-серверов путем использования недостатков программ, реализующих сетевые сервисы (реализация переполнения буфера и настройка системных регистров, позволяющая переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера)	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за низкой коммерческой ценности имеющейся в ИСПДн информации

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Использование скрытых программных и аппаратных закладок либо используемых штатных средств управления и администрирования компьютерных сетей для получения удаленного контроля над станцией в сети	Низкая	Маловероятно	Члены комиссии склоняются к маловероятности такой угрозы из-за низкой коммерческой ценности имеющейся в ИСПДн информации
Угрозы внедрения вредоносных программ (по сети)	Средняя	Средняя	Используется лицензионное антивирусное ПО.Необходимо постоянное обновление вирусных баз, необходимо использование сертифицированных межсетевых экранов
УГРОЗЫ, НЕ ЯВЛЯЮЩИЕСЯ АТАКОЙ (НЕПРЕДНАМЕРЕННЫЕ УГРОЗЫ)			
Угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления			
Землетрясение	Низкая	Маловероятно	Географическое местоположение организации практически исключает возможность стихийных бедствий
Наводнение	Низкая	Маловероятно	
Ураган	Низкая	Маловероятно	
Угрозы социально–политического характера			
Забастовка	Низкая	Маловероятно	Социальная обстановка в организации спокойная
Саботаж	Низкая	Маловероятно	
Локальный конфликт	Низкая	Маловероятно	
Террористический акт (взрывы, угрозы взрыва, захваты...)	Низкая	Маловероятно	Организация находится вне «горячих точек»
Ошибочные действия и (или) нарушения тех или иных требований лицами, санкционированно взаимодействующими с возможными объектами угроз			
Непредумышленное искажение или удаление программных компонентов АСЗИ	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция пользователя) и локальной политикой безопасности АРМ
Внедрение и использование неучтенных программ	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Игнорирование организационных ограничений (установленных правил) при работе с ресурсами АСЗИ, включая средства защиты информации			
Нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации)	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя и Инструкция администратора).

Вид угрозы	Опасность (ущерб)	Вероятность	Комментарии
Настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов	Низкая	Маловероятно	Регулируется организационно-контрольными мерами (Инструкция администратора)
Несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа	Низкая	Низкая	Регулируется организационно-контрольными мерами (Инструкция пользователя)
Угрозы техногенного характера			
Неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.	Средняя	Низкая	Регулярно проводятся мероприятия по пожарной безопасности, осуществляются текущие строительные, электрические и санитарно-технические ремонтные работы в помещениях организаций
Помехи и наводки, приводящие к сбоям в работе аппаратных средств	Средняя	Маловероятно	
Возгорание оборудования ИСПДн	Средняя	Маловероятно	
Затопление оборудования ИСПДн	Средняя	Маловероятно	

Выводы комиссии:

1. На основании экспертной оценки членов комиссии утвердить вероятности реализации угроз и показатели опасности угроз безопасности персональных данных, обрабатываемых в ИСПДн «Кадры» по видам угроз безопасности в соответствии с данными, указанными в Таблице 1.
2. Использовать сведения, указанные в Таблице 1, для определения актуальных угроз безопасности персональных данных для ИСПДн.

Председатель комиссии: _____ Торощина Ольга Валерьевна

Члены комиссии: _____ Мартынова Маргарита Анатольевна
_____ Зуйкова Вероника Александровна