Муниципальное бюджетное общеобразовательное учреждение
«Кезская средняя общеобразовательная школа №2»
Кезского района Удмуртской Республики

ПРИКАЗ

31 августа 2022 года **№ 300**

п. Кез

Об утверждении Положения об обработке персональных данных работников, обучающихся и их родителей (законных представителей) МБОУ «Кезская СОШ №2»

С целью организации обработки персональных данных в МБОУ «Кезская СОШ №2» в соответствии с пунктом 1 части 1 статьи 18.1 и части 1 статьи 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Требованиями к защите персональных данных при обработке в информационных системах персональных данных, утвержденными постановлением Правительства от 01.11.2012 № 1119

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке персональных данных работников, обучающихся и их родителей (законных представителей) МБОУ «Кезская СОШ №2» (Приложение 1)
2. Назначить ответственным за организацию обработки персональных данных учителя информатики Бузмакову Евгению Михайловну.
3. Утвердить инструкцию ответственного за организацию обработки персональных данных (Приложение 2).
4. Утвердить список должностных лиц, допущенных к обработке персональных данных (Приложение 3).
5. Утвердить Инструкция пользователя информационных систем персональных данных (Приложение 4).
6. Утвердить Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных (Приложение 5).
7. Утвердить Инструкцию по порядку учета, хранения съемных носителей персональных данных (Приложение 6).
8. Контроль за исполнением приказа оставляю за собой.

Директор школы Юферева Е.В.

Приложение № 1
к приказу № 300 от 31.08.2022г.

ПОЛОЖЕНИЕ
об обработке персональных данных работников, обучающихся и их родителей (законных представителей) МБОУ «Кезская СОШ №2»

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных работников, обучающихся и их родителей (законных представителей) (далее − Положение) муниципального бюджетного общеобразовательного учреждения «Кезская средняя общеобразовательная школа «2» (далее − Школа) разработано на основании:

− статьи 24 Конституции Российской Федерации;

− главы 14 Трудового Кодекса Российской Федерации;

− Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информатизации и защите информации»,

− Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;

− Федерального закона РФ от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Правил внутреннего трудового распорядка.

1.2. Цель разработки Положения – определение порядка обработки, систематизации, использования, хранения и передачи сведений, составляющих персональные данные; обеспечение защиты прав и свобод работников учреждения, учащихся и их родителей (законных представителей) при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников учреждения, учащихся и их родителей (законных представителей) за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Персональные данные относятся к категории конфиденциальной информации.

1.4. Все работники Школы, в соответствии со своими полномочиями владеющие информацией, относящейся к персональным данным, о сотрудниках, учащихся и их родителях (законных представителях), получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.5. Порядок ввода в действие и изменения Положения.

1.5.1. Все изменения в Положение вносятся приказом директора учреждения. До внесения изменений в настоящее Положение в связи с изменением законодательства, регламентирующего вопросы обработки персональных данных, настоящее Положение действует в части, не противоречащей законодательству.

1.5.2. Все работники Школы должны быть ознакомлены с настоящим Положением под роспись.

1.6. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75-летнего срока их хранения, если иное не определено законом.

2. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

- персональные данные – любая информация, относящаяся к прямо или косвенно

определенному или определяемому физическому лицу (субъекту персональных данных):

работнику, учащемуся и его родителям (законным представителям), в том числе их фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая учреждению в связи с трудовыми отношениями с работником, образовательными отношениями – учащимся, его родителем (законным представителем);

- оператор – юридическое лицо (Школа), самостоятельно организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели

обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых и использованием средств автоматизации или без

использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных работников, учащихся и их родителей (законных представителей);

- конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным

работников, учащихся и их родителей (законных представителей) требование не раскрывать третьим лицам и не распространять персональные данные без согласия работника или родителя (законного представителя) или иного законного основания;

- распространение персональных данных – действия, направленные на раскрытие персональных данных работников, учащихся и их родителей (законных представителей)

неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- использование персональных данных – действия (операции) с персональными данными, совершаемые должностным лицом в целях принятия решений или совершения

иных действий, порождающих юридические последствия в отношении работников, учащихся и их родителей (законных представителей), либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

– блокирование персональных данных – временное прекращение обработки персональных данных работников, учащихся и их родителей (законных представителей) (за исключением случаев, если обработка необходима для уточнения персональных данных);

– уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носителя персональных данных работников, учащихся и их родителей (законных представителей);

- обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить

принадлежность персональных данных конкретному работнику, учащемуся и его родителям (законным представителям);

- общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника, законного

представителя учащегося или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

- информация – сведения (сообщения, данные) независимо от формы их представления;
- документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника при его приеме, переводе и увольнении.

2.2.1. Информация, представляемая работником при поступлении на работу в учреждение, должна иметь документальную форму.

При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

− паспорт или иной документ, удостоверяющий личность;

− трудовую книжку и (или) сведения о трудовой деятельности, за исключением случаев, если трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

− документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета;

− документы воинского учета – для военнообязанных и лиц, подлежащих призыву на военную службу;

− документ об образовании и/или о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;

− справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям, выданную в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, – при поступлении на работу, связанную с деятельностью, к осуществлению которой в соответствии с настоящим Кодексом, иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию.

Свидетельство о присвоении ИНН работник представляет при его наличии.

2.2.2. При оформлении работника на работу (после заключения трудового договора) заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника: Ф.И.О., дата и место рождения, гражданство, уровень знания иностранных языков, сведения об образовании, профессии, стаже работы, семейном положении, данные паспорта, адрес регистрации, адрес проживания, контактный телефон); ИНН, номер документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета; сведения о воинском учете; информация о трудовой деятельности; результаты аттестаций работника (дата аттестации, дата и номер протокола, решение аттестационной комиссии); данные о повышении квалификации; сведения о профессиональной переподготовке; данные о наградах, поощрениях; информация о предоставляемых отпусках; право работника на социальные льготы; дополнительные сведения: группа инвалидности, наличие водительского удостоверения; основание расторжения трудового договора.

2.2.3. В Школе создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.2.3.1. Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; подлинники и копии приказов по личному составу; личные

дела и трудовые книжки работников; дела, содержащие основания к приказам по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых администрации учреждения, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления образованием и другие учреждения).

2.2.3.2. Документация по организации работы (положения, должностные инструкции, приказы, распоряжения администрации); документы по планированию, учету, анализу и отчетности в части работы с персоналом учреждения.

2.3. Информация, представляемая родителями (законными представителями) при поступлении учащегося в учреждение, должна иметь документальную форму. При поступлении учащегося в учреждение родители (законные представители) предъявляют учреждению:

- копию документа, удостоверяющего личность законного представителя;
- копию свидетельства о рождении ребенка или документа, подтверждающего родство заявителя;
- медицинские документы о состоянии здоровья (медицинская карта Ф-26, карта профпрививок Ф-63);
- сведения о родителях (законных представителях);
- справку о месте жительства;
- контактные данные;
- иные сведения, относящиеся к персональным данным учащегося.

Родители (законные представители) детей, являющихся иностранными гражданами или лицами без гражданства, дополнительно предъявляют документ, подтверждающий родство заявителя (или законность представления прав ребенка), и документ, подтверждающий право заявителя на пребывание в Российской Федерации.

Иностранные граждане и лица без гражданства все документы представляют на русском языке или с заверенным в установленном порядке переводом на русский язык.

2.4. Персональные данные учащихся содержатся в их личных делах.

3. Сбор и обработка персональных данных

3.1. Порядок получения персональных данных.

3.1.1. Все персональные данные работника учреждения и родителя (законного представителя) учащегося следует получать непосредственно у работника и родителя (законного представителя). Персональные данные учащихся следует получать у родителей (законных представителей). Если персональные данные возможно получить только у третьей стороны, то работник, родители (законные представители) должны быть уведомлены об этом заранее и от них должно быть получено письменное согласие. Должностное лицо учреждения должно сообщить работнику, родителям (законным представителям) о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.1.2. Учреждение не имеет права получать, обрабатывать и приобщать к личному делу работника и учащегося не установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и Трудовым кодексом Российской Федерации персональные данные об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах. В

случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации учреждение вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.2. Порядок обработки персональных данных

3.2.1. Обработка персональных данных осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия работникам и учащимся в прохождении обучения, их карьерном росте, обеспечения их личной безопасности и членов их семей, а также в целях обеспечения сохранности принадлежащего им имущества и имущества учреждения, учёта результатов исполнения ими обязанностей.

3.2.2. Обработка учреждением указанных выше персональных данных работников, учащихся и их родителей (законных представителей) возможна только с их согласия, либо без их согласия в следующих случаях:

– персональные данные являются общедоступными;

– персональные данные относятся к состоянию здоровья работника или учащегося и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника или родителя (законного представителя) невозможно;

– обработка персональных данных необходима для установления или осуществления прав их субъекта или третьих лиц либо в связи с осуществлением правосудия;

– обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, с уголовно-исполнительным законодательством РФ;

- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

- по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом;

- в случаях, если обработка персональных данных работников осуществляется на основании Трудового кодекса Российской Федерации или иного Федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке;

- обработка персональных данных осуществляется в целях исполнения трудового договора;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных.

3.2.3. Школа вправе обрабатывать персональные данные работников учреждения только с их письменного согласия.

3.2.4 Школа вправе обрабатывать персональные данные учащихся и их родителей (законных представителей) только с их письменного согласия.

3.2.5. Письменное согласие работника и родителей (законных представителей) учащихся на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта

персональных данных;

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

3.2.6. Работник учреждения, родитель (законный представитель) учащегося предоставляет учреждению достоверные сведения о себе, своем ребенке (детях).

3.2.7. В соответствии со ст. 86 гл. 14 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина директор учреждения и его представители (ответственные должностные лица) при обработке персональных данных работника должны соблюдать следующие общие требования:

– при определении объема и содержания, обрабатываемых персональных данных учреждение должно руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и иными нормативными правовыми и распорядительными документами Минпросвещения России, Рособрнадзора, другими федеральными законами;

- защита персональных данных работника от неправомерного их использования или утраты обеспечивается учреждением за счет его средств в порядке, установленном законодательством;
- при принятии решений, затрагивающих интересы работника, учреждение не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

– представители работника должны быть ознакомлены под расписку с федеральным законом, документами учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

– во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен;

– обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, регламентирующих образовательную деятельность организации и иных отношений, непосредственно связанных с образовательной деятельностью.

Обработка персональных данных учащихся может осуществляться в целях содействия учащимся в трудоустройстве через Центр занятости в рамках действующего законодательства, проведения государственной итоговой аттестации, поступления в образовательные организации.

4. Защита персональных данных

4.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

4.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

4.3. Защита персональных данных представляет собой предупреждение нарушения доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечение безопасности информации в процессе управленческой и производственной

деятельности учреждения.

4.4. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена учреждением за счет ее средств в порядке, установленном федеральным законом.

4.5. «Внутренняя защита»:

– регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и должностными лицами учреждения;

– для обеспечении внутренней защиты персональных данных необходимо соблюдать ряд мер: ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний; избирательное и обоснованное распределение документов и информации между работниками; рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации; знание работником требований нормативно - методических документов по защите информации и сохранении тайны; наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных; организация порядка уничтожения информации; своевременное выявление нарушения требований разрешительной системы доступа работниками учреждения; воспитательная и разъяснительная работа с сотрудниками учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами. защита персональных данных на электронных носителях. Все папки, содержащие персональные данные работников, учащихся и их родителей (законных представителей) хранятся на компьютере должностного лица (лиц) учреждения, защищенном паролем.

4.6. «Внешняя защита»:

- для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося

совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, и др.;

- под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к учреждению, посетители, работники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов;

- для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер: порядок приема, учета и контроля деятельности посетителей; пропускной режим

учреждения; технические средства охраны, сигнализации; требования к защите информации при интервьюировании и собеседованиях.

4.7. Все должностные лица учреждения, связанные с обработкой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников, учащихся и их родителей (законных представителей).

4.8. По возможности персональные данные обезличиваются.

4.9. Кроме мер защиты персональных данных, установленных законодательством, учреждение может вырабатывать иные меры защиты персональных данных работников, обучающихся и их родителей (законных представителей).

5. Передача и хранение персональных данных

5.1. При передаче персональных данных работника, учащегося и его родителей

(законных представителей) учреждение должно соблюдать следующие требования:

5.1.1. Не сообщать персональные данные работника, учащегося и его родителей (законных представителей) третьей стороне без их письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом.

5.1.2. Не сообщать персональные данные работника, учащегося и его родителей (законных представителей) в коммерческих целях без их письменного согласия.

5.1.3. Предупредить лиц, получивших персональные данные работника, учащегося и его родителей (законных представителей) о том, что полученные персональные данные могут быть использованы лишь в целях, для которых они сообщены (представлены), и требовать от этих лиц подтверждения того, что это правило соблюдено.

Лица, получившие персональные данные работника, учащегося и родителя (законного представителя) обязаны соблюдать режим секретности (конфиденциальности).

5.1.4. Разрешать доступ к персональным данным работников, учащихся и их родителей (законных представителей) возможно только специально уполномоченным лицам учреждения, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной трудовой функции, согласно списка специально уполномоченных лиц учреждения.

5.1.5. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.

5.1.6. Согласие на обработку персональных данных, разрешенных работником для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

Работодатель обязан обеспечить работнику возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на распространение персональных данных.

В случае если из предоставленного работником согласия на распространение персональных данных не следует, что работник согласился с распространением персональных данных, такие персональные данные обрабатываются работодателем без права распространения.

В случае если из предоставленного работником согласия на передачу персональных данных не следует, что работник не установил запреты и условия на обработку персональных данных или не указал категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, работодатель обрабатывает такие персональные данные без возможности передачи (распространения, предоставления, доступа) неограниченному кругу лиц.

В согласии на распространение персональных данных работник вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных работодателю неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ работодателя в установлении работником данных запретов и условий не допускается.

Передача (распространение, предоставление, доступ) персональных данных, разрешенных работником для распространения, должна быть прекращена в любое время по его требованию. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) работника, а также перечень персональных данных, обработка которых подлежит прекращению. Действие согласия работника на распространение персональных данных, прекращается с момента поступления работодателю данного требования.

Работник вправе обратиться с требованием прекратить передачу (распространение,

предоставление, доступ) своих персональных данных, ранее разрешенных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Федерального закона от 27.07.2006 № 152-ФЗ или обратиться с таким требованием в суд.

5.2. Хранение персональных данных работников, учащихся и их родителей (законных представителей):

5.2.1. Персональные данные работников, учащихся и их родителей (законных представителей) обрабатываются и хранятся в электронном виде в информационных системах. Доступ к персональным данным работников, учащихся и их родителей (законных представителей) в информационных системах осуществляется согласно разрешительной системы матрицы доступа к персональным данным.

5.2.2. Персональные данные работников, учащихся и их родителей (законных представителей) хранятся в бумажном варианте в личных делах в шкафу, закрывающемся на замок.

5.2.3. Трудовые книжки работников хранятся в сейфе у ведущего специалиста по кадрам.

5.2.4. Права доступа к персональным данным разграничены между различными категориями пользователей (системные администраторы, сотрудники, родители, ученики, ответственный за организацию персональных данных). Вход в систему осуществляется только при введении личного пароля пользователя.

5.2.5. Внешний доступ к персональным данным работников, учащихся и их родителей (законных представителей) имеют контрольно-ревизионные (надзорные) органы при наличии документов, на основании которых они проводят проверку. Дистанционно персональные данные могут быть представлены надзорным органам только по письменному запросу. Страховые фонды, негосударственные пенсионные фонды, другие организации и учреждения, а также родственники и члены семьи работника, учащегося или его родителей (законных представителей) не имеют доступа к персональным данным, за исключением наличия письменного согласия самого работника, родителей (законных представителей) учащегося.

5.2.6. Помещения, в котором хранятся персональные данные работников, учащихся и их родителей (законных представителей), должны быть оборудованы надежными замками.

6. Доступ к персональным данным

6.1. Внутренний доступ:

6.1.1 Право доступа к персональным данным работников, учащихся и их родителей (законных представителей) устанавливается приказом директора Школы.

6.2 Внешний доступ (другие организации, учреждения и граждане) регламентирован в п.5 данного Положения.

7. Права работника, родителей (законных представителей) в целях обеспечения защиты персональных данных

Работник, родители (законные представители) учащегося имеют право:

7.1. Получать доступ к своим персональным данным (данным своего ребенка) и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные.

7.2. Требовать от учреждения уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для учреждения персональных данных.

7.3. Требовать извещения учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях,

исправлениях или дополнениях.

7.4. Получать от учреждения:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

7.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия учреждения при обработке и защите персональных данных.

7.6. Родители (законные представители) учащегося не должны отказываться от своих прав на сохранение и защиту тайны.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

8.1. Работники учреждения, виновные в нарушении норм, регулирующих обработку персональных данных работника, учащегося и его родителей (законных представителей) несут дисциплинарную, административную, гражданско-правовую и/или уголовную ответственность в соответствии с федеральными законами.

Директор учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные работника.

Приложение № 2
К приказу № 300 от 31.08.2022г.

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности и права ответственного за организацию обработки персональных данных МБОУ «Кезская СОШ №2» (далее – школа).

1.2. Ответственный за организацию обработки персональных данных является сотрудником школы и назначается приказом директора.

1.3. Решение вопросов организации защиты персональных данных в школе входит в прямые служебные обязанности ответственного за организацию обработки персональных данных.

1.4. Ответственный за организацию обработки персональных данных обладает правами доступа к любым носителям персональных данных в школе.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.3. **Доступ к информации** – возможность получения информации и её использования.

2.4. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. **Информация** - сведения (сообщения, данные) независимо от формы их представления.

2.6. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.8. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

2.9. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.10. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.11. **Средство защиты информации (СЗИ)** – техническое, программное средство,

вещество и (или) материал, предназначенные или используемые для защиты информации.

2.12. **Угрозы безопасности персональных данных (УБПДн)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

2.13. **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

III. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Ответственный за организацию обработки персональных данных обязан:

3.1. Знать перечень и условия обработки персональных данных в школе.

3.2. Знать и предоставлять на утверждение директора школы изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей.

3.3. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения.

3.5. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.6. Реагировать на попытки несанкционированного доступа к информации в установленном ст.4 настоящей Инструкции порядке.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

3.8. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и правилам обработки персональных данных.

3.9. Проводить занятия и инструктажи с сотрудниками школы о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных.

3.10. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.11. Контролировать соблюдение сотрудниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными.

3.12. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.13. Организовать учет обращений субъектов персональных данных, контролировать заполнение «Журнала учета обращений субъектов персональных данных».

3.14. Представлять интересы школы при проверках надзорных органов в сфере обработки персональных данных.

3.15. Знать законодательство РФ о персональных данных, следить за его изменениями.

3.16. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

4.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных обязан:

4.2.1. прекратить несанкционированный доступ к персональным данным;

4.2.2. доложить директору школы служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4.2.4. известить администратора безопасности ИСПДн о факте несанкционированного доступа.

V. ПРАВА

Ответственный за организацию обработки персональных данных имеет право:

5.1. Требовать от сотрудников выполнения локальных нормативно-правовых актов в части работы с персональными данными.

5.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

5.3. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VI. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный за организацию обработки персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

6.2. Ответственный за организацию обработки персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 3 к приказу
№ 300 от 31.08.2022г.

Список работников, допущенных к обработке персональных данных в МБОУ «Кезская СОШ №2»

Должность	Ф. И. О.	Группа обрабатываемых данных
Директор	Юферева Елена Вениаминовна	Все персональные данные
Специалист по кадрам, делопроизводитель	Харитонова Елена Владимировна	Все персональные данные
Заместитель директора по УВР	Худякова Мария Сергеевна, Худякова Елена Вениаминовна, Тихонова Ольга Александровна	Персональные данные педагогов, учащихся и их родителей (законных представителей)
Заместитель директора по воспитательной работе	Корепанова Светлана Юрьевна	Персональные данные педагогов, учащихся и их родителей (законных представителей)
Социальный педагог	Ончукова Наталья Николаевна	Персональные данные учащихся и их родителей (законных представителей)
Классные руководители, учителя, педагоги ДО.	Белослудцев Олег Никандрович Бузмакова Мария Сергеевна Веретенникова Ландина Александровна Воронцова Наталья Евгеньевна Вяткина Татьяна Алексеевна Главатских Татьяна Валерьевна Данилова Анна Леонидовна Данилова Наталья Александровна Елисеева Анастасия Алексеевна Жигалова Елена Борисовна Иванова Любовь Ананьевна Ильина Ольга Николаевна Конев Иван Федорович Ложкина Оксана Михайловна Михайлова Людмила Николаевна Дементьева Ольга Ананьевна Разживина Вера Михайловна Сабурова Светлана Ананьевна Селиверстова Татьяна Владимировна Сунцов Игорь Витальевич Дунькина Любовь Серафионовна Федоров Роман Анатольевич Худяков АлександрНиколаевич	Персональные данные учащихся и их родителей (законных представителей)

	Николаева Екатерина Ивановна Конев Виктор Иванович Белослудцева Алина Ивановна	

Приложение № 4
к Приказу № 300 от 31.08.2022г.

Инструкция
пользователя информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Данная Инструкция определяет единый порядок сбора, систематизации, накопления, хранения, использования, уничтожения, защиты во время автоматизированной и неавтоматизированной обработки персональных данных (далее – ПДн) для работников МБОУ «Кезская СОШ №2» (далее – Оператор), допущенных к обработке ПДн и перечисленных в Перечне информационных систем персональных данных.

Пользователь информационных систем персональных данных (далее – Пользователь ИСПДн) обязан хранить в тайне конфиденциальную информацию, ставшую известной ему при исполнении должностных обязанностей – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, составляющие коммерческую, врачебную, служебную тайну, тайну страхования, персональные данные, иные сведения, носящие для Оператора конфиденциальный характер, охраняемые в соответствии с законодательством РФ и нормативными документами по защите конфиденциальной информации, обработке и защите ПДн. Пользователь ИСПДн обязан пресекать действия других лиц, которые могут привести к разглашению такой информации.

ПДн не подлежат разглашению (распространению). Прекращение доступа к данным не освобождает работника от взятых им обязательств по неразглашению конфиденциальной информации.

2. ОБЯЗАННОСТИ

Пользователь ИСПДн проходит обучение и инструктажи по вопросам обработки и обеспечения безопасности ПДн в объеме и порядке, установленные Администратором безопасности информационных систем персональных данных (далее – Администратор безопасности ИСПДн). Инструктаж и обучение проводят Администратор безопасности ИСПДн и Менеджер обработки персональных данных в пределах своих обязанностей. Пользователь ИСПДн в обязательном порядке должен ознакомиться со следующими документами:

– Политика в отношении обработки персональных данных;
– Документы, регламентирующие обработку и обеспечение безопасности персональных данных;
– настоящая инструкция.

Пользователь ИСПДн знает и строго выполняет правила работы со средствами защиты информации (средствами разграничения доступа, средствами антивирусной защиты), используемыми на персональных компьютерах.

Пользователь ИСПДн хранит в тайне свои данные для аутентификации (логин и пароль для входа) в информационных системах персональных данных (далее - ИСПДн), а также информацию о системе защиты, установленной в ИСПДн. Используемый пароль доступа удовлетворяет следующим условиям:

– длина пароля составляет не менее 8 символов;
– в составе символов пароля обязательно присутствуют буквы в верхнем и нижнем

регистрах, цифры и специальные символы (“ ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ? ,);

– при смене пароля новое значение отличается от предыдущего не менее чем в 4 позициях;

– пароль может повторяться не менее чем после использования 5 различных паролей;

– пароль не включает в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о Пользователе ИСПДн.

В рамках организации антивирусной защиты Пользователь ИСПДн:

– контролирует факт запуска модуля антивирусной защиты после загрузки операционной системы;

– ежедневно контролирует обновление антивирусных баз на своей персональной рабочей станции;

– осуществляет антивирусный контроль любой информации, получаемой по телекоммуникационным каналам;

– осуществляет антивирусный контроль любой информации, получаемой на съемных носителях (дискетах, оптических дисках, USB flash-накопителях);

– осуществляет антивирусный контроль всей исходящей информации непосредственно перед отправкой;

– осуществляет антивирусный контроль файлов, перемещаемых в электронный архив, в частности, на файловые серверы Оператора;

– немедленно ставит в известность Администратора безопасности ИСПДн в случае подозрений на наличие вредоносных программ, а также в случае иных инцидентов, связанных с организацией антивирусной защиты.

Пользователь ИСПДн, использующий для обработки ПДн съемные носители (гибкие магнитные диски, компакт-диски, USB flash-накопители и т.д.), соблюдает порядок, установленный Регламентом учета, хранения и уничтожения носителей ПДн.

В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных средств защиты Пользователь ИСПДн ставит в известность Администратора безопасности ИСПДн.

Пользователь ИСПДн немедленно ставит в известность ответственного за организацию обработки персональных данных.

– о ставших известных ему попытках разглашения конфиденциальной информации, в частности ПДн, а также о других причинах или условиях возможной утечки конфиденциальной информации;

– в случае утери носителя с ПДн или при подозрении компрометации личных ключей и паролей;

– в случае обнаружения фактов совершения в его отсутствие попыток несанкционированного доступа к персональной рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);

– в случае несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств автоматизированных систем;

– в случае возникновения иных инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн.

Пользователь ИСПДн при работе с конфиденциальной информацией принимает меры для исключения возможности визуального просмотра экрана видеомонитора лицами, не имеющими допуска к обрабатываемой информации.

Пользователю ИСПДн запрещается:

– передавать кому бы то ни было (в том числе родственникам) устно или письменно сведения, составляющие ПДн, доступ к которым он получил в связи с выполнением своих должностных обязанностей;

– использовать сведения, содержащие ПДн, которые подлежат защите, при подготовке открытых публикаций, докладов, научных работ и т.д.;

– снимать копии или производить выписки из документов, содержащих ПДн, без разрешения руководителя;

– накапливать ненужную для работы конфиденциальную информацию, в том числе ПДн;

– оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие ПДн, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера;

– использовать компоненты программного и аппаратного обеспечения автоматизированных систем подразделения в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

– осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить конфиденциальную информацию на неучтенных носителях информации (гибких магнитных дисках, USB-flash накопителях и т.п.);

– оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации.

Пользователь ИСПДн предоставляет всю необходимую информацию и документы при расследовании инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн, при проведении контрольных мероприятий по защите ПДн, а также проверок со стороны регулирующих органов.

3. ПРАВА

Пользователь ИСПДн имеет право получать доступ к ПДн в количестве и объеме, требуемом для выполнения возложенных на него должностных обязанностей.

Пользователь ИСПДн имеет право обратиться за консультацией по вопросам автоматизированной и неавтоматизированной обработки ПДн в рамках выполняемого процесса обработки ПДн к ответственному за организацию обработки персональных данных.

Пользователь ИСПДн имеет право обратиться к ответственному за организацию обработки персональных данных за консультацией по вопросам использования автоматизированных систем и технических средств обработки ПДн.

Пользователь ИСПДн имеет право обратиться к ответственному за организацию обработки персональных данных за консультацией по вопросам использования средств защиты информации, в частности ПДн, и общим вопросам обеспечения безопасности ПДн.

Пользователь ИСПДн имеет право вносить на рассмотрение предложения по совершенствованию процессов обработки ПДн, в которых он принимает участие в

соответствии со своими должностными обязанностями.

4. ОТВЕТСТВЕННОСТЬ

Пользователь ИСПДн несет ответственность за ненадлежащее соблюдение требований настоящей инструкции, а также других нормативных документов Оператора, касающихся обработки и обеспечения безопасности ПДн.

За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной предусмотренной законодательством ответственности.

5. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Пересмотр положений настоящего документа проводится в случае рассмотрения вопросов применения новых средств и методов обработки и защиты ПДн, существенно отличающихся от применяемых у Оператора, и случаев, указанных в Регламенте по реагированию на инциденты информационной безопасности.

Инициатором пересмотра настоящей Инструкции являются ответственный за организацию обработки персональных данных:

Внесение изменений производится на основании соответствующего приказа руководителя Оп.

Приложение № 5 к
приказу № 300 от 31.08.2022г.

Модель угроз безопасности персональных данных

при их обработке в информационной системе
персональных данных
МБОУ «Кезская СОШ №2»

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	–	автоматизированное рабочее место
ИС	–	информационная система
КЗ	–	контролируемая зона
НСД	–	несанкционированный доступ
КЗ	–	контролируемая зона
ОРД	–	организационно-распорядительная документация
ОС	–	операционная система
ПО	–	программное обеспечение
ПЭМИН	–	побочные электромагнитные излучения и наводки
СЗИ	–	средство защиты информации
СКЗИ	–	средство криптографической защиты информации
ТКУИ	–	технические каналы утечки информации
ТС	–	техническое средство

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Доступ к информации – возможность получения информации и ее использования.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

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

Нарушитель безопасности информации – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

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

Технические средства – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, программные средства, средства защиты информации, применяемые в информационных системах.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации по техническим каналам и (или) несанкционированными и (или) непреднамеренными воздействиями на нее с помощью штатного или специально разработанного программного обеспечения.

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Модель угроз безопасности информации (далее – Модель угроз) разрабатывается для определения возможных угроз безопасности информации и опасности этих угроз в случае их реализации. Целью разработки настоящей Модели угроз является формирование перечня актуальных угроз для информационной системы (далее – ИС) МБОУ «Кезская СОШ №2».

С использованием данных об уровне защищенности информации, обрабатываемой в ИСПДн, и перечня актуальных угроз формируются конкретные организационно-технические требования по защите обрабатываемой информации от утечки по техническим каналам, от несанкционированного доступа, и осуществляется выбор способов и средств защиты информации (далее – СЗИ).

Также в Модели угроз определяется перечень потенциальных нарушителей информационной безопасности, действия которых могут нанести значительных ущерб деятельности МБОУ «Кезская СОШ №2» и ущерб субъектам ПДн.

Модель угроз ИСПДн разработана на основании следующих документов:

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная ФСТЭК России 14 февраля 2008 года;

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная ФСТЭК России 15 февраля 2008 года.

Модель угроз должна быть актуализирована:

– при изменениях расположения, конфигурации, режима функционирования, изменения состава обрабатываемых данных ИСПДн;

– по результатам периодических мероприятий по контролю за выполнением требований по защите информации при ее обработке в ИСПДн.

2 ОПИСАНИЕ ИС

Хранение и обработка информации в ИСПДн осуществляется на серверах, размещенных в «серверной». Клиентское программное обеспечение (далее – ПО), посредством которого пользователи взаимодействуют с ИСПДн и создают запросы на обработку информации, установлено на рабочих местах школы.

ВИС осуществляется обработка персональных данных. Согласно требованиям Постановления Правительства РФ от 02.11.2012 № 1119 обрабатываемые ПДн относятся к категории «*Иные*» и объем их превышает 100000 записей. Для ИСПДн установлен <*третий*> тип актуальных угроз, а для ПДн, обрабатываемых в них, установлен 4 **уровень защищенности**.

3. КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ

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

– внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны (далее – КЗ), в пределах которой размещается оборудование ИСПДн ;

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

3.1 Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам (далее – ТС) и ресурсам ИСПДн , находящимся в пределах КЗ.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки информации (далее – ТКУИ), так как объем и ценность информации, хранимой и обрабатываемой в ИСПДн , является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по ТКУИ.

3.2 Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах КЗ ИСПДн ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь КЗ и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа (далее – НСД).

Система разграничения доступа в ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами).

К внутренним нарушителям могут относиться:

– администраторы ИСПДн (**категория I**): для ИСПДн инженер по защите информации, выполняющий функции системного администратора и администратора безопасности данной ИСПДн;

– администраторы конкретных подсистем или баз данных ИСПДн (**категория II**): для ИСПДн сотрудники, являющиеся администраторами прикладного ПО ИСПДн и осуществляющие ввод данных в систему, редактирование их структуры и содержания, удаление, настройку прикладного ПО;

– пользователи ИС (**категория III**): для ИСПДн сотрудники, осуществляющие обработку данных в ИСПДн;

– пользователи, являющиеся внешними по отношению к конкретной ИСПДн (**категория IV**): для ИСПДн сотрудники внешних организаций, осуществляющие просмотр и внесение данных в ИСПДн;

– сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (**категория V**);

– обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) (**категория VI**);

– уполномоченный персонал разработчиков, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (**категория VII**).

На лиц **категорий I и II** возложены задачи по администрированию ИСПДн ,и используемых в ней программно-аппаратных средств и баз данных. Администраторы потенциально могут реализовывать угрозы безопасности информации, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн , а также к техническим и программным средствам ИСПДн , включая СЗИ, в соответствии с установленными для них административными полномочиями. Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в ИСПДн , а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз безопасности информации. Данное оборудование может быть, как частью штатных средств, так и может относиться к легко получаемому (например, ПО, полученное из общедоступных внешних источников). Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам **категорий I и II**, ввиду их исключительной роли в ИСПДн, должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей. Предполагается, что в число лиц **категорий I и II** будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица **категорий III-VII** относятся к вероятным нарушителям. Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

3.3 Предположения об имеющейся у нарушителя информации об объектах реализации угроз безопасности информации

В качестве основных уровней знаний нарушителей о ИСможно выделить следующие:

– *общая информация* – информации о назначения и общих характеристиках ИС;

– *эксплуатационная информация* – информация, полученная из эксплуатационной документации;

– *чувствительная информация* – информация, дополняющая эксплуатационную информацию о ИС (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

– данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;

– сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

– данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;

– данные о реализованных в программных СЗИ принципах и алгоритмах;

– сведения о возможных каналах и способах реализации угроз безопасности ИС.

Предполагается, что лица **категории III** и **категории IV** владеют только эксплуатационной информацией, что обеспечивается организационными мерами.

Предполагается, что лица **категории V** и лица **категории VI** владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией о ИСПДн , использующей эту систему передачи информации, что обеспечивается организационными мерами. При этом эти лица не владеют парольной, аутентифицирующей и ключевой информацией, используемой в ИСПДн .

Предполагается, что лица **категории VII** обладают чувствительной информацией о ИСПДн , включая информацию об уязвимостях технических и программных средств ИСПДн . Организационными мерами предполагается исключить доступ лиц **категории VII** к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств информации, подлежащей защите в ИСПДн .

Таким образом, наиболее информированными о ИСПДн являются лица **категории III, категории IV** и лица **категории VII**.

3.4 Предположения об имеющихся у нарушителя средствах реализации угроз безопасности информации

Предполагается, что нарушитель имеет:

– доступные в свободной продаже (доступе)ТС и ПО.

Внутренний нарушитель может использовать штатные средства.

Вместе с тем предполагается, что нарушитель не имеет:

– средств перехвата в ТКУИ;

– средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы средства вычислительной техники);

– средств воздействия через цепи питания и через цепи заземления;

– средств активного воздействия на ТС (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица **категории III** и лица **категории VII**. Вместе с этим в виду небольшой ценности обрабатываемой информации предполагается, что нарушители имеют низкий потенциал реализации угроз.

4. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Под угрозами безопасности информации при ее обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации по техническим каналам и (или) несанкционированными и (или) непреднамеренными воздействиями на нее с помощью штатного или специально разработанного ПО.

Актуальной считается угроза безопасности, которая может быть реализована в ИСПДн и представляет опасность для обрабатываемой в ней информации. Порядок определения актуальных угроз безопасности информации в ИСПДн выполняется на основе документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Методика) с модификацией таблицы правил отнесения угроз к актуальным. В частности, введено дополнительное значение опасности угрозы – «очень низкая». Данное значение введено для угроз, реализация которых согласно данной Методике и введенным организационно-техническим мерам противодействия не приведет к какому-либо вредуи/или внедрены меры по реагированию на последствия реализации угрозы.

4.1 Уровень исходной защищенности ИС

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС, приведенных в таблице 1, представленной ниже.

Таблица 1 – Показатели исходной защищенности ИС

Технические и эксплуатационные характеристики ИС	**Уровни защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению: локальная (кампусная) ИС, развернутая в пределах нескольких близко расположенных зданий	–	+	–
2. По наличию соединения с сетями общего пользования: имеется многоточечный выход в сеть общего пользования.	–	–	+
3. По встроенным (легальным) операциям с записями баз данных ИС:модификация, передача.	–	–	+
4. По разграничению доступа к информации, обрабатываемой в ИС: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн	–	+	–
5. По наличию соединений с другими БД иных ИС: ИС, в которой используется одна база данных, принадлежащая организации – владельцу данной ИС.	+	–	–
6. По уровню обобщения (обезличивания) информации: ИС, в которой предоставляемые пользователю данные не являются обезличенными.	–	–	+
7. По объему информации, которая предоставляется сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющая никакой информации	+	–	–
Процентное соотношение	**28,6**	**28,6**	**42,8**

ИСПДн имеет низкий уровень исходной защищенности, т.к. менее 70% характеристик ИСПДн соответствуют уровню не ниже «среднего». При составлении перечня актуальных угроз безопасности информации низкому уровню исходной защищенности ставится в соответствие числовой коэффициент Y_1 равный 10.

4.2 Частота (вероятность) реализации угрозы безопасности информации

Под частотой (вероятностью) реализации угрозы безопасность информации понимается определенный экспертным путем показателя, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности информации для ИСПДн

в складывающихся условиях обстановки.

Используются четыре значения этого показателя:

– маловероятно– отсутствуют объективные предпосылки для осуществления угрозы;

– низкая вероятность – объективные предпосылки для реализации угрозы существуют, но применяемые меры существенно затрудняют ее реализацию;

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности информации недостаточны;

– высокая вероятность – объективные предпосылки для реализации угрозы существуют, а меры обеспечения безопасности информации не приняты.

При составлении перечня актуальных угроз безопасности информации каждому значению показателя ставится в соответствие числовой коэффициент Y_2, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

4.3 Реализуемость угрозы безопасности информации

По итогам оценки уровня исходной защищенности ИСПДн Y_1 и вероятности реализации угрозы безопасности информацииY_2 рассчитывается коэффициент реализуемости угрозы Y по следующей формуле: $Y= (Y_1 + Y_2)/20$.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы:

– если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признается низкой;

– если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней;

– если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признается высокой;

– если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

4.4 Оценка опасности угроз (вреда) для ИСПДн и ее пользователей

Непосредственный ущерб может проявляться в виде:

– причинения неудобств субъектам персональных данных;

– причинения морального ущерба субъектам персональных данных;

– возникновение ограничений прав и свобод субъектов персональных данных;

– нанесения вреда здоровью субъектам персональных данных; или создания угрозы жизни (для ИСПДн данный вид вреда невозможен, ввиду отсутствия обработки данных, влияющих на жизнь и здоровье субъектов).

При оценке опасности угрозы на основе опроса экспертов (специалистов в области защиты информации) определяется показатель опасности угрозы. Этот показатель имеет четыре значения:

– **очень низкая опасность** – если реализация угрозы не может привести к каким-либо последствиям для субъектов персональных данных и/или внедрены меры по реагированию на последствия реализации угрозы;

– **низкая опасность** – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

– **средняя опасность** – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

– **высокая опасность** – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

4.5 Выбор актуальных угроз безопасности информации для ИСПДн

Выбор актуальных угроз безопасности информации для рассматриваемой ИСПДн из общего (предварительного) перечня угроз осуществляется в соответствии с правилами, приведенными в таблице 2.

Таблица 2 – Правила отнесения угрозы безопасности информации к актуальной

Возможность реализации угрозы (Y)	Показатель опасности угрозы			
	Очень низкая	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	неактуальная	актуальная
Средняя	неактуальная	неактуальная	актуальная	актуальная
Высокая	неактуальная	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная	актуальная

4.6 Общий перечень угроз безопасности информации

Общий перечень угроз безопасности информации и единые исходные данные по ним приведены в документе «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Состав и содержание угроз безопасности информации определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к информации, обрабатываемой в ИСПДн и подлежащей защите. Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информационных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

Угрозы классифицируются в соответствии со следующими признаками:

1) по видам возможных источников 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 доступ к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и(или) сетей международного информационного обмена (внешний нарушитель);

2) по типу ИС, на которую направлена реализация угроз:

– угрозы безопасности информации, обрабатываемой в ИСПДн на базе автоматизированного рабочего места (далее – АРМ) с подключением или без подключения к сети общего пользования;

– угрозы безопасности информации, обрабатываемой в ИСПДн на базе локальных информационных систем с подключением или без подключения к сети общего пользования;

– угрозы безопасности информации, обрабатываемой в ИСПДн на базе распределенных информационных систем с подключением или без подключения к сети общего пользования;

3) по способам реализации угроз:

– угрозы, связанные с НСД к информации, обрабатываемой в ИСПДн (в том числе угрозы внедрения вредоносных программ);

– угрозы утечки информации по ТКУИ;

– угрозы специальных воздействий на ИСПДн;

4) по виду несанкционированных действий, осуществляемых с информацией:

– угрозы, приводящие к нарушению конфиденциальности информации (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

– угрозы, приводящие к несанкционированному воздействию на содержание информации, в результате которого осуществляется изменение или уничтожение информации;

– угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование информации;

5) по используемой уязвимости:

– угрозы, реализуемые с использованием уязвимости системного ПО;

– угрозы, реализуемые с использованием уязвимости прикладного ПО;

– угрозы, возникающие в результате использования уязвимости, вызванной наличием в автоматизированной информационной системе аппаратной закладки;

– угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

– угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от НСД;

– угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие ТКУИ;

– угрозы, реализуемые с использованием уязвимостей СЗИ;

6) по объекту воздействия:

– угрозы безопасности информации, обрабатываемой на АРМ;

– угрозы безопасности информации, обрабатываемой в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);

– угрозы безопасности информации, передаваемой по сетям связи;

– угрозы прикладным программам, с помощью которых обрабатывается информация;

– угрозы системному ПО, обеспечивающему функционирование ИСПДн.

4.7 Угрозы утечки информации по техническим каналам

Основными характеристиками угроз утечки информации по техническим каналам являются: источник угрозы, среда (пути) распространения информативного сигнала и носитель защищаемой информации.

Источниками угрозы являются физические лица, не имеющие доступа к ИСПДн.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником.

Носителем информации является пользователь ИСПДн, осуществляющий голосовой ввод информации вИС, акустическая система, воспроизводящая информацию, а также ТС ИСПДн, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

При обработке информации в ИСПДн за счет реализации технических каналов возможно возникновение следующих угроз безопасности информации:

– угроз утечки акустической информации;

– угроз утечки видовой информации;

– угроз утечки информации по каналам побочных электромагнитных излучений и наводок (далее – ПЭМИН).

Угроза, реализуемая за счет утечки акустической информации

В ИС не осуществляется голосовой ввод информации в данную ИСПДн и не используется акустическая система, воспроизводящая информацию.

Частота (вероятность) реализации угрозы – маловероятная ($Y_2 = 0$).

Возможный ущерб субъектам персональных данных ограничивается нанесением им морального ущерба от несанкционированного оглашения их персональных данных. Опасность угрозы для субъектов персональных данных – низкая.

Угроза, реализуемая за счет утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра

информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

В помещениях ИСПДн экраны дисплеев и других средств отображения вычислительной техники, используемых при обработке информации ИСПДн, расположены таким образом, что исключается возможность просмотра информации посторонними лицами. Кроме того, доступ в помещения, где располагаются элементы ИСПДн, ограничен, однако требование по расположению мониторов защищенным от несанкционированного просмотра способом в организационно-распорядительной документации на момент моделирования не зафиксированы.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

Возможный ущерб субъектам персональных данных ограничивается нанесением им морального ущерба от несанкционированного ознакомления с их персональными данными. Опасность угрозы для субъектов персональных данных – низкая.

Угроза, реализуемая за счет утечки по каналам ПЭМИН

Угроза утечки информации по каналам ПЭМИН реализуется за счет перехвата побочных (не связанных с прямыми функциональными значениями элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации ТС ИСПДн.

В помещениях ИСПДн функционирует множество вспомогательных технических средств и систем (телефонные средства, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, средства и системы кондиционирования и т.д.), создающих электромагнитные помехи.

Угрозы утечки информации по каналам ПЭМИН маловероятны, так как использование данного канала утечки является неэффективным и очень трудоемким (дорогостоящая специализированная аппаратура, длительное время на настройку и обработку данных).

Частота (вероятность) реализации угрозы – маловероятная ($Y_2 = 0$).

Возможный ущерб субъектам персональных данных ограничивается нанесением им морального ущерба от несанкционированного ознакомления с их персональными данными. Опасность угрозы для субъектов персональных данных – низкая.

4.8 Угрозы, реализуемые за счет несанкционированного доступа к информации

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированного распространение), целостности (уничтожение, изменение) и доступности (блокирование) информации.

4.8.1 Угрозы уничтожения, хищения аппаратных средств ИС путем физического доступа к элементам ИСПДн

Кража элементов, содержащих обрабатываемую в ИСПДн информацию

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В помещениях ИС установлен контрольно-пропускной режим доступа в КЗ ИСПДн, помещения оборудованы охранной сигнализацией, двери по окончании рабочего дня закрываются на замок, ключи сдаются службе охраны.

Частота (вероятность) реализации угрозы – маловероятная ($Y_2 = 0$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба всем субъектам, записи которых хранятся на серверах, от несанкционированного ознакомления с их персональными данными и задержки их обработки. Опасность угрозы для субъектов персональных данных – низкая.

Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В помещениях ИСПДн установлен контрольно-пропускной режим доступа в КЗ ИСПДн, помещения оборудованы охранной сигнализацией, двери по окончании рабочего дня закрываются на замок. В существующем комплекте организационно-распорядительной документации (далее – ОРД) на ИСПДн не описан порядок учета носителей информации. На момент написания Модели угроз учет носителей информации в ИС не осуществляются.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба всем субъектам, записи которых хранятся на серверах от несанкционированного ознакомления с их персональными данными и от задержки их обработки. Опасность угрозы для субъектов персональных данных – низкая.

Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В помещениях ИСПДн введен контроль доступа в КЗ ИСПДн, установлена охранная сигнализация, организованы учет и хранение ключей в защищенном месте.

Частота (вероятность) реализации угрозы – маловероятная ($Y_2 = 0$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба всем субъектам, записи которых хранятся на серверах от несанкционированного ознакомления с их персональными данными или от задержки их обработки из-за удаления записей о них. Опасность угрозы для субъектов персональных данных в центральном сегменте – низкая.

Кража, модификация, уничтожение информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и СЗИ, а также происходит работа пользователей.

В помещениях ИСПДн введен контроль доступа в КЗ ИСПДн, установлена охранная сигнализация, двери закрываются на замок. Закуплены сертифицированные средства защиты от НСД <*наименование средств защиты*>, реализующие механизмы разграничения доступа, однако данные средства не установлены и не настроены, процедуры и правила контроля доступа не задокументированы.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба всем субъектам, записи которых хранятся на серверах от несанкционированного ознакомления с их персональными данными или от задержки их обработки в результате удаления записей о них. Опасность угрозы для субъектов персональных данных – низкая.

Вывод из строя узлов ПЭВМ и каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В помещениях ИСПДн установлен контрольно-пропускной режим доступа в КЗ ИСПДн, помещения оборудованы охранной сигнализацией, двери по окончании рабочего дня закрываются на замок, ключи сдаются службе охраны.

Частота (вероятность) реализации угрозы – маловероятная ($Y_2 = 0$).

Недоступность ключевых узлов (сетевого оборудования) и каналов связи ИСПДн может привести к временной невозможности обработки информации. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от задержки обработки их данных в результате вывода из строя узлов ПЭВМ или каналов связи. Опасность угрозы для субъектов персональных данных – низкая.

Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ИС

Угроза осуществляется путем НСД к информации при проведении ремонта узлов ИСПДн и уничтожении носителей информации, обрабатываемой в ИСПДн.

В помещениях ИС за техническое обслуживание узлов ИС отвечают уполномоченные сотрудники. На момент написания Модели угроз в составе ОРД на ИСПДн нет документа, регламентирующего процедуры и правила технического обслуживания узлов ИС, не установлены требования по порядку передачи узлов в ремонт, а также нет отметок о прохождении уполномоченными сотрудниками инструктажа по порядку осуществления технического обслуживания узлов ИСПДн.

Частота (вероятность) реализации угрозы – высокая ($Y_2 = 10$).

При реализации угрозы нарушитель может получить полный доступ к информации, обрабатываемой в ИСПДн, что может повлечь за собой ее разглашение, модификацию и уничтожение. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или редактирования. Опасность угрозы для субъектов персональных данных – низкая.

Несанкционированное отключение средств защиты информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены СЗИ ИСПДн.

В помещениях ИСПДн установлен контрольно-пропускной режим доступа в КЗ ИСПДн, помещения оборудованы охранной сигнализацией, двери по окончании рабочего дня закрываются на замок. Правами на настройку и отключение СЗИ обладает только уполномоченный высококвалифицированный специалист – инженер по защите информации, выполняющий обязанности администратора безопасности ИСПДн. На момент написания Модели угроз в существующем комплекте ОРД на ИСПДн надлежащим образом не описан порядок действий пользователей ИСПДн в случае обнаружения фактов несанкционированного отключения СЗИ, СЗИ не установлены.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

В период временного отключения СЗИ могут быть реализованы угрозы, направленные на нарушение конфиденциальности, целостности и доступности информации, обрабатываемой в ИСПДн, противодействие которым осуществляется с помощью данных СЗИ. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или редактирования. Опасность угрозы для субъектов персональных данных – низкая.

4.8.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)

Действия вредоносных программ

Программно-математическое воздействие – это воздействие с помощью вредоносной программы (вируса), под которой подразумевают самостоятельную программу (набор инструкций), способную 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 или внешней 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 во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

На всех элементах ИСПДн будет установлена сертифицированная антивирусная защита <*наименование средств защиты*> и будет осуществляться ежедневное обновление антивирусного средства и антивирусных баз. На момент написания Модели угроз в составе ОРД на ИСПДн не установлены антивирусные средства, не разработана инструкция по антивирусной защите, описывающая правила работы с антивирусным средством.

Частота (вероятность) реализации угрозы – высокая ($Y_2 = 10$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или редактирования. Опасность угрозы для субъектов персональных данных – низкая.

Недекларированные возможности системного ПО и ПО для обработки информации

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.

В ИСПДн используется лицензионное ПО, разработчиками которого являются организации, длительный срок присутствующие на рынке информационных технологий и заботящиеся о качестве своей продукции и репутации своей компании. Кроме того, исходя из того, что обрабатываемая информация не представляет экономической или политической ценности, возможный ущерб субъектам персональных данных ограничивается моральным ущербом от ознакомления с их персональными данными и некорректной обработки или невозможности обработки их обращений, а защита от данных угроз является дорогостоящей, данный тип угроз устанавливается неактуальным.

Частота (вероятность) реализации угрозы – маловероятная ($Y_2 = 0$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или редактирования. Опасность угрозы для субъектов персональных данных – низкая.

Установка ПО, не требующегося для исполнения служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности информации, обрабатываемой в ИСПДн.

В ИСПДн введено разграничение прав пользователей на установку и использование дополнительного ПО. На момент написания Модели угроз в ИС разграничение прав пользователей осуществляется не прошедшими оценку соответствия средствами защиты, в документации прописан запрет установки дополнительного программного обеспечения.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

В случае установки стороннего ПО нарушитель может получить доступ к информации с более высокими правами доступа, чем те, которые для него установлены за счет использования уязвимостей прикладного, системного ПО и средств защиты, а также сетевых протоколов. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или редактирования. Опасность угрозы для субъектов персональных данных – низкая.

4.8.3 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и средств защиты информации, а также угроз неантропогенного и стихийного характера

Утрата или несоблюдение порядка действий с ключами и атрибутами доступа

Угроза осуществляется за счет действий пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

Для пользователей ИСПДн введена парольная политика, требования к сложности пароля, периоду его смены и правилам обращения с ним установлены. В парольной политике приводится порядок действий в случае утраты и компрометации паролей.

Частота (вероятность) реализации угрозы – низкая ($Y_2 = 2$).

При получении ключей и атрибутов доступа нарушитель получает несанкционированный доступ к обрабатываемой в ИСПДн информации.

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действий пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

В ИСПДн не осуществляется резервное копирование данных, что не позволит восстановить информацию, обрабатываемую в данной ИСПДн, подвергшуюся модификации или уничтожению. На момент написания данной Модели угроз в составе ОРД на ИСПДн отсутствуют регламенты (инструкции, процедуры) резервного копирования и восстановления информации.

Частота (вероятность) реализации угрозы – высокая ($Y_2 = 10$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

Непреднамеренное отключение средств защиты информации

Угроза осуществляется за счет действий пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и СЗИ или не осведомлены о них.

В помещениях ИС установлен контрольно-пропускной режим доступа в КЗ ИСПДн, помещения оборудованы охранной сигнализацией, двери по окончании рабочего дня закрываются на замок. Правами на настройку и отключение СЗИ обладает только уполномоченный высококвалифицированный специалист – инженер по защите информации, выполняющий обязанности администратора безопасности ИСПДн. Непривилегированные пользователи не обладают правами для отключения механизмов защиты. На момент написания Модели угроз в существующем комплекте ОРД на ИС отсутствует документ, надлежащим образом описывающий правила работы с СЗИ, функционирующими в данной ИСПДн.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

В период временного отключения СЗИ могут быть реализованы угрозы, направленные на нарушение конфиденциальности, целостности и доступности информации, обрабатываемой в ИС, противодействие которым осуществляется с помощью данных СЗИ.

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или редактирования. Опасность угрозы для субъектов персональных данных – низкая.

Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие техногенных причин (возможных неисправностях, отказов аппаратно-программных средств), из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В ИСПДн не осуществляется резервирование серверов с обрабатываемыми данными. Выход их из строя исключит доступность информации ИСПДн. Не определен порядок действий в случае выхода из строя технических средств.

Частота (вероятность) реализации угрозы – высокая ($Y_2 = 10$).

Реализация угрозы приведет к временной невозможности доступа к информации, обрабатываемой в ИСПДн, а также к возможной модификации и частичному уничтожению (нарушение целостности и доступности).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

Сбой системы электроснабжения ИСПДн

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В помещениях ИСПДн ко всем ключевым элементам ИС подключены источники бесперебойного питания и общесистемными средствами осуществляется резервное копирование виртуальных машин серверов.

Частота (вероятность) реализации угрозы – низкая ($Y_2 = 2$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от задержки обработки их данных в результате их уничтожения или искажения. Опасность угрозы для субъектов персональных данных – низкая.

Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В помещениях ИСПДн установлена пожарная сигнализация, но не разработан план действий пользователей ИСПДн в случае возникновения внештатных ситуаций.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

В случае реализации угрозы следует ожидать полного или частичного уничтожения информации, обрабатываемой в ИСПДн, а также временной невозможности доступа к информации.

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их уничтожения. Опасность угрозы для субъектов персональных данных – низкая.

4.8.4 Угрозы преднамеренных действий внутренних нарушителей

Доступ к информации, ее модификация и уничтожение лицами, не допущенными к обработке

Угроза осуществляется путем НСД нарушителей в помещения, где расположены элементы ИСПДн и СЗИ, а также происходит работа пользователей ИСПДн. НСД может быть осуществлен как за счет использования специализированного ПО посредством реализации уязвимостей в специальном и прикладном ПО, так и за счет несанкционированной загрузки АРМ и серверов ИСПДн с отчуждаемых носителей (USB, CD-ROM и др.).

В помещениях ИС установлен контрольно-пропускной режим доступа в КЗ ИСПДн, помещения оборудованы охранной сигнализацией, двери по окончании рабочего дня закрываются на замок. Также в ИСПДн закуплены сертифицированные средства защиты от НСД <*наименование средств защиты*>, с помощью которых будет обеспечиваться аутентификация пользователей и разграничение их доступа к ресурсам данной ИСПДн, однако эти средства не установлены и не настроены. В организационно-распорядительной

документации не описан порядок работы со средствами защиты. Обрабатываемые в ИСПДн данные хранятся в централизованном хранилище, расположенном в выделенном помещении, куда нет доступа обычным пользователям.

Частота (вероятность) реализации угрозы – высокая ($Y_2 = 10$).

Реализация угрозы может нарушить конфиденциальность, целостность и доступность части информации, обрабатываемой в ИСПДн. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

Разглашение информации, ее модификация и уничтожение сотрудниками, допущенными к обработке

Угроза осуществляется за счет действий пользователей ИСПДн, которые осознанно осуществляют несанкционированное изменение или удаление информации штатными средствами обработки, нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

Пользователи ИС осведомлены о порядке работы с обрабатываемой в данной ИСПДн информацией, однако в должностных инструкциях не определена ответственность за разглашения информации.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

Реализация угрозы может нарушить конфиденциальность, целостность и доступность части информации, обрабатываемой в ИСПДн. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

4.8.5 Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия

Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия, включают в себя:

1) анализ сетевого трафика;
2) перехват сетевого трафика;
3) сканирование сети;
4) подмена доверенного объекта сети;
5) навязывание ложного маршрута сети;
6) внедрение ложного объекта сети;
7) удаленный запуск приложений;
8) внедрение по сети вредоносных программ;
9) угроза выявления пароля.

Анализ сетевого трафика

Угроза реализуется с помощью специальной программы анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и позволяющей выявить идентификатор пользователя и его пароль и/или передаваемые данные.

В ходе реализации угрозы нарушитель:

– изучает логику работы ИСПДн, стремится 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 передаваемой информации, которой 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).

Перехват сетевого трафика за пределами контролируемой зоны

Передача информации за пределы КЗ в ИСПДн не осуществляется.

Частота (вероятность) реализации угрозы – маловероятно ($Y_2 = 0$).

В случае реализации угрозы нарушается конфиденциальность передаваемой по каналам связи информации. Возможность подмены передаваемых данных в результате перехвата сетевого трафика не рассматривается ввиду сложности реализации данного вида атак, не соответствующей ценности передаваемых данных. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными. Опасность угрозы для субъектов персональных данных – низкая.

Перехват в пределах контролируемой зоны внешними нарушителями

В помещениях ИСПДн установлен контрольно-пропускной режим доступа в КЗ ИСПДн, помещения оборудованы охранной сигнализацией, а двери по окончании рабочего дня закрываются на замок, провода каналов связи размещены в коробах. На момент написания данной Модели угроз в ИСПДн применяется СКЗИ ViPNet, которые установлены на всех рабочих местах и серверах ИСПДн.

Частота (вероятность) реализации угрозы – маловероятно ($Y_2 = 0$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными. Опасность угрозы для субъектов персональных данных – низкая.

Перехват в пределах контролируемой зоны внутренними нарушителями

В ИСПДн непривилегированные пользователи не имеют возможности несанкционированного подключения к каналам связи для прослушивания сетевого трафика, т.к. все сетевые кабели размещены в кожухах, используются сетевые коммутаторы и VLANдля управления сетевыми потоками. В помещениях ИСПДн установлен контрольно-пропускной режим доступа в КЗ ИСПДн, помещения оборудованы охранной сигнализацией, а двери по окончании рабочего дня закрываются на замок, что исключает возможность установки аппаратных анализаторов пакетов лицами, не имеющими право доступа к элементам данной ИСПДн. На момент написания данной Модели угроз в ИСПДн применяется СКЗИ ViPNet, которые установлены на всех рабочих местах и серверах ИСПДн.

Частота (вероятность) реализации угрозы – маловероятно ($Y_2 = 0$).

Реализация угрозы дает возможность нарушителю получить доступ к информации, обрабатываемой в ИСПДн, доступ к которой должен быть запрещен. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или искажения (в случае выявления паролей и последующего несанкционированного изменения или удаления данных). Опасность угрозы для субъектов персональных данных – низкая.

Сканирование сети

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них, в результате чего появляется возможность определить используемые протоколы, доступные порты сетевых служб, законы формирования идентификаторов соединений, активные сетевые сервисы, подобрать идентификаторы и пароли пользователей. Выявленные сетевые службы в дальнейшем могут быть скомпрометированы за счет уязвимостей в них.

На момент написания данной Модели угроз в ИСПДн применяется СКЗИ ViPNet, которые установлены на всех рабочих местах и серверах ИСПДн. Эти СКЗИ ограничивают возможность сетевого обращения к ресурсам ИСПДн со стороны сетевых узлов, не входящих в их состав. Также эти СКЗИ реализуют политику сетевой фильтрации трафика

для сетевых узлов, входящих в их состав. Однако политика фильтрации документально не зафиксирована.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

В случае реализации угрозы и успешной дальнейшей эксплуатации уязвимостей обнаруженных сетевых службу нарушителя появляется возможность получить доступ к информации, обрабатываемой в ИСПДн, что приведет к нарушению ее конфиденциальности, целостности и доступности. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

Выявление паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать 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, 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.

В данном случае будет рассматриваться угроза выявления паролей за счет перебора. Актуальность угроз выявления паролей за счет анализа трафика рассматривалась в анализе угроз перехвата трафика. Актуальность угроз выявления паролей за счет вредоносного ПО будет рассматривать в анализе угроз внедрения вредоносного ПО. Актуальность угроз выявления паролей за счет подмены доверенного объекта сети – в анализе угроз подмены доверенного объекта сети.

На момент написания данной Модели угроз в ИСПДн задокументирована политика ведения паролей (требования к их сложности и период обновления), не определена и не задокументирована политика аудита (в том числе требование регистрации событий неуспешной аутентификации).

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

В случае реализации угрозы и успешной дальнейшей эксплуатации уязвимостей обнаруженных сетевых службу нарушителя появляется возможность получить доступ к информации, обрабатываемой в ИСПДн, что приведет к нарушению ее конфиденциальности, целостности и доступности. Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

Подмена доверенного объекта сети

Данный вид угрозы эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу. Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

На момент написания данной Модели угроз в ИСПДн применяется СКЗИ ViPNet, которые установлены на всех рабочих местах и серверах ИСПДн. Эти СКЗИ за счет применения криптографических методов обеспечивают надежную идентификацию сетевых узлов, входящих в состав ИСПДн и исключают возможность их подмены. Также сложность реализации угроз данного вида требует от нарушителя высокой квалификации, при этом трудоемкость атаки превышает ценность полученной при её успешном осуществлении информации.

Частота (вероятность) реализации угрозы – маловероятно ($Y_2 = 0$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

Навязывание ложного маршрута сети

Данная угроза реализуется либо путем внутрисегментного, либо путем межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно перенаправить сетевые потоки на устройство нарушителя с возможностью влиять на их содержимое. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

Используемые в ИСПДн ОС и сетевое оборудование настроено на запрет использования и реагирования потенциально опасных управляющих сообщений в сетевых пакетах (например, ICMP-redirect). Потенциально опасные протоколы динамической маршрутизации внутри ИСПДн не используются. На момент написания данной Модели угроз в ИС применяется СКЗИ ViPNet, которые установлены на всех рабочих местах и серверах ИСПДн. Эти СКЗИ за счет применения криптографических методов обеспечивают конфиденциальность и целостность передаваемых по сети данных, ограничивая возможный ущерб от данной угрозы нарушением только доступности информации. Сложность реализации угроз данного вида требует от нарушителя высокой квалификации (потенциала), трудоемкость атаки превышает ценность полученной при её успешном осуществлении информации.

Частота (вероятность) реализации угрозы – низкая ($Y_2 = 2$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от временной задержки обработки их данных в результате несанкционированного изменения маршрута передачи сетевых пакетов и последующей недоступности сетевых сервисов. Опасность угрозы для субъектов персональных данных – низкая.

Внедрение ложного объекта сети

Угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче 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 с объектом-жертвой, будет проходить через ложный объект сети.

На момент написания данной Модели угроз в ИСПДн применяется СКЗИ ViPNet, которые установлены на всех рабочих местах и серверах ИСПДн. Эти СКЗИ за счет применения криптографических методов обеспечивают конфиденциальность и целостность передаваемых по сети данных между узлами ИСПДн, ограничивая возможный ущерб от данной угрозы нарушением только доступности информации.

Частота (вероятность) реализации угрозы – средняя ($Y_2 = 5$).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от временной задержки обработки их данных в результате несанкционированного изменения маршрута передачи сетевых пакетов и последующей недоступности сетевых сервисов. Опасность угрозы для субъектов персональных данных – низкая.

Угрозы типа «Отказ в обслуживании»

Угрозы основаны на недостатках сетевого ПО, его уязвимостях, позволяющих нарушителю создавать условия, когда ОС или ПО оказывается не в состоянии обрабатывать поступающие пакеты.

Разновидности угроз «Отказ в обслуживании»:

1) скрытый отказ в обслуживании, вызванный частичным исчерпанием ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов;

2) явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при этом 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.;

3) явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИС при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации;

4) явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер, что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

На момент написанияданной Модели угроз в ИСПДн закуплен сертифицированный межсетевой экран, реализующий в том числе функции противодействия атакам типа «отказ в обслуживании». Данный межсетевой экран не установлен и не настроен. Параметры его настройки не документированы.

Частота (вероятность) реализации угрозы – высокая ($Y_2 = 10$).

Реализация данной угрозы может привести к временной невозможности работы с информацией, обрабатываемой в ИСПДн (нарушение доступности).

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от задержки обработки их данных. Опасность угрозы для субъектов персональных данных – низкая.

Удаленный запуск приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: вирусы, «сетевые шпионы» или за счет использования уязвимостей сетевых служб, основная цель которых – нарушение

конфиденциальности, целостности, доступности информации и полный контроль за работой хоста.

Выделяют 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 документа, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на 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 за переполнением буфера).

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 (LandeskManagementSuite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

В ИСПДн закуплено сертифицированное средство антивирусной защиты <*наименование средств защиты*>, противодействующее данным угрозам при активации вредоносного кода, который пытается удаленно запустить нарушитель. Данное антивирусное средство не установлено и не настроено. В документации не регламентированы процедуры настройки и работы с ним.

Частота (вероятность) реализации угрозы – высокая ($Y_2 = 10$).

При реализации угрозы нарушитель получает доступ к информации, обрабатываемой в ИС, что может повлечь нарушение ее конфиденциальности, целостности и доступности.

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными даннымии от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

Внедрение по сети вредоносных программ

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 удаленной рабочей станции 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 ИС;

– программы-генераторы компьютерных вирусов;

– программы, демонстрирующие уязвимости СЗИ и др.

В ИСПДн закуплено сертифицированное средство антивирусной защиты

<*наименование средств защиты*>, противодействующее данным угрозам при активации вредоносного кода, который пытается удаленно запустить нарушитель. Данное антивирусное средство не установлено и не настроено. В документации не регламентированы процедуры настройки и работы с ним.

Частота (вероятность) реализации угрозы – высокая ($Y_2 = 10$).

При реализации угрозы нарушитель получает доступ к информации, обрабатываемой в ИС, что может повлечь нарушение ее конфиденциальности, целостности и доступности.

Возможный ущерб субъектам персональных данных ограничивается нанесением морального ущерба субъектам от несанкционированного ознакомления с их персональными данными и от задержки обработки их данных в результате их удаления или искажения. Опасность угрозы для субъектов персональных данных – низкая.

В таблице 3 приведен перечень угроз безопасности информации для ИСПДн с указанием их актуальности. При указании опасности угрозы для неё выбиралось наибольшее значение из возможных для оператора ИСПДн и для субъектов персональных данных.

Таблица 3 – Перечень угроз для ИСПДн

Наименование угрозы (ИС имеет низкий уровень исходной защищенности (Y_1=10))		**Частота (вероятность) реализации угрозы, Y_2**	**Возможность реализации угрозы, Y**	**Опасность угрозы**	**Актуальность**
Угрозы, реализуемые через технические каналы утечки информации					
1.	Угроза утечки акустической информации	Маловероятная (Y_2=0)	Низкая (Y=0,5)	Низкая	Неактуальная
2.	Угрозы утечки видовой информации	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
3.	Угрозы утечки информации по каналам ПЭМИН	Маловероятная (Y_2=0)	Низкая (Y=0,5)	Низкая	Неактуальная
Угрозы, реализуемые за счет несанкционированного доступа к информации					
4. Угрозы уничтожения, хищения аппаратных средств ИС путем физического доступа к элементам ИС					
4.1.	Кража элементов, содержащих обрабатываемую в ИС информацию	Маловероятная (Y_2=0)	Средняя (Y=0,5)	Низкая	Неактуальная
4.2.	Кража носителей информации	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
4.3.	Кража ключей и атрибутов доступа	Маловероятная (Y_2=0)	Средняя (Y=0,5)	Низкая	Неактуальная
4.4.	Кража, уничтожение, модификация информации	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
4.5.	Вывод из строя узлов ПЭВМ и каналов связи	Маловероятная (Y_2=0)	Средняя (Y=0,5)	Низкая	Неактуальная
4.6.	Несанкционированный доступ к информации при техническом обслуживании узлов ИС	Высокая (Y_2=10)	Оч. высокая (Y=1,0)	Низкая	Актуальная
4.7.	Несанкционированное отключение средств защиты информации	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная

Наименование угрозы (ИС имеет низкий уровень исходной защищенности (Y_1=10))		Частота (вероятность) реализации угрозы, Y_2	Возможность реализации угрозы, Y	Опасность угрозы	Актуальность
5. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
5.1.	Действия вредоносных программ (вирусов)	Высокая (Y_2=10)	Оч. высокая (Y=1,0)	Низкая	Актуальная
5.2.	Недекларированные возможности системного ПО и ПО для обработки информации	Маловероятная (Y_2=0)	Средняя (Y=0,5)	Низкая	Неактуальная
5.3.	Установка ПО, не требующегося для исполнения служебных обязанностей	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
6. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ, а также от угроз неантропогенного и стихийного характера					
6.1.	Утрата или несоблюдение порядка действий с ключами и атрибутами доступа	Низкая (Y_2=2)	Средняя (Y=0,6)	Низкая	Неактуальная
6.2.	Непреднамеренная модификация (уничтожение) информации сотрудниками	Высокая (Y_2=10)	Оч. высокая (Y=1,0)	Низкая	Актуальная
6.3.	Непреднамеренное отключение средств защиты	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
6.4.	Выход из строя аппаратно-программных средств	Высокая (Y_2=10)	Оч. высокая (Y=1,0)	Низкая	Актуальная
6.5.	Сбой системы электроснабжения	Низкая (Y_2=2)	Средняя (Y=0,6)	Низкая	Неактуальная
6.6.	Стихийное бедствие	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
7. Угрозы преднамеренных действий внутренних нарушителей					
7.1.	Доступ к информации, ее модификация и уничтожение лицами, не допущенными к обработке	Высокая (Y_2=10)	Очень высокая (Y=1)	Низкая	Актуальная
7.2.	Разглашение информации, ее модификация и уничтожение сотрудниками, допущенными к обработке	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
8. Угрозы, реализуемые с использование протоколов межсетевого взаимодействия					
8.1.	Перехват сетевого трафика за пределами	Маловероятная (Y_2=0)	Средняя (Y=0,5)	Низкая	Неактуальная

Наименование угрозы (ИС имеет низкий уровень исходной защищенности (Y_1=10))		Частота (вероятность) реализации угрозы, Y_2	Возможность реализации угрозы, Y	Опасность угрозы	Актуальность
	КЗ				
8.2.	Перехват в пределах КЗ внешними нарушителями	Маловероятная (Y_2=0)	Средняя (Y=0,5)	Низкая	Неактуальная
8.3.	Перехват в пределах КЗ внутренними нарушителями	Маловероятная (Y_2=0)	Средняя (Y=0,5)	Низкая	Неактуальная
8.4.	Сканирование сети	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
8.5.	Выявление паролей	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
8.6.	Подмена доверенного объекта сети	Маловероятная (Y_2=0)	Средняя (Y=0,5)	Низкая	Неактуальная
8.7.	Навязывание ложного маршрута сети	Низкая (Y_2=2)	Средняя (Y=0,6)	Низкая	Неактуальная
8.8.	Внедрение ложного объекта сети	Средняя (Y_2=5)	Высокая (Y=0,75)	Низкая	Актуальная
8.9.	Отказ в обслуживании	Высокая (Y_2=10)	Очень высокая (Y=1)	Низкая	Актуальная
8.10.	Удаленный запуск приложений	Высокая (Y_2=10)	Очень высокая (Y=1)	Низкая	Актуальная
8.11.	Внедрение по сети вредоносных программ	Высокая (Y_2=10)	Очень высокая (Y=1)	Низкая	Актуальная

5. МЕРЫ ПО ПРОТИВОДЕЙСТВИЮ АКТУАЛЬНЫМ УГРОЗАМ

В соответствии с актуальными угрозами безопасности информации, обрабатываемой в ИСПДн, необходимо принять ряд дополнительных организационных и технических мер по противодействию этим угрозам. Перечень актуальных угроз и соответствующих им возможных дополнительных мер по противодействию представлен в таблице 4. Конкретный перечень мер представлен в документации технического проекта на ИСПДн.

Таблица 4 – Перечень актуальных угроз и мер противодействия

Наименование актуальной угрозы безопасности информации		**Меры по противодействию актуальным угрозам безопасности информации**	
		Организационные	**Технические**
1.	Угрозы утечки видовой информации	Определить требования к размещению устройств вывода в ОРД	
2.	Кража носителей информации	Организовать учет носителей информации	
3.	Кража, уничтожение, модификация информации	Регламентировать процедуры контроля доступа (Матрица доступа и др.)	Использовать механизмы контроля доступа, прошедшие оценку соответствия
4.	Несанкционированный доступ к информации при техническом обслуживании узлов ИС	Регламентировать процедуры передачи техники в ремонт, и проведения технического обслуживания	
5.	Несанкционированное отключение средств защиты информации	Регламентировать порядок контроля состояния средств защиты и действий в случае обнаружения их несанкционированного отключения	Использовать средства защиты, прошедшие оценку соответствия
6.	Непреднамеренное отключение средств защиты		
7.	Действия вредоносных программ (вирусов)	Регламентировать процедуры работы с антивирусным ПО	Использовать антивирусное ПО, прошедшее оценку соответствия
8.	Удаленный запуск приложений		
9.	Угрозы внедрения по сети вредоносных программ		
10.	Установка ПО, не требующегося для исполнения служебных обязанностей	Определить перечень ПО, необходимого для выполнения задач ИС (и служебных задач)	Использовать механизмы контроля доступа, прошедшие оценку соответствия
11.	Выявление паролей	Задокументировать требования к политике, аудита	Настроить средства защиты и общесистемное ПО в соответствии с установленной политикой аудита
12.	Непреднамеренная модификация (уничтожение) информации	Задокументировать порядок выполнения процедур резервного копирования и	Реализовать резервное копирование баз данных средствами общесистемного или

Наименование актуальной угрозы безопасности информации		Меры по противодействию актуальным угрозам безопасности информации	
		Организационные	**Технические**
	сотрудниками	восстановления	специального ПО
13.	Выход из строя аппаратно-программных средств	Регламентировать порядок действий в случае сбоев.	Обеспечить резервирование серверов
14.	Стихийное бедствие	Регламентировать порядок действий в случае внештатной ситуации, а также процедуры и правила восстановления информационных ресурсов ИС	
15.	Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Регламентировать процедуры управления доступом, регистрации событий, контроля установки обновлений ПО	Использовать прошедшие оценку соответствия средства разграничения доступа, настроить аудит, обеспечить установку обновлений используемого ПО
16.	Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Задокументировать и довести до пользователей ответственность за нарушения порядка и режима обработки данных	
17.	Сканирование сети	Описать порядок работы и настройки межсетевого экрана	Использовать межсетевой экран, прошедший оценку соответствия
18.	Внедрение ложного объекта сети	Регламентировать порядок действий в случае потери доступности информации, включающий проверку подлинности сетевых узлов	
19.	Отказ в обслуживании	Описать порядок настройки межсетевого экрана в части противодействия данным угрозам.	Настроить на межсетевом экране предел количества входящих соединений в установленный интервал времени и/или время жизни бездействующих соединений

6. МОДЕЛЬ НАРУШИТЕЛЯ И ОБОСНОВАНИЕ НЕОБХОДИМОГО КЛАССА СКЗИ

В случае принятия решения об использовании в ИСПДн СКЗИ необходимо определить перечень актуальных для него угроз, и на основании этих данных определить минимальный класс СКЗИ, которое можно использовать в ИСПДн. На сегодняшний день единственным руководящим документом ФСБ, в котором указываются требования к применяемым СКЗИ, и под действие которого подпадало бы функционирование ИСПДн, является Приказ ФСБ № 378 от 10.07.2014. В данном документе устанавливается необходимость:

- формирования предположений о возможностях потенциальных злоумышленников (нарушителей) объектом атак которых является СКЗИ;
- определение актуальных угроз, исходя из сформированных предположений о возможностях нарушителей;
- определения класса СКЗИ, достаточного для нейтрализации актуальных угроз.

Первоначально следует выполнить моделирование типов нарушителей, актуальных для СКЗИ, применяемых в ИСПДн. Предполагается, что в число потенциальных нарушителей СКЗИ не входят специалисты в области разработки и анализа СКЗИ, в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ и в области использования для атак недокументированных (недекларированных) возможностей прикладного и системного ПО, так как ценность обрабатываемой в системе информации не соответствует стоимости привлечения данных специалистов. Также предполагается отсутствие возможного сговора между нарушителями, поскольку ценность обрабатываемых данных не соответствует сложностям осуществления такого сговора и возможным выгодам от его реализации.

СКЗИ в ИСПДн применяются для защиты данных, передаваемых по внутренним каналам связи. Они исключают возможность несанкционированного ознакомления и модификации передаваемой по сети информацией. Передача информации за пределы контролируемой зоны не осуществляется. В этом случае потенциальными нарушителями, против которых данные СКЗИ применяются, являются только пользователи, расположенные в пределах контролируемой зоны.

Далее приводится обоснование необходимого к применению класса СКЗИ исходя из сформированных предположений и описания актуальности или неактуальности угроз.

Согласно положениям Приказа ФСБ № 378 от 10.07.2014 СКЗИ класса КА должны применятся в случае, если соответствует действительности хотя бы одно из следующих допущений:

1) у потенциального нарушителя СКЗИ присутствует возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ. Оператор ИС не является разработчиком используемых в ИС аппаратных и программных компонентов СФ и не владеет конструкторской документацией на них. Таким образом, можно сделать вывод о том, что нарушители не имеют возможности получения сведения, содержащиеся в конструкторской документации на аппаратные и программные компоненты СФ;

2) у потенциального нарушителя СКЗИ присутствует возможность располагать всеми аппаратными компонентами СКЗИ и СФ. Вследствие организации контрольно-пропускного режима и формирования перечня пользователей СКЗИ, ко всем аппаратным компонентам СКЗИ и СФ имеет возможность получить доступ только ответственный пользователь СКЗИ (администратор безопасности). Данные лица относится к доверенному кругу лиц, проходили инструктаж о порядке и необходимости соблюдения безопасности обработки данных. Кроме того, исходя из установленных в разделе 3 Модели угроз возможностей нарушителей, предполагается, что они обладают низким потенциалом и не обладают достаточным уровнем квалификации для реализации угроз внедрения аппаратных закладок или проведения криптоанализа посредством доступа к аппаратным

компонентам СКЗИ и СФ. Таким образом, можно сделать вывод о том, что у нарушителя отсутствует возможность располагать всеми аппаратными компонентами СКЗИ и СФ;

Согласно положениям Приказа ФСБ № 378 от 10.07.2014 СКЗИ класса КВ должны применятся в случае, если соответствует действительности хотя бы одно из следующих допущений:

1) у потенциального нарушителя СКЗИ присутствует возможность проводить лабораторные исследования, ограниченные мерами по предотвращения НСД в ИСПДн, используемых вне контролируемой зоны СКЗИ. Исходя из сформированных моделей нарушителя, можно сделать вывод о том, что потенциальный нарушитель не обладает такой возможностью (установленные в данном разделе и в разделе 3 Модели угроз возможности нарушителей, предполагают, что они обладают низким потенциалом);

2) у потенциального нарушителя СКЗИ присутствует возможность проводить работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ. Исходя из сформированных моделей нарушителя, можно сделать вывод о том, что потенциальный нарушитель не обладает такой возможностью (установленные в разделе 3 Модели угроз возможности нарушителей, предполагают, что они обладают низким потенциалом).

Согласно положениям Приказа ФСБ № 378 от 10.07.2014 СКЗИ класса КС3 должны применятся в случае, если соответствует действительности хотя бы одно из следующих допущений:

1) у потенциального нарушителя СКЗИ присутствует возможность физического доступа к СВТ, на которых реализованы СКЗИ и СФ. Вследствие организации контрольно-пропускного режима доступ к СВТ, на которых реализованы СКЗИ ViPNetCoordinator и ViPNetAdministrator имеют только ответственные пользователи СКЗИ (администраторы безопасности), которые, как уже говорилось выше, относятся к доверенному кругу лиц и не входят в состав потенциальных нарушителей. Доступ к СВТ, на которых реализованы СКЗИ ViPNetClient имеют также пользователи СКЗИ. Таким образом, внешние пользователи не могут получить физический доступ к СВТ. Пользователи СКЗИ проходили соответствующий инструктаж и ознакомлены с требованиями обеспечения безопасности. Т.к. СКЗИ используются только для шифрования передаваемых по сети данных, то несанкционированный доступ к СВТ потенциального нарушителя из состава пользователей СКЗИ (включающий возможное получение пользователями ключевой информации) не позволит им ознакомиться с защищаемой прикладной информацией на данном СВТ. Потенциально такой факт НСД может привести к последующей атаке на шифрованный трафик в процессе реализации угрозы анализ сетевого трафика, однако согласно раздела 4 Модели угроз данная угроза является неактуальной. Таким образом, можно сделать вывод о том, что комплекс реализованных мер, порядок использования СКЗИ и сформированная модель нарушителя не позволяют вследствие наличия данной возможности потенциальному нарушителя каким-либо образом скомпрометировать СКЗИ;

2) у потенциального нарушителя СКЗИ присутствует возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная реализованными в ИС мерами по противодействию НСД. Вследствие организации контрольно-пропускного режима и формирования перечня пользователей СКЗИ, возможность располагать аппаратными компонентам СКЗИ и СФ имеют только ответственные пользователи СКЗИ (в части СКЗИ ViPNetCoordinatorи ViPNetAdministrator) и пользователи СКЗИ (в части СКЗИ ViPNetClient), внешние пользователи располагать аппаратными компонентами СКЗИ и СФ не могут. Ответственные пользователи СКЗИ относятся к числу доверенных лиц и не входят в состав возможных нарушителей, пользователи СКЗИ не обладают достаточной компетенцией для внедрения аппаратных закладок или проведения криптоанализа посредством доступа к аппаратным компонентам СКЗИ и СФ. Таким образом, можно

сделать вывод о том, что комплекс реализованных мер, порядок использования СКЗИ и сформированная модель нарушителя не позволяют вследствие наличия данной возможности потенциальному нарушителя каким-либо образом скомпрометировать СКЗИ;

Согласно положениям Приказа ФСБ № 378 от 10.07.2014 СКЗИ класса КС2 должны применятся в случае, если соответствует действительности хотя бы одно из следующих допущений:

1) у потенциального нарушителя СКЗИ присутствует возможность проведения атаки в пределах контролируемой зоны. Вследствие организации контрольно-пропускного режима и формирования перечня пользователей СКЗИ, возможность проведения атаки в пределах контролируемой зоны внешними пользователями исключена, атаку могут реализовать только ответственные пользователи СКЗИ (в части СКЗИ ViPNetCoordinatoru ViPNetAdministrator) и пользователи СКЗИ (в части СКЗИ ViPNetClient). Первые относятся к числу доверенных лиц и не входят в состав возможных нарушителей, а вторые не обладают достаточной компетенцией для организации НСДв СВТ, на которых реализованы СКЗИ и СФ. Таким образом, можно сделать вывод о том, что комплекс реализованных мер и сформированная модель нарушителя не позволяют вследствие наличия данной возможности потенциальному нарушителя каким-либо образом скомпрометировать СКЗИ;

2) у потенциального нарушителя СКЗИ присутствует возможность проведения на этапе эксплуатации СКЗИ атак на документацию СКЗИ и компонентов СФ; на помещения, в которых находятся СВТ, на которых функционируют СКЗИ и СФ. Вследствие организации контрольно-пропускного режима и формирования перечня пользователей СКЗИ, возможность проведения данной атаки внешними пользователями исключена, атаку могут реализовать только ответственные пользователи СКЗИ и пользователи СКЗИ. Ответственные пользователи СКЗИ относятся к числу доверенных лиц и не входят в состав возможных нарушителей. Возможные действия на документацию СКЗИ вследствие низкой компетенции (потенциала) потенциальных нарушителей ограничиваются её уничтожением, однако на объекте ведется учет документации и фактов ее выдачи только пользователям СКЗИ, что позволяет сделать вывод о невозможности проведения атаки на документацию. В ИСПДн не используется какое-либо прикладное ПО, которое бы взаимодействовало с СКЗИ ViPNet, что позволяет сделать вывод о том, что атака на документацию компонентов СФ никак не скомпрометирует используемые СКЗИ. Возможность проведения атаки на помещения, в которых находится СВТ, на которых функционируют СКЗИ и СФ отсутствует, т.к. в разделе 3 Модели угроз установлено, что вследствие низкой ценности информации у нарушителей не имеются какие-либо средства снятия информации по техническим каналам. Таким образом, можно сделать вывод о том, что комплекс реализованных мер и сформированная модель нарушителя не позволяют вследствие наличия данной возможности потенциальному нарушителя каким-либо образом скомпрометировать СКЗИ;

3) у потенциального нарушителя СКЗИ присутствует возможность получения в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты, сведений о мерах по обеспечению контролируемой зоны, сведений и мерах по разграничению доступа в помещения, где хранятся СВТ, на которых реализованы СКЗИ и СФ. Вследствие организации контрольно-пропускного режима и формирования перечня пользователей СКЗИ, возможность получения данной информации внешними пользователями исключена, эту информацию могут получить только ответственные пользователи СКЗИ и пользователи СКЗИ. Ответственные пользователи СКЗИ относятся к числу доверенных лиц и не входят в состав возможных нарушителей. Пользователи СКЗИ не обладают достаточной компетенцией для организации НСД на СВТ или передаваемые по сети зашифрованные данные вследствие получения дополнительной информации о реализованных мерах защиты. Таким образом, можно сделать вывод о том, что комплекс реализованных мер и сформированная модель

нарушителя не позволяют вследствие наличия данной возможности потенциальному нарушителя каким-либо образом скомпрометировать СКЗИ;

4) у потенциального нарушителя СКЗИ присутствует возможность использовать штатные средства, ограниченная мерами по противодействию НСД в ИСПДн. Вследствие организации контрольно-пропускного режима и формирования перечня пользователей СКЗИ, возможность использования штатных средств для компрометации СКЗИ внешними пользователями исключена, эту средства могут использовать только ответственные пользователи СКЗИ и пользователи СКЗИ. Ответственные пользователи СКЗИ относятся к числу доверенных лиц и не входят в состав возможных нарушителей. Пользователи СКЗИ не обладают достаточной компетенцией для организации НСД или сбора штатными средствами информации, необходимой для последующей организации НСД. Таким образом, можно сделать вывод о том, что комплекс реализованных мер и сформированная модель нарушителя не позволяют вследствие наличия данной возможности потенциальному нарушителя каким-либо образом скомпрометировать СКЗИ.

Таким образом, по результатам анализа описанных допущений можно сделать вывод о том, что в ИСПДн достаточно применять криптосредства класса КС1 и выше.

Приложение 6 к приказу
№ 300 от 31.08.2022г.

ИНСТРУКЦИЯ
по порядку учета, хранения съемных носителей персональных данных в муниципальном бюджетном образовательном учреждение «Кезская средняя общеобразовательная школа №2» Кезского района Удмуртской Республики

1. Общие положения

1.1. Ответственный за организацию обработки персональных данных - технический специалист, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники (далее - Администратор).

1.2. АРМ - автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

1.3. ИБ - информационная безопасность - комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

1.4. ИСПД - информационная система персональных данных - это совокупность программных и технических средств (компьютеры, принтеры, сканеры, коммутационное оборудование и т.д.), на которых обрабатываются персональные данные.

1.5. Съемный носитель ПД - любой материальный объект, используемый для хранения и передачи электронной информации, содержащей персональные данные (дискеты, флеш- накопитель, съемные жесткие диски, оптические диски и т.д.).

1.6. Паспорт ПК - документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

1.7. ПД - персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.8. ПК - персональный компьютер.

1.9. ПО - программное обеспечение вычислительной техники.

1.10. ПО вредоносное - ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

1.11. ПО коммерческое- ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

1.12. Пользователь- муниципальный служащий и работник Департамента образования (далее- Администрация, сотрудник), использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

2. Порядок использования съемных носителей ПД

2.1. Под использованием съемных носителей ПД при работе с ИСПД понимается их подключение к инфраструктуре ИСПД с целью обработки, приема/передачи информации между ИСПД и носителями информации.

2.2. В ИСПД допускается использование только учтенных съемных носителей ПД, которые являются собственностью МДОУ и подвергаются регулярной ревизии и контролю.

2.3. К съемным носителям ПД предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ПД).

2.4. Съемные носители ПД предоставляются сотрудникам по инициативе

руководителей структурных подразделений в случаях:

– необходимости выполнения вновь принятыми сотрудниками своих должностных обязанностей;

– возникновения производственной необходимости по обработки ПД.

3. Порядок учета, хранения и обращения со съемными носителями ПД

3.1. Все находящиеся на хранении и в обращении съемные носители ПД подлежат учету.

3.2. Каждый съемный носитель ПД с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.3. Учет и выдачу съемных носителей ПД осуществляют заместители заведующего МДОУ на которых возложены функции хранения съемных носителей ПД. Факт выдачи съемного носителя ПД фиксируется в журнале учета защищаемых носителей информации по форме согласно приложению № 1 к настоящей Инструкции.

3.4. Сотрудники получают учтенный съемный носитель ПД от заместителей заведующего МДОУ для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета защищаемых носителей информации. По окончании работ пользователь сдает съемный носитель ПД для хранения заместителям заведующего МДОУ, о чем делается соответствующая запись в журнале учета защищаемых носителей информации.

3.5. При использовании сотрудниками съемных носителей ПД необходимо:

3.5.1. соблюдать требования настоящей Инструкции;

3.5.2. использовать съемные носители ПД исключительно для выполнения своих служебных обязанностей;

3.5.3. ставить в известность администратора безопасности информации о любых фактах нарушения требований настоящей Инструкции;

3.5.4. бережно относиться к съемным носителям ПД;

3.5.5. обеспечивать физическую безопасность съемным носителям ПД всеми разумными способами;

3.5.6. извещать администратора безопасности информации о фактах утраты (кражи) съемного носителя ПД.

3.6. При использовании съемных носителей ПД запрещено:

3.6.1. использовать съемные носители ПД в личных целях;

3.6.2. передавать съемные носители ПД другим лицам (за исключением администратора безопасности информации);

3.6.3. хранить съемные носители ПД вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

3.6.4. выносить съемные носители ПД из помещений Департамента образования, в которых ведётся обработка персональных данных для работы с ними на дому и т.д.

3.7. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником между ИСПД и неучтенными (личными) съемными носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администратором безопасности информации заранее). Администратор безопасности информации оставляет за собой право блокировать или ограничивать использование съемных носителей информации.

3.8. Информация об использовании сотрудником съемных носителей ПД в ИСПД протоколируется и, при необходимости, может быть представлена администратором безопасности информации.

3.9. В случае выявления фактов несанкционированного и/или нецелевого использования съемных носителей ПД инициализируется служебная проверка, проводимая комиссией по защите персональных данных МДОУ (далее - Комиссия).

3.10. По факту выясненных обстоятельств Комиссия составляется акт расследования инцидента для принятия мер согласно локальным правовым актам и действующему законодательству.

3.11. Информация, хранящаяся на съемных носителях ПД, подлежит обязательной проверке на отсутствие вредоносного ПО.

3.12. При отправке или передаче персональных данных адресатам на съемные носители ПД записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях ПД осуществляется в порядке, установленном для документов для служебного пользования.

3.13. Вынос съемных носителей ПД для непосредственной передачи адресату осуществляется только с письменного разрешения администратора безопасности информации.

3.14. В случае утраты или уничтожения съемных носителей ПД либо разглашении содержащихся в них сведений, немедленно ставится в известность администратор безопасности информации. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета бумажных и съемных носителей ПД.

3.15. Съемные носители ПД, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей ПД осуществляется Комиссией. По результатам уничтожения съемных носителей ПД составляется акт уничтожения ПД согласно приложению № 2 к настоящей Инструкции.

3.16. В случае увольнения или перевода сотрудника в другое структурное подразделение, предоставленные съемные носители ПД изымаются.

4. Ответственность

4.1. Сотрудники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством и локальными правовыми актами.