Принято
заседании педагогического Совета
Протокол от 12.10.2023г. № 12

Утверждено приказом директора на
МОУ «Каменноключинская ООШ»
от 13.10.2023 г. № 172-ОД

Положение об обработке и защите персональных данных в информационных системах МОУ «Каменноключинская ООШ»

1.Общие положения.

Настоящее «Положение об обработке и защите персональных данных в информационных системах МОУ «Каменноключинская ООШ» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России. Положение разработано в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных МОУ «Каменноключинская ООШ» (далее – ИСПДн).

Положение определяет порядок работы коллектива МОУ «Каменноключинская ООШ» (далее - ОУ) в ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений при их обработке, порядок обучения коллектива ОУ практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2.Порядок предоставления допуска пользователей к работе в ИСПДн

Настоящий порядок определяет действия коллектива ОУ в ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

Первоначальный допуск пользователей к работе в ИСПДн осуществляется на основании приказа, который издается директором ОУ (далее директор). В приказе определяется список сотрудников, допущенных к работе в ИСПДн.

С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации и выполнения необходимых мероприятий по обеспечению безопасности в ИСПДн директором на основании приказа назначается ответственный за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных обязан, ознакомится с инструкцией ответственного за организацию обработки персональных данных под роспись (Приложение 1).

Ответственный за организацию обработки персональных данных вносит предложение директору о назначении администратора безопасности. Администратор безопасности назначается директором на основании приказа. Администратор безопасности обязан, ознакомится с инструкцией администратору безопасности информации на автоматизированных системах обработки персональных данных МОУ «Каменноключинская ООШ» под роспись (Приложение 2).

С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе в ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться, и работать в ИСПДн. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя запрещено.

В дальнейшем, процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется администратором безопасности.

Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное значение пароля, которое он обязан сменить при первом же входе в систему.

Привилегии пользователей задаются в разрешительной системе доступа к ИСПДн.

3.Порядок работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

Перед началом работы в ИСПДн, сотрудники ОУ, допущенные к работе с ПДн, принимают под роспись обязательство о неразглашении персональных данных (Приложение 3).

Пользователь обязан, ознакомится с инструкцией пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники МОУ «Каменноключинская ООШ» (Приложение 4), а также с инструкцией пользователя, по проведению антивирусного контроля на объектах вычислительной техники МОУ «Каменноключинская ООШ» (Приложение 5) под роспись. Вход пользователя в систему должен осуществляться по выдаваемому ему электронному идентификатору и по персональному паролю;

Запись информации, содержащей ПДн, должна осуществляться только на машинные носители информации, соответствующим образом учтенные в Журнале учета защищаемых носителей информации. Ответственным за ведение Журнала учета является администратор безопасности;

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн.

В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения;

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан: -строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн; хранить в тайне свой пароль (пароли). В соответствии с п. 7. данного Положения и с установленной периодичностью менять свой пароль (пароли);

хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для посторонних месте;

выполнять требования Положения по организации антивирусной защиты в полном объеме. Немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении

компрометации личных ключей и паролей, а также при обнаружении: фактов совершения попыток несанкционированного доступа (далее - НСД) к ИСПДн;
несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн; отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения; некорректного функционирования установленных на компьютеры технических средств защиты; непредусмотренных отводов кабелей и подключенных устройств.
Пользователю категорически запрещается:
- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях; - самовольно вносить какие-либо изменения в конфигурацию аппаратнопрограммных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц; - записывать и хранить ПДн на неучтенных машинных носителях информации;
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры); - оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие ПДн;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению конфиденциальности ПДн; - размещать средства отображения информации (монитор, принтер и т.п.) таким образом, чтобы с них существовала возможность визуального считывания информации посторонними лицами. Администратор безопасности обязан: знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;
производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом: реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);
вводить описания пользователей ИСПДн в информационную базу системы разграничения доступа в ИСПДн; своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;
проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;
контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;
осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;
настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;
организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации; периодически тестировать функции СЗИ от НСД с использованием специальных средств анализа защищенности, особенно при изменении

программной среды и полномочий исполнителей; восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;
вести две копии программных средств СЗИ от НСД и контролировать их работоспособность; периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;
проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание персональных данных на носителях информации); присутствовать (участвовать) в работах по внесению изменений в аппаратнопрограммную конфигурацию ИСПДн;
вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

4.Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных, защищаемой информации и средств защиты информации

Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в Журнале учета носители. Администратор безопасности обязан осуществлять периодическое резервное копирование персональных данных.

Носители информации, предназначенные для создания резервной копии и хранения персональных данных, выдаются установленным порядком администратором безопасности.

По окончании процедуры резервного копирования электронные носители сдаются на хранение администратору безопасности, или директору.

При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания.

При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся у администратора безопасности.

После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

Ответственность за проведение резервного копирования, мероприятий по восстановлению работоспособности технических средств, мероприятий по восстановлению средств защиты информации возлагается на администратора безопасности.

5.Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных

Перед началом работы в ИСПДн пользователи должны ознакомиться с требованиями настоящего Положения под роспись;

Пользователи должны продемонстрировать администратору безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения;

Ответственным за организацию обучения и оказание методической помощи в ОУ является администратор безопасности;

6.Правила антивирусной защиты

Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение.

К использованию на компьютерах допускаются только лицензионные антивирусные средства; Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности;

Администратор безопасности осуществляет периодическое обновление антивирусных средств и контроль их работоспособности;

Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы;

Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров;

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель);

Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль;

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка ИСПДн;

На компьютеры пользователей запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации; При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан: приостановить обработку данных в ИСПДн;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе; совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования; провести лечение или уничтожение зараженных файлов. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего

Положения возлагается на администратора безопасности;

Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

7. Правила парольной защиты

Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

При доступе пользователя в систему должна осуществляться идентификация и проверка подлинности по идентификатору и паролю, а также с использованием электронных идентификаторов.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

- пароль должен быть длиной не менее шести буквенно-цифровых символов;
- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры; - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущих;
- пользователь не имеет права сообщать личный пароль другим лицам.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 365 дней. Удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой, на основании приказа директора. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри учреждения и другие обстоятельства) администратора безопасности.

В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по изменению его пароля. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности. В АИС «Электронная школа» ежемесячно менять пароли с занесением в «Журнал по смене паролей» для пользователей системы «Администратор», «Сотрудник», «Учитель», «Классный руководитель». Ответственным за своевременным изменением паролей является администратор безопасности.

8. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

Право на установку, обновление и модификацию общесистемного и прикладного программного обеспечения компьютеров ИСПДн предоставляется администратору безопасности.

Право внесения изменений в конфигурацию аппаратно-программных средств защиты информации предоставляется администратору безопасности, по согласованию с директором ОУ.

Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме администратора безопасности запрещено. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем. Установка и обновление ПО (системного, прикладного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.).

Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.
После установки (обновления) ПО, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки.
При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

9. Порядок контроля обеспечения защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления.

Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

Основными задачами контроля являются:

проверка организации выполнения мероприятий по защите информации в учреждении, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

выявление демаскирующих признаков объектов ИСПДн;

уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программнотехнических воздействий на информацию;

проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

10. Порядок охраны и допуска посторонних лиц в помещения ИСПДн

В ОУ должна быть предусмотрена физическая охрана технических средств ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации.

В помещениях должна быть установлена охранная и пожарная сигнализация.

Серверное и коммутационное оборудование ИСПДн должно находиться под надежным замком, в отдельном помещении или запирающемся шкафу, ключ должен храниться у администратора безопасности.

Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не

вскрывается, а составляется акт, в присутствии сторожа. О происшествии немедленно сообщается директору.

11. Заключительные положения

Требования настоящего Положения обязательны для всего коллектива ОУ, обрабатывающих персональные данные.

Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 1
к Положению об обработке и защите персональных данных
в информационных системах МОУ «Каменноключинская ООШ»

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 МОУ "Каменноключинская ООШ" (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 № 2
к Положению об обработке и защите персональных данных
в информационных системах МОУ «Каменноключинская ООШ»

ИНСТРУКЦИЯ АДМИНИСТРАТОРУ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ МОУ «КАМЕННОЛЮЧИНСКАЯ ООШ»

Настоящая Инструкция определяет функции, права и обязанности Администратора безопасности информации на автоматизированных системах обработки персональных данных МОУ «Каменноключинская ООШ».
Администратор безопасности информации - субъект доступа в автоматизированную систему, владеющий паролем администратора безопасности информации и имеющий право изменять настройки системы защиты от НСД.
Администратор безопасности информации АС назначается директором школы МОУ «Каменноключинская ООШ»

В обязанности администратора безопасности информации входит:

1 Заводить/удалять новых пользователей АС;
2 Назначать/отменять пароли для пользователей АС;
3 Редактировать параметры (полномочия) пользователей АС;

4 Просматривать системный журнал на предмет попыток НСД к информации и анализировать случаи разрушения, уничтожения или порчи информации;

5 Проводить плановую смену паролей пользователей АС;
6 Проводить резервное копирование данных АС;
7 Следить за исправностью средств защиты, установленных в АС;
8 Периодически контролировать наличие на системных блоках АС целостности специальных защитных знаков;
9 Периодически контролировать неизменность состава технических средств, входящих в АС и неизменность расположения технических средств АС;
10 Постоянно контролировать выполнение пользователями АС «Инструкции пользователя АС»;
11 Осуществлять периодическое обновление антивирусных средств (баз данных), установленных на АС, контроль за соблюдением пользователями порядка и правил проведения антивирусного тестирования АС;
12 Докладывать обо всех нарушениях порядка обработки конфиденциальной информации в АС директору школы МОУ «Каменноключинская ООШ».

Работа с пользователями:

1 Назначение/удаление пользователя АС осуществляется администратором безопасности информации АС на основании «Списка должностных лиц, допущенных к обработке конфиденциальной информации в АС», и сопровождается установкой/отменой персональных паролей для пользователей АС;
2 Редактирование параметров (полномочий) пользователей АС выполняется администратором безопасности информации с учетом полномочий пользователя по отношению к защищаемым информационным ресурсам в данной АС;

3 Плановая смена паролей осуществляется администратором безопасности информации в присутствии пользователя АС с периодичностью не реже одного раза в квартал или досрочно по указанию начальника;

4 Администратор безопасности информации АС обязан разрешать конфликтные ситуации пользователей при входе в систему с персональными паролями;

5 Администратор безопасности информации АС следит за выполнением пользователями «Инструкции пользователя АС».

Ремонтные и регламентные работы в АС:

1. Администратор безопасности информации следит за исправностью средств защиты, установленных в АС, и докладывает о неисправностях директору школы МОУ «Каменноключинская ООШ». На время ремонта технических средств АС обработка информации в АС ЗАПРЕЩЕНА..

Резервное копирование данных:

1. Резервное копирование баз данных производится администратором безопасности информации АС с периодичностью, определенной в соответствии с режимом обработки конфиденциальной информации в АС (по мере ее накопления, но не реже одного раза в месяц), а также по указанию директора школы МОУ «Каменноключинская ООШ».

2. Резервные копии хранятся на учтенных в школе магнитных носителях (дискетах, винчестерах, CD-дисках).

Администратор безопасности информации АС имеет право:

1. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

2. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

ЗАПРЕЩАЕТСЯ:

Передавать пароль администратора безопасности информации другим лицам.

Администратор безопасности информации несет личную ответственность за его сохранность.

Приложение № 3
к Положению об обработке и защите персональных данных
в информационных системах МОУ «Каменноключинская ООШ»

Соглашение о неразглашении
персональных данных субъекта

Я, _____, паспорт серии _____, номер _____, выданный _____
« ___ » _____ _____ года, понимаю, что получаю доступ к персональным данным работников и/или обучающихся_____
_____. (наименование организации)
Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных. Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный. В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в «Положении об обработке и защите персональных данных» требования. Я подтверждаю, что не имею права разглашать сведения:
- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;

- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- подлинники и копии приказов по личному составу и основной деятельности;
- личные дела и трудовые книжки сотрудников;

- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
- копии отчетов, направляемые в органы статистики.

- фото и видео материалы. Я предупрежден о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со ст. 90 Трудового Кодекса Российской Федерации.
« ___ » _____ 20__ г. _____ (подпись)

Приложение № 4
к Положению об обработке и защите персональных данных
в информационных системах МОУ «Каменноключинская ООШ»

ИНСТРУКЦИЯ
пользователя, осуществляющего обработку персональных данных
на объектах вычислительной техники МОУ "Каменноключинская ООШ"

I. Общие положения

1. Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники (далее - Инструкция), регламентирует основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) образовательного учреждения (далее - ОУ).

2. Инструкция регламентирует деятельность пользователя, который имеет допуск к обработке соответствующих категорий персональных данных и обладает необходимыми навыками работы на ПЭВМ.

II. Обязанности пользователя

3. При выполнении работ в пределах своих функциональных обязанностей пользователь несет персональную ответственность за соблюдение требований нормативных документов по защите информации.

4. Пользователь обязан:

- выполнять требования Инструкции по обеспечению режима конфиденциальности проводимых работ;
- при работе с персональными данными исключать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, а также располагать во время работы экран видеомонитора так, чтобы отображаемая на нем информации была недоступна для просмотра посторонними лицами;
- соблюдать правила работы со средствами защиты информации, а также установленный режим разграничения доступа к техническим средствам, программам, данным и файлам с персональными данными при ее обработке;
- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня производить стирание остаточной информации с жесткого диска ПЭВМ; • оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- не допускать "загрязнения" ПЭВМ посторонними программными средствами;
- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, меры предотвращения ухудшения ситуации;

знать и соблюдать правила поведения в экстренных ситуациях, порядок действий при ликвидации последствий аварий;

- помнить личные пароли и персональные идентификаторы;
- знать штатные режимы работы программного обеспечения, пути проникновения и распространения компьютерных вирусов;
- при применении внешних носителей информации перед началом работы проводить их проверку на наличие компьютерных вирусов.

5.При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) пользователь должен

провести внеочередной антивирусный контроль своей рабочей станции. В случае обнаружения зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, администратора системы ;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

6. Пользователю ПЭВМ запрещается:

- записывать и хранить персональные данные на неучтенных в установленном порядке машинных носителях информации;
- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
- самостоятельно подключать к ПЭВМ какие-либо устройства, а также вносить изменения в состав, конфигурацию и размещение ПЭВМ;
- самостоятельно устанавливать и/или запускать на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- осуществлять обработку персональных данных в условиях, позволяющих просматривать их лицами, не имеющими к ним допуска, а также нарушающих требования к эксплуатации ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения, на исполнение которых предусмотрены утвержденными регламентами и инструкциями;
- бесконтрольно оставлять ПЭВМ с загруженными персональными данными, установленными маркированными носителями, электронными ключами и выведенными на печать документами, **содержащими персональные данные.**

III. Права пользователя

7. Пользователь ПЭВМ имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;
- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

IV. Заключительные положения

8. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

9. Работники подразделений ОУ и лица, выполняющие работы по договорам и контрактам и имеющие отношение к обработке персональных данных на объектах вычислительной техники, должны быть ознакомлены с Инструкцией под расписку

Приложение № 5
к Положению об обработке и защите персональных данных
в информационных системах МОУ «Каменноключинская ООШ»

ИНСТРУКЦИЯ
пользователя, по проведению антивирусного контроля
на объектах вычислительной техники МОУ «Каменноключинская ООШ»

1. Настоящая Инструкция предназначена для пользователей, хранящих и обрабатывающих информацию на объектах вычислительной техники МОУ «Каменноключинская ООШ» (далее ОВТ МОУ «Каменноключинская ООШ»
2. В целях обеспечения антивирусной защиты на ОВТ МОУ «Каменноключинская ООШ» производится антивирусный контроль.
3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации.
4. К применению на ОВТ МОУ «Каменноключинская ООШ» допускаются лицензионные антивирусные средства.
5. На ОВТ МОУ «Каменноключинская ООШ» запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.
6. Пользователь ОВТ МОУ «Каменноключинская ООШ» при работе с машинными носителями (МН) информации обязан перед началом работы осуществить проверку МН на предмет отсутствия компьютерных вирусов.
7. Ярлык для запуска антивирусной программы должен быть вынесен в окно "Рабочий стол" системы Windows. Приложение № 5 к Положению об обработке и защите персональных данных в информационных системах МОУ «Каменноключинская ООШ»
8. Пользователь осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.
9. Пользователь проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.
10. При обнаружении компьютерного вируса пользователь обязан немедленно поставить в известность администратора безопасности информации и прекратить какие-либо действия на ОВТ МОУ «Каменноключинская ООШ»
11. Администратор безопасности информации проводит, в случае необходимости, лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

12. В случае обнаружения на МН нового вируса, не поддающегося лечению, администратор безопасности информации обязан прекратить использование МН. 13. В случае обнаружения на ЖМД не поддающегося лечению вируса, администратор безопасности информации обязан поставить в известность руководство, прекратить работу на ОВТ МОУ «Каменноключинская ООШ» и в возможно короткие сроки устранить проблему.

Приложение № 6
к Положению об обработке и защите персональных данных
в информационных системах МОУ «Каменноключинская ООШ»

ЧАСТНАЯ МОДЕЛЬ УГРОЗ
безопасности персональных данных информационной системы персональных данных
«АИС Электронная школа» в МОУ «Каменноключинская ООШ»

Обозначения и сокращения.
АРМ - автоматизированное рабочее место
ВИ - видовая информация
ВТСС - вспомогательные технические средства и системы
ИСПДн - информационная система персональных данных
КЗ - контролируемая зона
МЭ - межсетевой экран
НДВ - недекларированные возможности
НСД - несанкционированный доступ
ОБПДн - обеспечение безопасности персональных данных
ОС - операционная система
ПДн - персональные данные
ПМВ - программно-математическое воздействие
ПО - программное обеспечение
ПЭМИН - побочные электромагнитные излучения и наводки
РИ - речевая информация
СВТ - средство вычислительной техники
СЗИ - средство защиты информации
СПИ - стеганографическое преобразование информации
СЭУПИ - специальные электронные устройства перехвата информации
ТКУИ - технический канал утечки информации
ТСОИ - технические средства обработки информации
УБПДн - угрозы безопасности персональных данных

1. **Термины и определения**

В настоящем документе используются следующие термины и их определения:
Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.
Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных

технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи. **Вирус (компьютерный, программный**) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению. **Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

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

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных. *Информационная система персональных данных* - это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств. *Информационные технологии* - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации. *Контролируемая зона* - это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за

информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

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

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

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

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов. **Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания. **Пользователь информационной системы персональных данных** - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем. **Субъект доступа (субъект)** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. Общие положения.

Настоящая «Частная модель угроз безопасности персональных данных информационной системы «АИС Электронная школа» (далее – Модель угроз) содержит систематизированный перечень угроз безопасности ПДн информационной системы персональных данных «АИС Электронная школа» (далее – ИСПДн).

Модель угроз содержит данные по УБПДн, реализация которых может привести к нарушению безопасности ПДн, обрабатываемых в ИСПДн.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов ИСПДн.

Разработка Модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности ПДн, обрабатываемых в ИСПДн, и проектирования СЗПДн. Модель угроз необходима для:

– анализа защищённости ИСПДн от УБПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

– разработки СЗПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием мер по обеспечению безопасности ПДн, предусмотренных для соответствующего уровня защищённости ПДн;

– проведения мероприятий, направленных на предотвращение НСД к ПДн и (или) передачи ПДн лицам, не имеющим права доступа к ПДн;
– недопущения воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
– контроля (мониторинга) за обеспечением уровня защищённости Пдн, обрабатываемых в ИСПДн. В Модели угроз представлено описание ИСПДн и их структурно функциональных характеристик, описание УБПДн, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИСПДн, способов реализации УБПДн и последствий от нарушения свойств безопасности информации, а также произведён анализ УБПДн
Анализ УБПДн включает:
– описание угроз;
– оценку вероятности возникновения угроз;
– оценку реализуемости угроз;
– оценку опасности угроз;
– определение актуальности угроз.
В процессе функционирования ИСПДн, предполагается конкретизировать и пересматривать данную Модель угроз. УБПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых уязвимостей, источников угроз, развития способов и средств реализации УБПДн в ИСПДн.
Модель угроз может быть пересмотрена:

– на основе периодически проводимых анализа и оценки УБПДн с учетом особенностей и (или) изменений ИСПДн;
– по результатам мероприятий по контролю за выполнением требований по защите информации в ИСПДн

3. Исходные данные по ИСПДн.

3.1. Назначение и состав информационной системы персональных данных «АИС Электронная школа» В ИСПДн обрабатываются ПДн субъектов ПДн МОУ «Каменноключинская ООШ», к которым относятся:
– учащиеся
– родители (законные представители) учащихся;
– будущие первоклассники
– выпускники.
В ИСПДн обрабатываются следующие Пдн:
учащегося, выпускники, будущие первоклассники
Фамилия Имя Отчество
Дата рождения
Пол
Место жительства
Место регистрации
Домашний телефон
Свидетельство о рождении, паспорт (с 14 лет)
Номер личного дела
Отметки\оценки текущей и итоговой успеваемости
СНИЛС
Класс
Фото
Видео
Дипломы и грамоты
Паспортные данные родителей (законных представителей)

Фамилия
Имя
Отчество
Дата рождения
Телефон

Должность Место работы
E-mail
Дети
СНИЛС Номер СНИЛС
Паспортные данные

3.2. Условия размещения ИСПДн.

ИСПДн обеспечивает информационный обмен ПДн с использованием средств автоматизации с АУ УР «Региональный центр информатизации и оценки качества образования», являющееся оператором ведомственной региональной АИС «Электронная школа» (Адрес: 426057, г. Ижевск, ул. Ленина, д. 16).

3.3. Порядок ввода, хранения и передачи персональных данных в ИСПДн.

Получение ПДн происходит непосредственно от субъекта ПДн и (или) родителей (законных представителей) субъекта ПДн: В процессе обработки ПДн хранятся в ИСПДн АИС «Электронная школа» (Адрес: 426057, г. Ижевск, ул. Ленина, д. 16). Трансграничная передача ПДн не осуществляется.

3.4. Режим и степень участия субъектов в обработке персональных данных

В процессе обработки ПДн участвуют следующие категории субъектов:

– пользователи ИСПДн МОУ «Каменноключинская ООШ»;

– системные администраторы МОУ «Каменноключинская ООШ».

Пользователями ИСПДн являются административно-управленческий и педагогический персонал МОУ «Каменноключинская ООШ», в должностные обязанности которых входит обработка ПДн. Системные администраторы МОУ «Каменноключинская ООШ» выполняют обслуживание и настройку, поддерживают работоспособность АРМ, выполняют установку и настройку ПО, обслуживание и конфигурирование, разграничивают права доступа субъектов доступа к объектам доступа в ИСПДн.

5.4. Реализованные меры защиты.

Разработано и утверждено Положение об обработке персональных данных работников и обучающихся МОУ «Каменноключинская ООШ»

Приказом назначено лицо, ответственное за организацию обработки персональных данных. Опубликован и размещен на сайте организации документ, определяющий Политику в отношении обработки персональных данных, а также лист согласия на обработку персональных данных. Разработаны локальные акты по вопросам обработки персональных данных.

Осуществляется внутренний контроль соответствия обработки персональных данных Федеральному закону от 27.07.2006 No 152- ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных. Работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

Разработана частная модель угроз безопасности.

Компьютеры с персональными данными защищены секретным паролем, используются системы паролей при работе в сети (портале), обеспечено ограничение доступа к компьютерной технике для определенных категорий работников.

4.Классификация угроз безопасности.

Классификация ИСПДн - это присвоение каждой идентифицированной ИСПДн класса (К1, К2, К3, К4), соответствующего её индивидуальным признакам.
В соответствии с рекомендациями ФСТЭК России, класс ИСПДн определяется с учётом категорий и объёма обрабатываемых ПДн, и ей должен быть присвоен буквенно-цифровой индекс К1, К2, К3 или К4.
Типовым ИСПДн могут быть присвоены следующие классы:
– класс 1 (К1) – информационные системы, для которых нарушения могут привести к значительным негативным последствиям для субъектов персональных данных;
– класс 2 (К2) – информационные системы, для которых нарушения могут привести к негативным последствиям для субъектов персональных данных;
– класс 3 (К3) – информационные системы, для которых нарушения могут привести к незначительным негативным последствиям для субъектов персональных данных;
– класс 4 (К4) – информационные системы, для которых нарушения не приводят к негативным последствиям для субъектов персональных данных.
Категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни. Данные этой категории не обрабатываются в ИСПДн школы.
Разъяснение: данные о больничном или декретном отпуске, обрабатываемые в бухгалтерии – не являются ПДн 1 категории. Это не информация о состоянии здоровья и вообще не относится к персональным данным. Это информация о временной нетрудоспособности (именно так эти данные должны быть отражены в «Отчёте о внутренней нетрудоспособности» в разделе, описывающем бухгалтерскую систему).
Категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1. Это совокупность данных 3 категории с еще какими-либо данными. Например, сами по себе данные об образовании в совокупности с данными 4 категории (например, ФИО), не образуют данных 2 или 3 категории – это все так же останутся данные 4 категории. Но если данные об образовании обрабатываются вмести с данными 3 категории (ФИО и адрес прописки), то эта совокупность данных становится данными 2 категории.
Категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных. Под идентификацией понимается – однозначное выделение субъекта из множества. К персональным данным позволяющим идентифицировать человека относятся такие данные, которые позволяют установить личность человека.
Объяснение: обработка только фамилии, имени и отчества – не позволяет идентифицировать человека, т.к. встречаются полные однофамильцы. Наиболее часто встречающиеся совокупности данных, позволяющих идентифицировать субъекта:
– паспортные данные (полностью);
– ФИО (полностью) + дата рождения;
– ФИО (полностью) + адрес проживания;
– ФИО (полностью) + должность (если в базе данных указано название организации);
– ФИО + фотография (качества не хуже, чем на паспорте).
Объяснение: совокупность данных позволяющих идентифицировать субъекта (например, ФИО + дата рождения + адрес проживания) относится к 2 категории, как к данным позволяющим идентифицировать человека и получить о нем дополнительные сведения.
Объяснение: обработка других данных о субъекте вместе с данными 3 категории (например, ФИО + дата рождения + данные об образовании), относит персональные данные к 2 категории. **Объяснение**: при определении объема ПДн бухгалтерские системы имеют Хнпд равный 3. **Категория 4** – обезличенные и / или общедоступные персональные данные. Это данные не позволяющие идентифицировать человека.

Наиболее часто встречающиеся совокупности данных, не позволяющих идентифицировать субъекта:

– фамилия и инициалы + любые другие данные;

– порядковый номер + любые другие данные.

Обезличивание данных, является одним из основных способов понижения класса ИСПДн.

В МОУ «Каменноключинская ООШ» обрабатываются следующие персональные данные:

ФИО, даты рождения, пол, серии и номер документа удостоверяющего личность, домашние адреса и телефоны, семейное положение, а так же различные типы документов для участия в ГИА и ЕГЭ. Таким образом, категория ПДн (Хпд), обрабатываемых в ИСПДн может быть отнесена **ко 2-й категории**, так как позволяют идентифицировать субъектаПДн и получить о нём дополнительную информацию, за исключением ПДн, относящейся к 1-й категории (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни). В зависимости от объёма обрабатываемых ПДн (Хнпд) может быть присвоено значение 3 . Класс ИСПДн МОУ «Каменноключинская ООШ» определяется в соответствии с таблицей №1

Хнпд Хпд	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

По данным характеристикам обрабатываемых ПДн ИСПДн школы относится к специальной информационной системе, так как в ИСПДн кроме обеспечения конфиденциальности ПДн, требуется обеспечить защищённость от уничтожения ПДн. МОУ «Каменноключинская ООШ» может быть присвоен класс 3 (К3 - специальная) – информационные системы, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПДн.

1. **Классификация угроз безопасности персональных данных.**

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы. К характеристикам ИСПДн, обусловливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в ИСПДн персональных данных, структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Информационные системы ПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке ПДн.

Основными элементами ИСПДн являются:

персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;

информационные технологии, применяемые при обработке ПДн;

технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационновычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенноцифровой информации) (далее - технические средства ИСПДн);

программные средства (операционные системы, системы управления базами данных и т.п.); средства защиты информации;

вспомогательные технические средства и системы (ВТСС) - технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях (далее - служебные помещения), в которых расположены ИСПДн, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн.

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ). Основными элементами канала реализации УБПДн являются:

- источник УБПДн - субъект, материальный объект или физическое явление, создающиеУБПДн;

- среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

- носитель ПДн - физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

По способам реализации УБПДн выделяются следующие классы угроз:

- угрозы, связанные с НСД к ПДн (в том числе угрозы внедрения вредоносных программ);

- угрозы утечки ПДн по техническим каналам утечки информации;

- угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

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

- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;

- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого

осуществляется блокирование ПДн. По используемой уязвимости выделяются следующие классы угроз:
- угрозы, реализуемые с использованием уязвимости системногоПО;
- угрозы, реализуемые с использованием уязвимости прикладного ПО;
- угрозы, возникающие в результате использования уязвимости, вызванной наличием вАС аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;
- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей СЗИ.
По объекту воздействия выделяются следующие классы угроз:
- угрозы безопасности ПДн, обрабатываемых на АРМ;
- угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);
- угрозы безопасности ПДн, передаваемых по сетям связи; - угрозы прикладным программам, с помощью которых обрабатываются ПДн;
- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

6.Общая характеристика результатов несанкционированного или случайного доступа

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:
- нарушению конфиденциальности (копирование, неправомерное распространение); - нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).
Нарушение конфиденциальности может быть осуществлено в случае утечки информации:
- копирования ее на отчуждаемые носители информации;
- передачи ее по каналам передачи данных;
- при просмотре или копировании ее в ходе ремонта, модификации и утилизации программно-аппаратных средств;
- при "сборке мусора" нарушителем в процессе эксплуатации ИСПДн.

Нарушение целостности информации осуществляется за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:
- микропрограммы, данные и драйвера устройств вычислительной системы;
- программы, данные и драйвера устройств, обеспечивающих загрузку операционной системы;
- программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) операционной системы; - программы и данные прикладного программного обеспечения; - программы и данные специального программного обеспечения;
- промежуточные (оперативные) значения программ и данных в процессе их обработки (чтения/записи, приема/передачи) средствами и устройствами вычислительной техники.

Нарушение целостности информации в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.
Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью: конфигурацией сети;
адресами и маршрутизацией передачи данных в сети;

функциональным контролем сети;
безопасностью информации в сети.
Нарушение доступности информации обеспечивается путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.
Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:
средств обработки информации; средств ввода/вывода информации;
средств хранения информации;
аппаратуры и каналов передачи; средств защиты информации.

7.Типовые модели угроз безопасности ПДн, обрабатываемых в АРМ, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

При обработке ПДн на автоматизированном рабочем месте, имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующихУБПДн:
- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теми же условиями и факторами, что и для автоматизированного рабочего места, не имеющего подключения к сетям общего пользования и (или) сетям международного информационного обмена.
Угрозы НСД в ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.
Угрозы НСД в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования.
Угрозы из внешних сетей включают в себя: - угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа "Отказ в обслуживании";
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

7.1. Классификация вероятного нарушителя безопасности ИСПДн.

Потенциальными нарушителями безопасности ИСПДн «АИС Электронная школа» МОУ «Каменноключинская ООШ» могут быть:
– внешние нарушители, осуществляющие атаки из-за пределов КЗ ИСПДн;
– внутренние нарушители, осуществляющие атаки, находясь в пределах КЗ ИСПДн.
Внешний нарушитель имеет следующие возможности:
– осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;

– осуществлять деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах КЗ режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к ИСПДн и контролю порядка проведения работ.

Таблица 3 – Классификация нарушителей ИСПДн «АИС Электронная школа

Категория нарушителя	**Описание нарушителя**	**Потенциальный нарушитель в ИСПДн**
Н0	К категории Н0 относятся лица, не имеющие санкционированного доступа к ИСПДн. Лицо этой категории, может: – осуществлять НСД к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок; – осуществлять НСД через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами КЗ	Лица, не имеющие санкционированного доступ к ИСПДн, осуществляющие атаки из-за пределов КЗ. К данным лицам относятся: – посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке; – криминальные структуры.
Н1	К категории Н1 относятся лица, не имеющие санкционированного доступа к ИСПДн. Лица этой категории обладают всеми возможностями лиц категории Н0 и дополнительно им могут быть известны, полученные в рамках предоставленных полномочий, а также в результате наблюдений сведения о мерах защиты применяемых в ИСПДн.	Лица, не имеющие санкционированного доступа к ИСПДн, осуществляющие атаки из-за пределов КЗ ИСПДн, обладающие сведениями о мерах защиты объектов, в которых размещены ресурсы ИСПДн. К данным лицам относятся сотрудники МОУ «Каменноключинская ООШ», не допущенные к ИСПДн, а также бывшие сотрудники МОУ «Каменноключинская ООШ»,
Н2	К категории Н2 относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн. Лицо этой категории, может: – иметь доступ к фрагментам информации, содержащей ПДн; – располагать именами и вести выявление паролей зарегистрированных пользователей;	Сотрудники МОУ «Каменноключинская ООШ», не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам ИСПДн, но имеющие санкционированный доступ в КЗ, в том числе сантехники, уборщицы, гардеробщицы,

	– изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.	сторожа и другие лица, обеспечивающие нормальное функционирование организации.
Н3	К категории Н3 относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места. Лицо этой категории: – обладает всеми возможностями лиц категории Н2; – знает, по меньшей мере, одно легальное имя доступа; – обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ПДн; – располагает конфиденциальными данными, к которым имеет доступ. Его доступ, аутентификация и права по доступу к некоторому подмножеству Пдн должны регламентироваться соответствующими правилами разграничения доступа	Сотрудники БОУ «Каменноключинская ООШ», являющиеся зарегистрированными пользователями ИСПДн, имеющие право доступа к ресурсам ИСПДн для выполнения своих должностных обязанностей
Н4	К категории Н4 относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн. Лицо этой категории: – обладает всеми возможностями лиц категории Н3; – обладает полной информацией об ИСПДн; – обладает полной информацией о системном и прикладном ПО ИСПДн; – обладает полной информацией о технических средствах и конфигурации ИСПДн; – имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; – обладает правами конфигурирования и административной настройки технических средств ИСПДн. – имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Системный администратор выполняет конфигурирование и управление ПО и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта, за соблюдение правил разграничения доступа, за смену паролей, за архивацию и защиту от НСД	Сотрудники МОУ «Каменноключинская ООШ» с полномочиями системного администратора ИСПДн, выполняющего конфигурирование и управление ПО и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, регистрации, архивации, защиты от несанкционированного доступа.
Н5	К категории Н5 относятся программисты-	Программисты-разработчики

	разработчики (поставщики) прикладного ПО. Лицо этой категории: – обладает информацией об алгоритмах и программах обработки информации в ИСПДн; – обладает возможностями внесения ошибок, декларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения.	прикладного ПО применяемого в ИСПДн, но не имеющие санкционированный доступ к ресурсам ИСПДн.
Н6	К категории Н6 относятся лица, обладающие возможностью: – создания способов, подготовки и проведения атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО; – проведения работ по созданию способов и средств атак в научно-исследовательских центрах; – располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СЗИ; – располагать всеми аппаратными компонентами СЗИ.	К типу нарушителей Н6 можно отнести группы специалистов по разработке и использованию специальных средств эксплуатации уязвимостей.

Обоснование перечня лиц, которые не рассматриваются в качестве потенциальных нарушителей, приведено в таблице 4.

Таблица 4 – Обоснование перечня лиц, которые не рассматриваются в качестве потенциальных нарушителей

Обоснование исключения лиц из числа потенциальных нарушителей	**Отметка об исключении лиц из групп потенциальных нарушителей**						
	Н0	Н1	Н2	Н3	Н4	Н5	Н6
Лица, отнесённые к категории нарушителей Н2, имеющие санкционированный доступ в КЗ, либо являются доверенными, либо их действия контролируется пользователем и (или) администратором ИСПДн.			+	+			
Лица, отнесённые к категории нарушителей Н3, в рамках выполнения своих функциональных обязанностей имеют возможность непосредственного доступа к ПДн, обрабатываемым в ИСПДн, и поэтому проведение атак с их стороны бессмысленно.				+			
Функции лиц, отнесённых к категории нарушителей Н4, выполняют лица, которые осуществляют техническое					+		

обслуживание как общесистемных средств ИСПДн, так и СЗИ, включая их настройку, конфигурирование и распределение паролей и ключевой документации между остальными пользователями. Лица, отнесённые к категориям нарушителей Н4, назначаются из числа особо проверенных ответственных и доверенных лиц. Эффективность всей системы безопасности ПДн зависит от адекватности действий данных лиц Поэтому устанавливать систему защиты от них было бы нецелесообразно в связи с её беспрецедентной сложностью и низкой эффективностью (исходя из соображений, что если кто-то из этих лиц преднамеренно задумает нарушить безопасность ПДн, то предупредить реализацию такой угрозы можно только в комплексе со специальными мероприятиями, сложность которых несоразмерна с более простыми возможностям и привилегированных лиц, обойти установленные для них ограничения)							
Лица, отнесённые к категориям нарушителей Н5, не имеют санкционированного доступа к ИСПДн, их действия контролируются администратором ИСПДн. Работы данной группой нарушителя осуществляются на основании договоров и соглашений, которые предусматривают ответственность за утечку конфиденциальной информации.						+	
Предполагается, что для категорий нарушителей Н6 проведение атак является средством менее предпочтительным, чем средства, основанные на агентурных методах, которые они предпринимают в целях получения ПДн о конкретно интересующем их лице, а не по всей базе ПДн, обрабатываемых в ИСПДн							+

Обоснование исключения лиц из числа потенциальных нарушителей	**Отметка об исключении лиц из групп потенциальных нарушителей**						
	Н0	Н1	Н2	Н3	Н4	Н5	Н6
Вывод			+	+	+	+	+

В соответствии с проведённым анализом потенциальных нарушителей в ИСПДн устанавливаются следующие категории нарушителей:

– внешние нарушители Н0 и Н1. Различают высокий, средний и низкий потенциалы нарушителя. Высокий потенциал подразумевает наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей.

Средний потенциал подразумевает наличие возможностей уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей.

Низкий потенциал подразумевает наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей.

Предполагается, что внешний нарушитель может обладать низким и средним потенциалом.

8. Определение класса средств криптографической защиты информации

Шифровальные (криптографические) средства: не используются

9. Определение актуальных угроз безопасности персональных данных в ИСПДн.

Актуальные УБПДн определяются в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных».

Для выявления УБПДн, актуальных для ИСПДн, оцениваются два показателя:

– уровень исходной защищенности ИСПДн;

– частота (вероятность) реализации рассматриваемой угрозы.

9.1. Уровень исходной защищённости ИСПДн.

Результаты анализа исходной защищенности ИСПДн приведены в таблице 5.

Таблица 5 – Анализ исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
локальная ИСПДн, развернутая в пределах одного здания	+		
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования			+
3. По встроенным (легальным) операциям с записями персональных данных: базе			
запись, удаление, сортировка		+	
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся пользователем ИСПДн либо субъект ПДн		+	
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
ИСПДн, в которой используется одна база Пдн, принадлежащая организации-владельцу данной ИСПДн			+
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые			+

пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, не предоставляющая никакой информации	+		
Характеристики ИСПДн	29%	29%	42%

Таким образом, ИСПДн имеет низкий (Y1=10) уровень исходной защищённости.

9.2. Частота (вероятность) реализации угроз безопасности персональных данных. При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

9.2.1. Угрозы утечки информации по техническим каналам

Угрозы утечки акустической (речевой) информации В ИСПДн функции голосового ввода ПДн или функции воспроизведения Пдн акустическими средствами отсутствуют.
Вероятность реализации угрозы – маловероятна.

2.Угрозы утечки видовой информации

В здании МОУ «Каменноключинская ООШ» введен контроль доступа в контролируемую зону, АРМ с ИСПДн расположено в здании, окна выходят во двор контролируемой зоны так, что практически исключен визуальный просмотр посторонними лицами информации на мониторе. Вывод на печать ПДн осуществляется. Отпечатанные данные не расрпостраняются за пределы школы. Вероятность реализации угрозы – маловероятна.

3.Угрозы утечки информации по каналам ПЭМИН Угрозы данного класса маловероятны, т.к. размер контролируемой зоны большой, и элементы ИСПДн, находятся на большом расстоянии от ее границы и экранируются несколькими несущими стенами, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

9.2.2. Угрозы несанкционированного доступа к информации. Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

9.2.2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПД.

1. Кража ПЭВМ. В здании МОУ «Каменноключинская ООШ» введен круглосуточный контроль доступа в контролируемую зону, который осуществляется сторожами. Вероятность реализации угрозы – маловероятной.

2. Кража носителей информации В здании МОУ «Каменноключинская ООШ» введен контроль доступа в контролируемую зону, двери закрываются на замок. Вероятность реализации угрозы – маловероятна.

3. Кража ключей и атрибутов доступа В здании школы введен контроль доступа в контролируемую зону, двери закрываются на замок, организовано хранение ключей. Вероятность реализации угрозы – маловероятна.

4.Кражи, модификации, уничтожения информации В здании школы введен контроль доступа в контролируемую зону, двери закрываются на замок. Вероятность реализации угрозы – маловероятна.

5. Вывод из строя узлов ПЭВМ, каналов связи В здании школы введен контроль доступа в контролируемую зону, двери закрываются на замок. Вероятность реализации угрозы – маловероятна.

6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ В Учреждении техническое обслуживание ПЭВМ осуществляется сотрудниками, подписавшими соглашение о неразглашении. Вероятность реализации угрозы – маловероятна.
7. Несанкционированное отключение средств защиты В здании школы введен контроль доступа в контролируемую зону, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн. Вероятность реализации угрозы – низкая вероятность.

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

1. Действия вредоносных программ (вирусов). В учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения. Вероятность реализации угрозы – низкая вероятность.
2. Не декларированные возможности системного ПО и ПО для обработки персональных данных. Разработку и сопровождение программного обеспечения ИСПДн осуществляет доверенная организация. Вероятность реализации угрозы – маловероятна.
3. Установка ПО, не связанного с исполнением служебных обязанностей Все пользователи проинструктированы о политике установки ПО и осуществляется контроль. Вероятность реализации угрозы – средняя вероятность.

9.2.2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

1. Утрата ключей и атрибутов доступа В Учреждении введена парольная политика, предусматривающая требуемую сложность пароля, осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей. Вероятность реализации угрозы – средняя вероятность.
2. Непреднамеренная модификация (уничтожение) информации сотрудниками В Учреждении резервное копирование обрабатываемых ПДн не осуществляется. Вероятность реализации угрозы – низкая.
3. Непреднамеренное отключение средств защиты В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн. Вероятность реализации угрозы – маловероятна.
.4. Выход из строя аппаратно-программных средств В Учреждении резервирование ключевых элементов ИСПДн не осуществляется. Вероятность реализации угрозы – низкая.
5. Сбой системы электроснабжения В Учреждении источники бесперебойного питания к ключевым элементам ИСПДн не подключены. Вероятность реализации угрозы – низкая.
6.Стихийное бедствие В Учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций. Вероятность реализации угрозы – маловероятна.

9.2.3. Угрозы преднамеренных действий внутренних нарушителей.

1. Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке В здании школы введен контроль доступа в контролируемую зону, двери закрываются на замок. Вероятность реализации угрозы – маловероятна.

2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке В Учреждении пользователи осведомлены о порядке работы с персональными данными, а также подписали Соглашение о неразглашении ПДн. Вероятность реализации угрозы – маловероятна.

9.2.4. Угрозы несанкционированного доступа по каналам связи.

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей по сети;
- угрозы навязывание ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений; - угрозы внедрения по сети вредоносных программ.

1. Угроза «Анализ сетевого трафика»

Передача информации осуществляется по защищенным каналам связи.

Перехват за переделами контролируемой зоны.

Вероятность реализации угрозы – маловероятна.

Перехват в пределах контролируемой зоны внешними нарушителями

Вероятность реализации угрозы – маловероятна.

Перехват в пределах контролируемой зоны внутренними нарушителями. Вероятность реализации угрозы – маловероятна.

2.Угроза «сканирование сети» Вероятность реализации угрозы – высокая вероятность.

3. Угроза выявления паролей

В Учреждении применяются стойкие пароли. Вероятность реализации угрозы – маловероятна.

4.Угрозы навязывание ложного маршрута сети

Вероятность реализации угрозы – высокая.

5. Угрозы подмены доверенного объекта Вероятность реализации угрозы – высокая.

6. Внедрение ложного объекта сети Вероятность реализации угрозы – высокая.

7. Угрозы типа «Отказ в обслуживании» Вероятность реализации угрозы – маловероятно.

8. Угрозы удаленного запуска приложений Вероятность реализации угрозы – маловероятно.

9. Угрозы внедрения по сети вредоносных программ На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений. Вероятность реализации угрозы – маловероятно.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы равен двум, т.е. объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2 низкая вероятность). Коэффициент реализуемости угрозы Y будет определяться исходя из исходного уровня защищенности ИСПДн и вероятности реализации УБПДн соотношением: Y = (Y1+Y2)/20 Y = (10+2)/20 = 0,6 По значению коэффициента реализуемости угрозы Y формируется вербальная

интерпретация реализуемости угрозы. Возможность реализации угрозы признается средней т.к. 0,3 Y 0,6 . < ≤ Показатель опасности угрозы низкий (реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных).

9.3. Определение актуальности угроз безопасности персональных данных. Угрозы безопасности ПДн относятся к неактуальным, исходя из возможности реализации угроз и показателя опасности угрозы, в соответствии с таблицей 6.

Таблица 6 – Правила отнесения УБПДн к актуальной

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая опасность	**Средняя опасность**	**Высокая опасность**
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

10. Заключение.

Модель угроз МОУ «Каменноключинская ООШ» содержит следующие возможные УБПДн для ИСПДн:

1. Непреднамеренная модификация (уничтожение) информации сотрудником;

2. Угроза сканирования, направленная на выявление типа или типов используемых оператором систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и пр.

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

1. Обеспечить защиту сетевого периметра АРМ с ИСПДн с помощью межсетевого экрана