Согласовано
на заседании Совета родителей
Протокол № от_ _ _ _ _ _ _ _

Согласовано
на заседании Совета обучающихся
Протокол №_____

Принято
на заседании педагогического Совета
Протокол №_____

Утверждено приказом директора
МКОУ «Архангельская ООШ»
от _____

Положение об обработке и защите персональных данных в информационных системах МКОУ «Архангельская ООШ»

с. Архангельское

1. Общие положения

Настоящее «Положение об обработке и защите персональных данных в информационных системах МКОУ «Архангельская 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 МКОУ «Архангельская ООШ» (далее – ИСПДн).

Положение определяет порядок работы коллектива МКОУ «Архангельская 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 МКОУ «Архангельская 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 МКОУ «Архангельская ООШ»** (Приложение 4), а также с **инструкцией пользователя, по проведению антивирусного контроля на объектах вычислительной техники МКОУ «Архангельская 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 аппаратно-программных 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 аппаратно-программную 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 программно-технических 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 МКОУ «АрхангельскаяООШ»

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

I. ОБЩИЕ ПОЛОЖЕНИЯ

Данная Инструкция определяет основные обязанности и права ответственного за организацию обработки персональных данных МКОУ "Архангельская ООШ" (далее – школа).

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

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

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

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

Доступ к информации – возможность получения информации и её использования.

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

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

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

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.

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

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.

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

Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

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.

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:

Знать перечень и условия обработки персональных данных в школе.

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

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

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

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

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

Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

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.

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

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.

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

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.

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

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

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

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

IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

К попыткам несанкционированного доступа относятся:

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;

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.

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

прекратить несанкционированный доступ к персональным данным;

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

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

известить администратора безопасности ИСПДн о факте несанкционированного доступа.

V. ПРАВА

Ответственный за организацию обработки персональных данных имеет право:

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

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

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

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.

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 МКОУ «АрхангельскаяООШ»

ИНСТРУКЦИЯ
АДМИНИСТРАТОРУ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ МКОУ «АРХАНГЕЛЬСКАЯ ООШ»

Настоящая Инструкция определяет функции, права и обязанности Администратора безопасности информации на автоматизированных системах обработки персональных данных МКОУ «Архангельская 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 МКОУ «Архангельская 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 МКОУ «Архангельская 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

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.
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 МКОУ «АрхангельскаяООШ»

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 МКОУ «АрхангельскаяООШ»

ИНСТРУКЦИЯ
пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники МКОУ "Архангельская 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 МКОУ «АрхангельскаяООШ»

ИНСТРУКЦИЯ
пользователя, по проведению антивирусного контроля на объектах вычислительной техники МКОУ «Архангельская ООШ»

1. Настоящая Инструкция предназначена для пользователей, хранящих и обрабатывающих информацию на объектах вычислительной техники МКОУ "Архангельская ООШ" (далее ОВТ МКОУ "Архангельская ООШ")

2. В целях обеспечения антивирусной защиты на ОВТ МКОУ "Архангельская 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 МКОУ "Архангельская ООШ" допускаются лицензионные антивирусные средства.

5. На ОВТ МКОУ "Архангельская ООШ" запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

6. Пользователь ОВТ МКОУ "Архангельская 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.

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 МКОУ "Архангельская 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 МКОУ "Архангельская ООШ" и в возможно короткие сроки устранить проблему.