УТВЕРЖДАЮ

Директор
МКОУ СОШ №2 г.Алагира
_____ Сидомонидзе Ф.Н.
«_1_» _____02_____ 20_17_г.

ИНСТРУКЦИЯ
пользователя объекта информатизации «Информационная система персональных данных «АРМ» МКОУ СОШ №2 г.Алагира»

Настоящая инструкция определяет права и обязанности пользователя на объекте информатизации «Информационная система персональных данных «АРМ» МКОУ СОШ №2 г.Алагира» (далее - ИСПДн).

1. Общие положения:

Пользователь ИСПДн МКОУ СОШ №2 г.Алагира назначается приказом по МКОУ СОШ №2 из числа штатных сотрудников, имеющих оформленное разрешение на доступ к защищаемой информации. В части эксплуатации ИСПДн он подчиняется непосредственному руководителю соответствующего подразделения, ответственному за защиту информации на объекте информатизации и Администратору информационной безопасности ИСПДн.

Назначение и освобождение от исполнения обязанностей согласовывается с ответственным за защиту информации, Администратором ИБ ИСПДн, директором МКОУ СОШ №2 г.Алагира.

К самостоятельной работе в ИСПДн допускаются пользователи, изучившие эксплуатационно-техническую документацию, требования аттестационной документации объекта информатизации, в части касающейся пользователей эксплуатирующих данную ИСПДн, инструкции описывающие порядок эксплуатации ИСПДн и освоившие основные правила работы с СЗИ.

Допуск производится после проверки знания требований руководящих документов и практических навыков в работе с разрешения ответственного за защиту информации и Администратора ИБ ИСПДн, по письменному распоряжению директора МКОУ СОШ №2 г.Алагира.

В практической деятельности пользователь ИСПДн руководствуется:

- Федеральным законом «Об информации, информационных технологиях и о защите информации» от 08.06.2006 г. № 149-ФЗ;
- Федеральным законом «О безопасности» от 5.03.1992 г. № 2446-I;
- Федеральным законом «О персональных данных» от 27 июля 2006 г. №152-ФЗ;
- Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», введенное в действие постановлением Правительства Российской Федерации от 15.09.1993 г. № 912-51;
- Положением по аттестации объектов информатизации по требованиям безопасности информации», Гостехкомиссия России, 1994 г;
- Положением о сертификации продукции по требованиям безопасности информации», Гостехкомиссия России, 1994 г;
- Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», Гостехкомиссия России, 2002 г;
- ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила

управления информационной безопасностью;
- Международным стандартом ИСО/МЭК 27001-2005 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования;
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения;
- ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения;
- ГОСТ Р ИСО/МЭК 13335 Информационная технология. Методы и средства обеспечения безопасности;
- ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации;
- Основными мероприятиями по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных, утверждены заместителем директором ФСТЭК России 15 февраля 2008 г;
- Базовой моделью угроз безопасности персональных данных при их обработке в информационной системе персональных данных, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г;
- Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационной системе персональных данных, утверждена заместителем директора ФСТЭК России 14 февраля 2008 г;
- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных, утверждены заместителем директора ФСТЭК России 15 февраля 2008 г;
- РД Гостехкомиссии РФ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Гостехкомиссия России, 1992 г;
- РД Гостехкомиссии РФ. Защита от несанкционированного доступа к информации. Термины и определения. 1992 г;
- РД Гостехкомиссии РФ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. 1997 г;
- РД Гостехкомиссии РФ. Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации Классификация по уровню контроля отсутствия недекларированных возможностей, Гостехкомиссия России, Москва, 1999 г;
- РД Гостехкомиссии РФ. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» 1992 г;
- РД Гостехкомиссии РФ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» 1992 г;
- Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Введена в действие приказом от 13 июня 2001 года №152 (ФАПСИ) ;
- Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), введено приказом ФСБ РФ от 9 февраля 2005 г. № 66;
- Требованиями к средствам криптографической защиты конфиденциальной информации, ФСБ РФ, Москва;
- Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационной системе персональных данных с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г., №149/54-144;

- Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных, ФСБ России, №149/6/6-622;
- другими нормативными документами ФСБ России, ФСТЭК (Гостехкомиссии) России по защите информации;
- приказами и распоряжениями директора МКОУ СОШ №2 г.Алагира;
- эксплуатационно-технической документацией на объекты информатизации МКОУ СОШ №2 г.Алагира.

Инструкция корректируется и дополняется установленным порядком.

2. Функции пользователя:

Основными функциями пользователя ИСПДн являются:

Выполнение мероприятий, направленных на предотвращение непреднамеренного доступа и НСД к защищаемой информации;

Обеспечение режима конфиденциальности при автоматизированной обработке защищаемой информации в ИСПДн;

Автоматизированная обработка защищаемой информации в соответствии с заданием вышестоящего руководителя;

Комиссионное удаление защищаемой информации с машинных носителей информации, совместно с ответственным за защиту информации на объекте информатизации и Администратором ИБ ИСПДн;

Проверка новых данных на отсутствие вирусов.

3. Обязанности пользователя ИСПДн:

Пользователь ИСПДн обязан:

Четко знать и выполнять требования действующих нормативных и руководящих документов, внутренних инструкций, инструкций по эксплуатации СЗИ, распоряжений, регламентирующих порядок действий по ЗИ;

В случае неисправности СЗИ НСД, выявления попыток НСД к защищаемой информации, либо обнаружения следов вскрытия ОТСС, немедленно прекратить работу в ИСПДн, ограничить доступ в помещение где располагается АС, поставить в известность Администратора ИБ ИСПДн и ответственного за ЗИ и действовать в соответствии с «Инструкцией по действиям персонала в нештатных ситуациях…»;

Проверять все новые данные на отсутствие вирусов;

Обрабатывать защищаемую информацию в соответствии с заданием и утвержденной технологией;

Регулярно производить смену личного пароля доступа (не реже 1 раза в 6 месяцев) с записью факта смены пароля в журнале учета профилактических работ, фактов вскрытия и опечатывания ПЭВМ, выполнения, установки и модификации аппаратных и программных средств защищенных ПЭВМ информационной системы. ***Запрещается сообщать кому-либо свой пароль доступа!*** Минимальная длина пароля – **шесть** буквенно-цифровых символов;

При обработке на ПЭВМ защищаемой информации и необходимости использовать носители информации, применять только учтенные носители;

В случае возникновения каких либо нештатных ситуаций действовать в соответствии с «Инструкцией по действиям персонала в нештатных ситуациях…».

4. Порядок действий пользователя при работе:

4.1. Общие положения и требования:

4.1.1. Обработка защищаемой информации разрешается на основании приказа директора МКОУ СОШ №2 г.Алагира о вводе объекта информатизации «АРМ» МКОУ СОШ №2 г.Алагира в промышленную эксплуатацию;

4.1.2. Допуск лиц, работающих с защищаемой информацией, производится установленным порядком. Ответственность за обеспечение защиты информации в процессе эксплуатации объекта информатизации, возлагается на исполнителей, производивших ее обработку;

4.1.3. Обработка (в том числе создание и хранение) защищаемой информации в ИСПДн разрешается только на учтенных машинных носителях информации - ГМД, ЖМД, флеш-дисках, оптических накопителях и т.п. При этом уровень конфиденциальности накопителя должен быть не ниже уровня конфиденциальности записываемой на него информации;

4.1.4. На период обработки защищаемой информации в помещении, в котором размещаются СВТ ИСПДн, могут находиться только лица, наделенные правом самостоятельного доступа в помещение на основании приказа директора МКОУ СОШ №2 г.Алагира;

4.1.5. Двери в помещения при обработке защищаемой информации должны быть закрыты;

4.1.6. В начале работы и по ее окончании проверить сохранность опломбирования системного блока ИСПДн;

4.1.7. Ввод информации с отчуждаемых машинных носителей информации (далее - МНИ) в ИСПДн осуществляется в соответствии с «Технологией обработки информации в автоматизированной системе…», разделом 4.4. настоящей инструкции и «Инструкции по организации антивирусной защиты…»;

4.1.8. По окончании обработки защищаемой информации или при передаче управления другому допущенному пользователю необходимо уничтожить остаточную и не нужную информацию на жестком магнитном диске ПЭВМ или других МНИ;

4.1.9. По окончании обработки защищаемой информации произвести перезагрузку ПЭВМ;

4.1.10. Работа с СЗИ НСД осуществляется в соответствии с «Руководством пользователя» комплекта документации на СЗИ от НСД;

4.1.11. Файлы с защищаемой информацией должны храниться только в установленных для этого каталогах (разделах) – защищаемых ресурсах, соответствующего уровня конфиденциальности. Запрещается перенос (копирование) файлов в каталоги (разделы) с низшим уровнем конфиденциальности;

4.1.12. Уничтожение файлов, машинных носителей содержащих защищаемую информацию, осуществляется по акту о стирании информации соответствующего уровня конфиденциальности, уничтожении машинных носителей информации, машинных документов;

4.1.13. При компрометации учетных данных (логин и пароль) пользователя работа в ИСПДн должна быть **НЕМЕДЛЕННО** прекращена, а ответственный за ЗИ на объекте информатизации и Администратор ИБ ИСПДн должны быть поставлены в известность об этом;

4.1.14. Распечатка любой защищаемой информации на печатающем устройстве производится в соответствии с утвержденной организационно-распорядительной документацией, на учтенных носителях.

4.2. Общий порядок работы:

4.2.1. Получить персональный идентификатор и пароль под роспись, при первоначальном доступе к ИСПДн;

4.2.2. Выполнить предусмотренные организационно-технические мероприятия по ЗИ;

4.2.3. Убедиться в целостности и сохранности печатей на корпусе системного блока ИСПДн (системный блок должен быть опечатан ответственным за ЗИ или Администратором ИБ ИСПДн);

4.2.4. Включить ПЭВМ (ОТСС), убедиться в исправности и нормальном функционировании. При появлении приглашения к идентификации пользователя предъявить идентификатор, после приглашения на ввод пароля ввести с клавиатуры свой индивидуальный пароль и нажать клавишу <Enter>;

4.2.5. Выполнить работу согласно заданию;

4.2.6. Сделать при необходимости записи в журналах учета нештатных ситуаций и учета выполнения профилактических работ, фактов вскрытия и опечатывания ПЭВМ ИСПДн;

4.2.7. Выключить ПЭВМ (ОТСС).

Удаление защищаемой информации:

Отбор и удаление документированной защищаемой информации на учтенных съемных МНИ, а так же уничтожение МНИ производиться комиссионно в составе: ответственный за ЗИ ИСПДн, Администратор ИБ объекта информатизации и пользователь, отвечающий за обновление (обработку) данной информации;

Определить информацию, подлежащую стиранию, о чем сделать запись в акте об уничтожении информации соответствующего уровня конфиденциальности;

Удалить эту информацию;

Правильность записей в акте проверяет уполномоченное лицо, о чем также расписывается.

Выполнить действия согласно п.п. 4.2.6 – 4.2.7.

Запись новой информации на жесткий диск ИСПДн:

Выполнить действия согласно п.п. 4.2.1 – 4.2.4;

Запустить программу антивирусной защиты;

Проверить все данные на носителе новой информации на отсутствие вирусов. Дальнейшая работа с носителем допускается только при отсутствии на нем вирусов. При обнаружении вируса действовать согласно «Инструкции по организации антивирусной защиты…»;

В соответствии с заданием на обработку выполнить обработку данных, соблюдая требования п. 4.1.13

В случае возникновения каких-либо нештатных ситуаций действовать в соответствии с «Инструкцией по действиям персонала в нештатных ситуациях…»;

Выполнить действия согласно п.п. 4.2.6 – 4.2.7.

5. Запрещается:

Передавать (сообщать) кому-либо свой логин и пароль;

Оставлять работающую ПЭВМ (ОТСС), без включения режима блокировки консоли;

Использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целя;

Передавать работающую ПЭВМ (ОТСС) другому пользователю без перезагрузки;

Оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа;

Оставлять без личного присмотра в легкодоступном месте на рабочем месте или где бы то ни было свои машинные носители и распечатки, содержащие сведения ограниченного распространения.

Использовать в работе неучтенные носители информации для обработки защищаемой информации

Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты. Об обнаружении такого рода ошибок – ставить в известность Администратора ИБ ИСПДн и руководителя своего подразделения.

Ответственный за защиту информации _____ / _____ /

Лист ознакомления
с «Инструкцией пользователя объекта информатизации ИСПДн МКОУ СОШ №2 г.Алагира, утвержденной и введенной в действие «01» 02 2017 г.

№ п/п	Фамилия, инициалы сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении