УТВЕРЖДАЮ

директор МБОУСОШ №1 с.Аскино
_____ Шаймарданов Ф.З.
приказ № 95 от«10» 03 2025г.

ИНСТРУКЦИЯ
по эксплуатации средств защиты информации МБОУ СОШ №1 с.Аскино

1. Информационные системы (далее—ИС) МБОУСОШ №1 с.Аскино (далее—ОУ) представляют собой локальную вычислительную сеть, в которой обрабатывается информация ограниченного доступа, содержащая персональные данные сотрудников ОУ, обучающихся и их родителей. Обработка информации осуществляется в многопользовательском режиме с разграничением прав доступа. Осуществляется подключение рабочих станций пользователей к сетям связи общего доступа. На технические средства установлены сертифицированные по требованиям ФСТЭК России средства защиты информации (СЗИ).
2. В ИС установлены настроены средства защиты информации согласно Приложению №1.
3. Обязанности по сопровождению и настройке средств защиты возлагаются на администратора безопасности информации (АБИ), являющимся ответственным за эксплуатацию СЗИ.
4. Ответственный за эксплуатацию СЗИ должен:
   1. Осуществлять оперативные действия по конфигурированию установленных средств и механизмов защиты и их поддержке в работоспособном состоянии в соответствии с утвержденным положением и инструкциями, включая:
      1) определение состава и настроек антивирусного программного обеспечения;
      2) определение параметров и субъектов для процедур резервного копирования;
      3) определение категорий пользователей и назначение им прав;
      4) настройку политики контроля событий безопасности на серверах и рабочих станциях, входящих в состав ИС;
      5) конфигурирование средств межсетевого экрана (МЭ) и коммуникационного оборудования.
      6) оценку эффективности реализованных механизмов защиты.
   2. Подготавливать предложения для включения в планы и программы работ мероприятий по принятию организационных и инженерно-технических мер защиты ИС.
   3. Выполнять комплекс работ, связанных с контролем и защитой информации, на основе разработанных программ и методик.
   4. Организовывать работы по сбору, анализу и систематизации сведений об объектах ИС и о подлежащей защите информации ограниченного доступа, циркулирующей в ИС.
   5. Контролировать защищенность всех пользовательских рабочих мест ИС.

6. Вести журналы регистрации событий информационной безопасности и мер, которые были приняты для устранения неполадок НСД.

5. Особенности настройки и конфигурирования средств защиты информации приведены в эксплуатационной и технической документации на соответствующие средства защиты согласно Приложению №2.

6. Обязанности пользователя ИС:

1. Знать и соблюдать установленные требования по режиму обработки информации ограниченного доступа, учету, хранению и пересылке машинных носителей информации, а также руководящих и организационно-распорядительных документов на ИС.
2. Пользователи перед началом обработки в ИС файлов, хранящихся иа съемных носителях информации, должны осуществить проверку файлов на наличие компьютерных вирусов.
3. Соблюдать установленный режим разграничения доступа к информационным ресурсам, получать у АБИ пароли, надежно его запоминать и хранить в тайне.
4. Немедленно докладывать обо всех фактах и попытках НСД к обрабатываемой на объектах вычислительной техники (ОВТ) информации или об ее исчезновении (искажении).

7. Пользователям ОВТ запрещается:

1. записывать и хранить информацию на неучтенных носителях информации;
2. оставлять во время работы магнитные носители информации без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработки информации;
3. отключать (блокировать) средства защиты информации, предусмотренные организационно - распорядительными документами на ИС;
4. обрабатывать информацию с выключенным или не функционирующими устройствами защиты информации;
5. самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
6. сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ОВТ;
7. работать в ИС при обнаружении каких-либо неисправностей;
8. вводить в информационную систему под диктовку или с микрофона;
9. привлекать посторонних лиц для производства ремонта технических средств без согласования со специалистом по защите информации.

8. Все изменения конфигурации технических и программных средств СЗИ, а также внесение необходимых изменений в настройки СЗИ от НСД и средств контроля целостности файлов, должны производиться под контролем администратора безопасности информации.

9. Проведение работ по изменения конфигурации технических и программных средств осуществляется в соответствии с инструкцией по модификации технических и программных средств.

10. Проведение работ по изменению состава технических и программных средств СЗИ без согласования с органом по аттестации прекращает действие выданного Аттестата соответствия.

Приложение№1
к инструкции по эксплуатации
средств защиты информации

ПЕРЕЧЕНЬ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Начат«_____»_____20__г.

Окончен«____»_____20__г.

На _____листах

_____
(Фамилия И.О.)

_____ _____
(должность руководителя) (подпись)

№ п/п	Наименование СЗИ	Сертификат РФ	Срок действия сертификата	Характеристики	Заводской (учетный) номер СЗИ	КОЛ-ВО, Шт.