УТВЕРЖДЕНО
Приказом МДОУ ДС «Морошка»
№ 23 - ОД от 18.11.2022 г

ИНСТРУКЦИЯ
по эксплуатации средств защиты информации в муниципальном дошкольном образовательном учреждение детский сад «Морошка»

Приложение **№ 5**
к приказу № 23 - ОД от 18.11.2022 г.

ИНСТРУКЦИЯ
по эксплуатации средств защиты информации в муниципальном дошкольном образовательном учреждение детский сад «Морошка»

1. Информационная система персональных данных (далее - информационная система; ИС) Муниципальном дошкольном образовательном учреждение детский сад «Морошка» (далее - МДОУ) представляет собой распределённую вычислительную сеть, в которой обрабатывается информация ограниченного доступа, содержащая персональные данные работников в том числе сотрудников МДОУ. 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 (далее - СЗИ).

2. В ИС установлены и настроены следующие средства защиты информации:

- Средство антивирусной защиты ESET NOD Antivirus4;
- ПО ViPNet Client.

3. Обязанности по сопровождению и настройке средств защиты возлагаются на администратора безопасности информации (далее - АБИ), являющегося ответственным за эксплуатацию СЗИ.

4. Ответственный за эксплуатацию СЗИ должен:

4.1. осуществлять оперативные действия по конфигурированию установленных средств и механизмов защиты и их поддержке, в работоспособном состоянии в соответствии с утвержденным положением и инструкциями, включая:

- определение состава и настроек антивирусного программного обеспечения;
- определение параметров и субъектов для процедур резервного копирования;
- определение категорий пользователей и назначение им прав;
- настройку политики контроля событий безопасности на серверах и рабочих станциях, входящих в состав ИС;
- конфигурирование средств межсетевого экрана (далее- МЭ) и коммуникационного оборудования;
- оценку эффективности реализованных механизмов защиты;

4.2. подготавливать предложения для включения в планы и программы работ мероприятий по принятию организационных и инженерно-технических мер защиты ИС;

4.3. выполнять комплекс работ, связанных с контролем и защитой информации, на основе разработанных программ и методик;

4.4. организовывать работы по сбору, анализу и систематизации сведений об объектах ИС и подлежащей защите информации ограниченного доступа, циркулирующей в ИС;

4.5. контролировать защищенность всех пользовательских рабочих мест ИС;

4.6. вести журнал учета средств защиты информации, эксплуатационной и технической документации к ним, используемых в информационной системе персональных данных МДОУ по форме согласно приложению, к настоящей Инструкции.

5. Особенности настройки и конфигурирования средств защиты информации приведены в эксплуатационной и технической документации на соответствующие средства защиты.

6. Обязанности пользователя ИС:

6.1. 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;

6.2. пользователи перед началом обработки в ИС файлов, хранящихся на съемных носителях информации, должны осуществить проверку файлов на наличие компьютерных вирусов;

6.3. соблюдать установленный режим разграничения доступа к информационным ресурсам: получать у АБИ пароль, надежно его запоминать и хранить в тайне;

6.4. немедленно докладывать АБИ обо всех фактах и попытках несанкционированного доступа (далее- НСД) к обрабатываемой на объектах вычислительной техники (далее- ОВТ) информации или об ее исчезновении (искажении).

7. Пользователям ОВТ запрещается:

7.1. записывать и хранить информацию на неучтенных носителях информации;

7.2. оставлять во время работы магнитные носители информации без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;

7.3.отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на ИС;

7.4. обрабатывать информацию с выключенным или нефункционирующими устройствами защиты информации;

7.5. самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

7.6. сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ОВТ;

7.7. работать в ИС при обнаружении каких-либо неисправностей;

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 изменению 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
к Инструкции по эксплуатации средств защиты информации в МДОУ ДС «Морошка»

ЖУРНАЛ УЧЕТА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, ИСПОЛЬЗУЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МДОУ ДС «МОРОШКА»

Начат «_____»_____20_____г.
Окончен «____»_____20_____г.
На_____листах

(должность) (подпись) (Ф.И.О.)

_____ _____ _____

Индекс и наименование средства защиты информации (наименование эксплуатационной/технической поддержки)	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей средство защиты	Примечание (данные о сертификате, ФИО и подпись)