

Муниципальное автономное дошкольное образовательное учреждение детский сад № 15 «Сказка» комбинированного вида г. Благовещенска Республики Башкортостан

ПРИНЯТО

На общем собрании работников МАДОУ
детский сад № 15 «Сказка»
Протокол № 3 от 04.03.2021

СОГЛАСОВАНО

Председатель профкома МАДОУ
Детский сад № 15 «Сказка»
О.А.Веровкина



УТВЕРЖДАЮ

Заведующий МАДОУ детский сад № 15
«Сказка»

Л.В. Галимуллина
Приказ № 17 от 04.03.2021

ИНСТРУКЦИЯ

**по эксплуатации средств защиты информации в
муниципальном автономном дошкольном образовательном
учреждении детский сад № 15 «Сказка» комбинированного вида г.
Благовещенска Республики
Башкортостан**

1 В муниципальном автономном дошкольном образовательном учреждении детский сад № 15 «Сказка» комбинированного вида г. Благовещенска Республики Башкортостан по требованиям ФСТЭК России на технические средства установлены сертифицированные средства защиты информации (далее - СЗИ).

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

Версия антивирусной программы :1.425.81.0

Версия антишпионского ПО: 1.425.81.0

3 Обязанности по сопровождению и настройке средств защиты возлагаются на ответственного по 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 МАДОУ 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.

ЖУРНАЛ УЧЕТА
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ,
ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ

Индекс и наименование средства защиты информации (наименование эксплуатационной/технической поддержки)	инструкция по эксплуатации средств защиты.pdf	Индекс и наименование средства	Серийный (заводской) номер	Номер специального