

Инструкция
по эксплуатации средств защиты информации в
МОБУ гимназия №1 г. Благовещенска

1. В муниципальном общеобразовательном бюджетном учреждении гимназия №1 города Благовещенска (далее - учреждение) по требованиям ФСТЭК России на технические средства установлены сертифицированные средства защиты информации (далее - СЗИ).

2. В информационной системе установлены и настроены следующие средства защиты информации:

- встроенная система безопасности Windows.

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 конфигурации 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. Организовать 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 к ним, используемых в информационной системе персональных данных гимназии 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 так же 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 не функционирующим устройством 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

Начат: _____

Окончен: _____

(должность)

(подпись)

(ФИО)

Индекс и наименование средств 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)