

Башкортостан Республикаһынын
Мәғариф һәм фән министрлығы
Бөрө калаһы
күп йүнәлешле
һөнәрселек колледжы
дәүләтбюджет
һөнәри
белем биреү учреждениеһы
(Бөрө калаһы күп йүнәлешле
һөнәрселек колледжы ДБһББУ)

Министерство образования и науки
Республики Башкортостан
государственное бюджетное
профессиональное
образовательное учреждение
Бирский
многопрофильный
профессиональный колледж
(ГБПОУ Бирский многопрофильный
профессиональный колледж)

БОЙОРОК

«30» май 2025й.

ПРИКАЗ

№ 209/9 - К

«30» мая 2025г.

Об утверждении инструкции по эксплуатации средств защиты информации в ГБПОУ Бирский многопрофильный профессиональный колледж

Во исполнение требований главы 14 Трудового кодекса «Защита персональных данных работника» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», п р и к а з ы в а ю:

1. Утвердить и ввести в действие с 30 мая 2025 года инструкцию по эксплуатации средств защиты информации в ГБПОУ Бирский многопрофильный профессиональный колледж (приложение №1).
2. Поручить программисту Ахмадееву В.А. в срок до 10 июня 2025 года оформить журнал учета средств защиты информации в ГБПОУ Бирский многопрофильный профессиональный колледж.
3. Контроль за исполнением настоящего приказа оставляю за собой

Директор

Е.Н. Литвинова

С приказом ознакомлен:



В.А.Ахмадеев

ИНСТРУКЦИЯ по эксплуатации средств защиты информации

1. Понятие и описание информационной системы (далее – ИС).
2. В ИС установлены и настроены следующие средства защиты информации:
 - (наименование СрЗИ);
 - (наименование СрЗИ);
 - ...
3. Обязанности по сопровождению и настройке средств защиты возлагаются на администратора безопасности информации (далее – АБИ, программист), 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 (Наименование информационной системы) 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: не передавать посторонним лицам и иным сотрудникам свои учётные данные, предоставляющие доступ к конфиденциальной информации в ИС и другой защищаемой информации.

6.4. Немедленно докладывать АБИ (программисту) 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 средствами 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.

Инструкция по ведению журнала

Записи в журнале делаются по мере установки и настройки средств защиты информации.

В графе **«Название средства защиты информации»** указывается наименование средства защиты информации.

В графе **«Тип средства защиты информации»** указывается тип средства защиты информации – программные или программно-аппаратный.

В графе **«Зав. номер (номер знака соответствия)»** указывается заводской номер и номер знака соответствия согласно формуляру на средство защиты (знак соответствия – голограмма ФСТЭК, которая вклеена либо в формуляр, либо наклеена на коробку диска дистрибутива средства защиты). Для средств защиты, сертифицированных ФСБ (например, ViPNet Client) вместо знака соответствия указывается регистрационный номер ФСБ.

В графе **«Сертификат»** указывается номер сертификата ФСТЭК России и/или ФСБ России и дата до которого он действует.

В графе **«Место и дата установки»** указывается номер АРМ согласно техпаспорту на систему (если он разработан), либо доменное имя АРМ (или виртуальной машины/сервера), а также дата установки (в ОС Windows можно узнать в меню «Панель задач» - «Программы и компоненты»).

В графе **«Примечание»** можно делать любые пометки, например об удалении данного экземпляра средства защиты.

ЖУРНАЛ
учета средств защиты информации в
(Наименование ИС)

№ п/п	Наименование средства защиты информации	Тип средства защиты информации	Зав. номер (номер знака соответствия)	Сертификат	Место и дата установки	Примечание
1.						
2.						
...						