Муниципальное общеобразовательное бюджетное учреждение
средняя общеобразовательная школа с. Мирный
муниципального района Благоварский район Республики Башкортостан

(Наименование организации)

СОГЛАСОВАНА
с выборным органом первичной
профсоюзной организации
Протокол от 29.09.2026 №3

УТВЕРЖДЕНА
приказом директора
МОБУ СОШ с. Мирный
от 30.09.2026 №202-ОД

ИНСТРУКЦИЯ
по эксплуатации средств защиты информации

1. Общие положения

1.1. Настоящая Инструкция регламентирует порядок эксплуатации средств защиты информации (далее – СЗИ) в муниципальном общеобразовательном учреждении бюджетном средняя общеобразовательная школа с. Мирный муниципального района Благоварский район Республики Башкортостан (далее – Учреждение).

1.2. Инструкция разработана в соответствии с:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- эксплуатационной и технической документацией на применяемые СЗИ.

1.3. Требования Инструкции обязательны для всех сотрудников Учреждения, имеющих доступ к информационным системам (далее — ИС) и автоматизированным рабочим местам (далее — АРМ).

1.4. Ответственность за организацию защиты информации в Учреждении несёт руководитель Учреждения. Непосредственное сопровождение и настройку СЗИ осуществляет ответственный за обеспечение безопасности информации (далее — АБИ), назначаемый приказом директора.

1.5. Доступ Учреждения к сети Интернет осуществляется через Единую сеть передачи данных (далее – ЕСПД), организованную ПАО «Ростелеком» на основании распоряжения Правительства РФ от 02.04.2020 № 794-р. Часть мер по защите информации обеспечивается оператором связи на уровне сети ЕСПД; локальные меры защиты реализуются силами Учреждения.

2. Состав средств защиты информации

2.1. Защита информации в Учреждении реализована в двух контурах: внешнем (через ЕСПД) и локальном (на АРМ и в локальной сети Учреждения).

2.2. Внешний контур защиты (обеспечивается ПАО «Ростелеком» в рамках ЕСПД):

№ п/п	Мера защиты	Назначение
1	Контентная фильтрация трафика	Блокировка доступа к сайтам из реестра Роскомнадзора, экстремистским материалам, нежелательному контенту; поддержка «белых» и «чёрных» списков, безопасного режима поиска
2	Шлюзовой антивирус	Проверка входящего интернет-трафика, блокировка заражённых файлов и вредоносных сайтов до попадания в локальную сеть Учреждения
3	Криптографическая защита канала связи	Сквозное шифрование данных при передаче по сети ЕСПД
4	Защита от DDoS-атак	Блокировка сетевых атак на уровне инфраструктуры оператора
5	Мониторинг состояния канала	Круглосуточный контроль качества связи, техническая поддержка по тел. 8-800-301-34-14

2.3. Локальный контур защиты (обеспечивается Учреждением):

№ п/п	Наименование СЗИ	Назначение	Где установлено
1	Kaspersky Endpoint Security	Антивирусная защита рабочих станций	Все АРМ
2	Брандмауэр Windows (Windows Defender Firewall)	Межсетевой экран, фильтрация локального трафика	Все АРМ
3	КриптоПро CSP + Рутокен ЭЦП 2.0 (или JaCarta-2 SE)	Криптографическая защита, работа с электронной подписью	1–АРМ (директор)
4	Средства контроля целостности ОС (встроенные средства Windows)	Контроль целостности системных файлов и настроек	Все АРМ
5	Средства резервного копирования Windows / ручное копирование	Резервное копирование данных	АРМ с базами данных
6	Средства разграничения доступа ОС	Парольная политика, разделение учётных записей, блокировка экрана	Все АРМ
7	Физические средства защиты	Замки, сейф, опечатывание системных блоков со СКЗИ	Помещения, системные блоки

2.4. Управление контентной фильтрацией ЕСПД осуществляется АБИ через личный кабинет на портале espd.rt.ru: формирование и корректировка «белых» и «чёрных» списков, проверка статуса фильтрации, просмотр отчётов.

2.5. Перечень и конфигурация локальных СЗИ могут изменяться приказом директора Учреждения на основании предложений АБИ.

3. Обязанности ответственного за обеспечение безопасности информации (АБИ)

3.1. АБИ обязан:

3.1.1. Осуществлять оперативные действия по конфигурированию установленных локальных средств защиты и поддержанию их в работоспособном состоянии, включая:

- определение состава и настроек антивирусного программного обеспечения (далее – АВПО);
- определение параметров и субъектов для процедур резервного копирования;
- определение категорий пользователей и назначение им прав доступа;
- настройку политики контроля событий безопасности на рабочих станциях;
- конфигурирование брандмауэра Windows на АРМ;
- оценку эффективности реализованных механизмов защиты.

3.1.2. Устанавливать и обновлять версии АВПО, проводить проверку на наличие вирусов, производить лечение или удаление заражённых файлов.

3.1.3. Хранить дистрибутивы программного обеспечения, включая СЗИ, в месте, исключающем несанкционированный доступ третьих лиц.

3.1.4. Вести журнал учёта средств защиты информации, эксплуатационной и технической документации к ним по форме согласно приложению к настоящей Инструкции.

3.1.5. Осуществлять поэкземплярный учёт средств криптографической защиты информации (далее – СКЗИ), эксплуатационной и технической документации к ним, а также учёт пользователей СКЗИ.

3.1.6. Контролировать защищённость всех пользовательских рабочих мест ИС.

3.1.7. Управлять контентной фильтрацией через личный кабинет на портале espd.rt.ru: актуализировать «белые» и «чёрные» списки сайтов, контролировать статус работы фильтрации, формировать запросы в техподдержку ПАО «Ростелеком» при инцидентах.

3.1.8. Контролировать работоспособность канала связи ЕСПД, при длительных сбоях обращаться в техподдержку ПАО «Ростелеком» по тел. 8-800-301-34-14.

3.1.9. Подготавливать предложения для включения в планы работ мероприятий по принятию организационных и инженерно-технических мер защиты ИС.

3.1.10. Проводить расследование и составление заключений по фактам нарушения условий эксплуатации СЗИ, которые могут привести к снижению уровня защищённости информации.

3.1.11. Не разглашать конфиденциальную информацию, к которой допущен, в том числе сведения о криптографических ключах.

4. Порядок ввода в эксплуатацию СЗИ

4.1. Ввод в эксплуатацию локальных СЗИ проводится в соответствии с формуляром и эксплуатационной документацией на соответствующие средства.

4.2. Перед установкой СЗИ необходимо проверить программное обеспечение ИС на отсутствие вирусов и программных закладок.

4.3. Установка СЗИ производится только лицами, имеющими соответствующие полномочия и подготовку (АБИ или уполномоченный специалист).

4.4. Системные блоки АРМ с установленными СКЗИ опечатываются специально выделенной печатью. Допускается применение иных средств контроля вскрытия.

4.5. Все экземпляры СЗИ, криптографических ключей выдаются пользователям под роспись в журнале учёта СЗИ.

5. Обязанности пользователей ИС

5.1. Пользователь ИС обязан:

5.1.1. Знать и соблюдать установленные требования по режиму обработки информации ограниченного доступа, учёту, хранению и пересылке машинных носителей информации.

5.1.2. Ежедневно, в начале работы, обеспечивать запуск АВПО на своём АРМ; не допускать блокирования или выключения антивирусного средства в процессе работы.

5.1.3. В обязательном порядке проводить антивирусную проверку съёмных носителей информации перед началом работы с ними — даже если носитель получен от сотрудников Учреждения. Шлюзовой антивирус ЕСПД проверяет только входящий интернет-трафик и не контролирует съёмные носители.

5.1.4. Получать у АБИ пароль для доступа, надёжно его запоминать и хранить в тайне. Запрещается записывать пароли в открытом виде на материальных носителях.

5.1.5. Соблюдать установленный режим разграничения доступа к информационным ресурсам.

5.1.6. Использовать режим экранной заставки с парольной защитой. Рекомендуется устанавливать максимальное время бездействия до появления заставки не более 15 минут.

5.1.7. Немедленно докладывать АБИ обо всех фактах и попытках несанкционированного доступа (далее – НСД) к информации или об её исчезновении (искажении).

5.1.8. При обнаружении нарушений целостности пломб (наклеек, печатей) на аппаратных средствах АРМ, несанкционированных изменений в конфигурации СЗИ, отклонений в работе программных или аппаратных средств — немедленно прекратить работу и сообщить АБИ.

5.1.9. Использовать только учтённые съёмные машинные носители информации для выполнения должностных обязанностей.

5.1.10. По окончании работы блокировать АРМ или производить выход из операционной системы.

6. Пользователям ИС запрещается

6.1. Записывать и хранить информацию на неучтённых носителях информации.

6.2. Оставлять во время работы носители информации без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации.

6.3. Отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами.

6.4. Обрабатывать информацию с выключенным или нефункционирующим устройствами защиты информации.

6.5. Самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

6.6. Сообщать или передавать посторонним лицам личные атрибуты доступа к ресурсам ИС (пароли, ключевые носители, электронные подписи).

6.7. Работать в ИС при обнаружении каких-либо неисправностей средств защиты информации.

6.8. Осуществлять несанкционированное копирование СКЗИ.

6.9. Использовать ключевые носители и электронную подпись для работы на других рабочих местах.

6.10. Привлекать третьих лиц к работам по установке и настройке СЗИ, замене комплектующих системного блока, системному и сетевому администрированию.

6.11. Использовать компоненты СЗИ в неслужебных целях.

6.12. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении, которые могут привести к нарушению безопасности персональных данных.

6.13. Подключать к локальной сети Учреждения личные устройства (телефоны, планшеты, ноутбуки) без согласования с АБИ.

6.14. Использовать средства обхода контентной фильтрации ЕСПД (прокси-серверы, анонимайзеры, VPN-сервисы и т. п.) для доступа к заблокированным ресурсам.

7. Антивирусная защита

7.1. Антивирусная защита в Учреждении реализована в два уровня:

- **первый уровень – шлюзовой антивирус ЕСПД** (обеспечивается ПАО «Ростелеком»): проверка входящего интернет-трафика до его попадания в локальную сеть Учреждения, автоматическое обновление антивирусных баз со стороны оператора;
- **второй уровень — локальное АВПО** (Kaspersky Endpoint Security / Dr.Web): защита рабочих станций от угроз со съёмных носителей, локальной сети и программного обеспечения.

7.2. Обязательному антивирусному контролю на уровне рабочих станций подлежат:

- информация на съёмных носителях — вне зависимости от источника их получения;
- устанавливаемое (изменяемое) программное обеспечение;
- файлы, получаемые по локальной сети от других АРМ.

Примечание: шлюзовой антивирус ЕСПД не проверяет съёмные носители и локальный трафик — эти зоны покрываются только локальным АВПО.

7.3. Обновление антивирусных баз локального АВПО должно производиться автоматически не реже одного раза в день. Периодическая полная проверка всех компьютеров – не реже одного раза в неделю.

7.4. Внеочередная антивирусная проверка проводится при возникновении подозрения на наличие вируса (нетипичная работа программ, искажения данных, пропадание файлов и т. п.).

7.5. Пользователям запрещается: отключать АВПО во время работы; устанавливать иное антивирусное ПО; изменять настройки и конфигурацию АВПО.

7.6. При обнаружении вируса пользователь обязан немедленно приостановить все работы и сообщить АБИ. Ликвидация последствий заражения осуществляется АБИ.

8. Контентная фильтрация через ЕСПД

8.1. Доступ пользователей Учреждения к сети Интернет осуществляется через ЕСПД с обязательной контентной фильтрацией.

8.2. Контентная фильтрация обеспечивает блокировку:

- сайтов из единого реестра запрещённых ресурсов Роскомнадзора;
- материалов, содержащих экстремистский контент, пропаганду наркотиков, порнографию, информацию о способах суицида и кибербуллинга;
- нежелательной рекламы.

8.3. Дополнительно к базовой фильтрации АБИ через личный кабинет на портале espd.rt.ru может:

- формировать «белые» списки сайтов, доступ к которым разрешён всегда;
- формировать «чёрные» списки сайтов, доступ к которым блокируется дополнительно;
- включать принудительный безопасный режим поиска.

8.4. При некорректной блокировке образовательного ресурса (ложное срабатывание) АБИ направляет запрос на разблокировку через личный кабинет espd.rt.ru или по телефону техподдержки 8-800-301-34-14.

8.5. Пользователям запрещается использовать средства обхода контентной фильтрации: анонимайзеры, прокси-серверы, VPN-сервисы, средства обхода блокировок.

9. Учёт, хранение и обращение с СКЗИ и криптографическими ключами

9.1. СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учёту в журнале поэкземплярного учёта СКЗИ.

9.2. Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация хранятся у АБИ в условиях, исключающих бесконтрольный доступ и непреднамеренное уничтожение.

9.3. Криптографические ключи, электронная подпись и ключевые носители хранятся у пользователей СКЗИ в закрываемых на замок металлических хранилищах или сейфах. Резервные криптографические ключи хранятся у АБИ.

9.4. Ключевые носители подлежат обязательной маркировке с указанием реквизитов регистрации из журнала учёта и/или сертификата.

9.5. Изготовление криптографических ключей производится АБИ в присутствии пользователя. Плановая смена ключей осуществляется в сроки, указанные в сертификате ключа подписи.

9.6. Передача СКЗИ, документации и ключевых документов допускается только между пользователями и/или АБИ под подпись в журнале учёта СКЗИ и только с санкции АБИ.

9.7. Передача криптоключей по техническим средствам связи не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

9.8. Уничтожение криптоключей производится путём физического уничтожения ключевого носителя или стирания ключевой информации без повреждения носителя (для многократного использования). Уничтожение оформляется актом.

9.9. Выведенные из эксплуатации открытые ключи электронной подписи сохраняются в архивах в течение 5 (пяти) лет.

10. Действия при компрометации криптографических ключей

10.1. Компрометация ключевой информации — утрата или хищение действующих криптоключей, разглашение или несанкционированное копирование ключевой информации, угроза разглашения вследствие увольнения и иные аналогичные обстоятельства.

10.2. При возникновении обстоятельств, указывающих на возможную компрометацию, пользователь СКЗИ обязан незамедлительно уведомить АБИ.

10.3. АБИ обязан сообщить о компрометации руководителю Учреждения и оперативно оповестить всех пользователей СКЗИ.

10.4. Расследование проводится на месте происшествия уполномоченными лицами. По результатам составляется заключение о квалификации или отказе в квалификации события как компрометации.

10.5. При установлении факта компрометации скомпрометированные секретные ключи уничтожаются, производится изготовление и распределение новых ключей.

11. Резервное копирование

11.1. Резервное копирование данных осуществляется в автоматическом режиме с использованием встроенных средств Windows или вручную на внешний носитель.

11.2. Параметры и состав данных для резервного копирования определяются АБИ.

11.3. Резервные копии хранятся в условиях, исключающих несанкционированный доступ.

12. Порядок модификации технических и программных средств

12.1. Все изменения конфигурации технических и программных средств СЗИ, а также внесение изменений в настройки средств защиты от НСД и средств контроля целостности файлов производятся под контролем АБИ.

12.2. Вскрытие системного блока АРМ с установленным СКЗИ для ремонта или технического обслуживания осуществляется в присутствии АБИ.

13. Контроль и ответственность

13.1. Контроль за соблюдением требований настоящей Инструкции возлагается на АБИ.

13.2. Все сотрудники Учреждения, допущенные к работе с ИС, несут персональную ответственность за нарушение установленного порядка обработки и защиты информации.

13.3. За нарушение требований настоящей Инструкции сотрудники несут дисциплинарную ответственность в соответствии с действующим законодательством Российской Федерации.

13.4. При увольнении или переводе сотрудника: доступ к системам блокируется в течение 24 часов; проводится аудит активности сотрудника; сотрудник возвращает все носители информации и оборудование.

14. Заключительные положения

14.1. Все сотрудники Учреждения, допущенные к работе с ИС и СЗИ, должны быть ознакомлены с настоящей Инструкцией под роспись.

14.2. Изменения и дополнения в Инструкцию вносятся не реже одного раза в три года для обеспечения соответствия мер защиты актуальным условиям и требованиям законодательства в области информационной безопасности.

14.3. Инструкция вступает в силу с момента утверждения приказом директора Учреждения.