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
пользователя информационной системы по обеспечению защиты информации

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности и запреты для пользователей информационных систем (далее – ИС) МОБУ СОШ с. Мирный (далее – Учреждение).

1.2. Пользователь – сотрудник Учреждения, имеющий доступ к автоматизированному рабочему месту (далее – АРМ) и информационным ресурсам Учреждения.

1.3. Доступ к сети Интернет осуществляется через Единую сеть передачи данных (ЕСПД) с обязательной контентной фильтрацией и шлюзовым антивирусом, обеспечиваемыми ПАО «Ростелеком».

1.4. Ответственный за обеспечение безопасности информации (далее – АБИ) назначается приказом директора.

2. Обязанности пользователя

2.1. Перед началом работы убедиться, что антивирусное ПО запущено и работает корректно. Не отключать и не блокировать антивирус в течение рабочего дня.

2.2. Проводить антивирусную проверку любого съёмного носителя перед использованием — даже если носитель получен от коллеги. Шлюзовой антивирус ЕСПД проверяет только интернет-трафик и не контролирует флешки.

2.3. Использовать только личную учётную запись и пароль, полученный у АБИ. Не записывать пароль на бумаге, не сообщать его другим лицам, включая коллег и технических специалистов.

2.4. Использовать экранную заставку с паролем. Время бездействия до блокировки — не более 15 минут.

2.5. По окончании работы заблокировать экран или выйти из системы.

2.6. Использовать только учтённые съёмные носители. Запрещено использовать личные флешки без согласования с АБИ.

2.7. При работе с электронной подписью (СКЗИ) хранить ключевой носитель (Рутокен) в сейфе или запираемом ящике. Не передавать его другим лицам.

2.8. Немедленно сообщать АБИ о:

- подозрении на вирус (нетипичная работа программ, искажение данных, пропадание файлов);
- попытках несанкционированного доступа к информации;
- нарушении пломб/наклеек на системном блоке;
- некорректной работе СЗИ;
- обнаружении доступа к заблокированным сайтам (если это не связано с образовательной задачей).

2.9. Соблюдать правила контентной фильтрации ЕСПД. При необходимости доступа к образовательному ресурсу, который ошибочно заблокирован, обратиться к АБИ – он направит запрос на разблокировку через личный кабинет espd.rt.ru.

3. Пользователю запрещается

3.1. Отключать, удалять или изменять настройки антивирусного ПО, брандмауэра и других СЗИ.

3.2. Самостоятельно устанавливать, удалять или модифицировать любое программное обеспечение.

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

3.4. Использовать средства обхода контентной фильтрации ЕСПД: анонимайзеры, прокси-серверы, VPN-сервисы и т. п.

3.5. Записывать и хранить информацию на неучтённых носителях.

3.6. Передавать ключевые носители и электронную подпись другим лицам, использовать их на чужих АРМ.

3.7. Оставлять включённый компьютер без присмотра без блокировки экрана.

3.8. Копировать, тиражировать СКЗИ или использовать недокументированные свойства программного обеспечения.

3.9. Привлекать третьих лиц к работам с техникой и СЗИ без согласования с АБИ и руководителем.

3.10. Выносить носители информации за пределы помещения, в котором разрешена обработка, без разрешения АБИ.

4. Ответственность

4.1. Пользователь несёт персональную ответственность за нарушение требований настоящей Инструкции.

4.2. За нарушение установленных правил обработки и защиты информации к пользователю могут быть применены меры дисциплинарного взыскания в соответствии с Трудовым кодексом РФ.

4.3. При увольнении или переводе пользователь обязан сдать АБИ все носители информации, ключевые носители и оборудование, а также вернуть пароли и доступы.