ПРИНЯТО	СОГЛАСОВАНО	УТВЕРЖДЕНО
педагогическим советом	Управляющим	приказом директора
протокол №1	советом	МКОУ СОШ № 5
от 28.08.2025	протокол №1	г. Майского
	от 27.08.2025	№302/1 -ОД
		от 29.08.2025

ПОЛОЖЕНИЕ
о проведении проверок контентной фильтрации в МКОУ «Средняя общеобразовательная школа № 5 г. Майского» (с использованием ЕСПД ПАО «Ростелеком»)

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с:

Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 18.07.2017 № 26 «Об утверждении требований к единой сети передачи данных» (в части обнаружения и устранения инцидентов, Приложение 5) ;

Контрактом на оказание услуг доступа к сети Интернет с использованием ЕСПД, заключенным между ПАО «Ростелеком» и МКОУ «СОШ № 5 г. Майского»;

Уставом и локальными актами школы.

1.2. Настоящее Положение определяет порядок организации и проведения проверок функционирования системы контентной фильтрации, предоставляемой ПАО «Ростелеком» в рамках Единой сети передачи данных (ЕСПД).

1.3. ЕСПД (Единая сеть передачи данных) — это совокупность сетей, объединенных в единую систему с централизованным управлением и фильтрацией трафика. Оператором ЕСПД является ПАО «Ростелеком» .

1.4. Контентная фильтрация в рамках ЕСПД обеспечивает :

запрет доступа к ресурсам, входящим в реестр запрещенных сайтов Роскомнадзора и Федеральный список экстремистских материалов;

поддержание «белых» и «черных» списков интернет-сайтов;

блокировку вредоносного ПО и нежелательной рекламы;

принудительное включение безопасного режима поиска для поисковых систем.

2. Основные задачи проверок

2.1. Контроль работоспособности системы контентной фильтрации ЕСПД на всех устройствах школы.

2.2. Проверка корректности установки и актуальности корневого сертификата ПАО «Ростелеком» на рабочих станциях.

2.3. Контроль настроек прокси-сервера (адрес и порт, выдаваемые провайдером) на устройствах и оборудовании школы используемые в учебных процессах.

3. Ответственные лица

3.1. Ответственным за организацию проверок контентной фильтрации ЕСПД назначается приказом директора школы ответственный за функционирование системы контентной фильтрации.

3.2. Непосредственное проведение технических проверок осуществляется системным администратором (либо лицом, выполняющим его функции).

3.3. Администратор Личного кабинета ЕСПД назначается приказом директора и уполномочен на работу с порталом https://espd.rt.ru для формирования запросов на разблокировку/блокировку ресурсов.

3.4. Контроль за исполнением Положения возлагается на заместителя директора по учебно-воспитательной работе.

4. Виды и периодичность проверок

4.1. Ежедневный мониторинг осуществляется системным администратором путем выборочной проверки доступности интернета и загрузки сайтов через прокси-сервер ЕСПД.

4.2. Плановые проверки проводятся ежемесячно, не позднее 10-го числа текущего месяца. В ходе плановой проверки оцениваются:

работоспособность прокси-сервера ЕСПД;

наличие и корректность установленного сертификата Ростелекома на компьютерах;

актуальность настроек фильтрации (отображение в Личном кабинете);

анализ отчетов о заблокированных/разблокированных ресурсах за период;

проверка принудительного включения безопасного режима поиска.

4.3. Внеплановые проверки проводятся:

при сбоях в работе интернета и/или контентной фильтрации (инцидентах);

при поступлении информации о возможном доступе к запрещенным ресурсам;

после изменений в настройках оборудования или обновления ПО;

по предписанию органов управления образованием.

5. Порядок проведения проверки

5.1. Плановая проверка проводится комиссией, назначаемой приказом директора. В состав комиссии входят: ответственный за контентную фильтрацию, системный администратор.

5.2. В ходе проверки выполняется:

Проверка наличия и корректности настроек прокси-сервера на рабочих станциях и серверном оборудовании (адрес прокси, порт, обычно 10.0.7.52:3128);

Проверка установки корневого сертификата ПАО «Ростелеком» в доверенные центры сертификации ОС;

Проверка доступа к сайтам из контрольного перечня (запрещенные и разрешенные);

Вход в Личный кабинет ЕСПД через ЕСИА (Госуслуги) для проверки текущих списков фильтрации и статуса заявок.

5.3. При выявлении фактов доступа к ресурсам, подлежащим блокировке, комиссия проверяет:

наличие данных ресурсов в «черном списке» через Личный кабинет;

корректность работы прокси-сервера;

возможные причины сбоя (отключение фильтрации на устройстве, проблемы с сертификатом).

6. Порядок взаимодействия с ПАО «Ростелеком»

6.1. Для разблокировки или блокировки интернет-ресурсов, а также для решения технических проблем уполномоченный сотрудник (администратор Личного кабинета) направляет заявку через Личный кабинет ЕСПД по адресу: https://espd.rt.ru.

6.2. Авторизация в Личном кабинете осуществляется через Единую систему идентификации и аутентификации (ЕСИА) — учетную запись на портале Госуслуг.

6.3. При возникновении инцидентов (отсутствие доступа, сбой фильтрации более 1 минуты) школа незамедлительно уведомляет оператора ЕСПД

по телефону технической поддержки: 8 (800) 301-34-14;

через электронную почту: espd@rt.ru;

через Личный кабинет (раздел «Создание заявки»).

6.4. Устранение инцидентов на оборудовании (средствах связи) оператора осуществляется ПАО «Ростелеком». Школа обязана предоставить доступ к помещениям с оборудованием ЕСПД по запросу оператора.

7. Технические меры обеспечения безопасности

7.1. Использование фильтров контента, прокси-серверов, антивирусного ПО

7.2. Сегментация сети: отдельные VLAN для учебных устройств, административных компьютеров, гостевой сети.

7.3. Обязательное применение уникальных учётных записей и паролей соответствующей стойкости для сотрудников; смена пароля не реже одного раза в 6 месяцев для привилегированных аккаунтов.

7.4. Запрет на подключение к сети несертифицированных сетевых устройств без согласования с ИТ-администратором.

8. Удалённый доступ

8.1. Удалённый доступ (удалённый рабочий стол) предоставляется только сотрудникам по согласованию с директором и ИТ-администратором.

8.2. При использовании удалённого доступа обязательны: защищённые каналы связи, использование учётных данных Учреждения, обновлённое антивирусное ПО на клиентском устройстве.

9. Правила использования Интернета для учащихся и сотрудников

9.1. Интернет используется преимущественно в учебных и служебных целях. Личное использование допускается в свободное от учебного процесса время и в разумных пределах.

9.2. Запрещается:

- использовать Интернет для противоправной деятельности;
- устанавливать и запускать программное обеспечение без разрешения системного администратора;
- использовать несанкционированные VPN/прокси для обхода фильтров;
- распространять персональные данные и конфиденциальную информацию без разрешения;
- посещать запрещённые ресурсы.

9.3. Родители (законные представители) информируются о правилах и несут ответственность за действия несовершеннолетних при пользовании личными устройствами.

10. Реагирование на инциденты

10.1. Любые подозрительные события или нарушения немедленно сообщаются системному администратору и директору.

10.2. При подтверждённом инциденте доступ пользователя может быть временно приостановлен; проводится расследование, по результатам которого принимаются меры (восстановление доступа, дисциплинарные, уведомление родителей/правоохранительных органов при необходимости).

11. Ответственность и дисциплинарные меры

11.1. Нарушение Положения влечёт дисциплинарную ответственность в соответствии с внутренними правилами и трудовым законодательством.

11.2. В отдельных случаях возможно привлечение к административной или уголовной ответственности согласно законодательству.

12. Обучение и информирование

12.1. Все сотрудники проходят вводное обучение по безопасному использованию сети.

12.2. Для учащихся проводятся уроки и беседы по цифровой безопасности, защите персональных данных и правилам поведения в сети.