



**Порядок
контроля качества услуг, оказываемых провайдером,
в том числе проверки работы системы контентной фильтрации**

1. Общие положения.

1.1. Контроль качества услуг, в том числе проверка работы системы контентной фильтрации (далее – «СКФ») осуществляется на основании Федерального Закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федерального Закона от 28.07.2012 № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельных законодательных актов Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет», письма Министерства просвещения Российской Федерации от 07.06.2019 № 04-474 «О методических рекомендациях» (вместе с «Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования»).

1.2. Все компьютеры в школе (за исключением бухгалтерии) подключены к сети Интернет в соответствии с государственным контрактом № 19-ПК/20 на оказание услуг по предоставлению образовательным учреждениям Ярославской области в 2021г. доступа к сети «Интернет», к внутрисетевым ресурсам образовательных учреждений, подключаемых в рамках государственного контракта, и ГУ ЯО «Центр телекоммуникаций и информационных систем в образовании», и по ограничению доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (https://www.edu.yar.ru/index/inet_req2020.html) (далее - «Контракт»). Провайдером является Публичное акционерное общество «Ростелеком» (ПАО «Ростелеком») (далее – «Оператор», «Исполнитель»).

1.3. Предоставляемые услуги:

- организация каналов связи с целью обеспечения физического и логического доступа к сети «Интернет» в 2021 году с адресами подключений и скоростью доступа к ресурсам сети Интернет не менее 100 Мегабит в секунду;
- организация каналов связи с целью обеспечения физического и логического доступа к ресурсам других ОУ, перечисленных в приложении к Техническому заданию;
- организация каналов связи с целью обеспечения физического и логического доступа к ресурсам, предоставляемым ГУ ЯО «Центр телекоммуникаций и информационных систем в образовании» (находящемуся по адресу: 150000, г. Ярославль, ул. Собинова, д. 31/6, офис 204);
- контентная фильтрация и блокирование доступа к Интернет-ресурсам, причиняющим вред здоровью и (или) развитию детей, а также несовместимым с задачами обучения и воспитания;
- самовосстановление канала доступа после программно-аппаратных сбоев (сетевые атаки, взлом, перезагрузка, проверка на наличие ошибок и их исправление, возвращение к настройкам по умолчанию и т.д.) встроенными средствами самовосстановления;
- оказание круглосуточной технической поддержки.

1.4. Срок оказания услуги: с 01 января 2021 года по 31 декабря 2021 года включительно, ежедневно (включая выходные и праздничные дни), круглосуточно.

1.5. Данный Порядок устанавливает последовательность действий по организации контроля качества услуг, оказываемых провайдером.

2. Состав комиссии

Для проверки соответствия качества услуг требованиям, установленным Контрактом, создается комиссия, которая утверждается приказом по школе, в следующем составе:

- 1) заместитель директора школы по учебно-воспитательной работе, курирующий информационную безопасность, председатель комиссии
- 2) заместитель директора по безопасности, член комиссии
- 3) учитель информатики, член комиссии
- 4) учитель информатики, член комиссии

3. Порядок действий по проверке соответствия качества услуг, оказываемых провайдером

3.1. Проверка соответствия качества услуг, оказываемых провайдером, проводится в дни с наименьшей загруженностью сети Интернет. Накануне проверки в учительской размещается объявление о необходимости отключения компьютеров от сети Интернет на время проведения проверки.

3.2. Для проверки скорости Интернет-подключения перейти на сайт <https://www.speedtest.net/>
Зафиксировать в акте значение показателя Download, в Мегабитах в секунду.

3.3. Проверить доступ к ресурсам, предоставляемым ГУ ЯО «Центр телекоммуникаций и информационных систем в образовании» на сайте, расположенном по адресу <https://edu.yar.ru/>

3.4. Для проверки работы СКФ, предоставляемой Оператором, комиссия выбирает 3-4 материала, содержание которых может причинить вред здоровью и развитию обучающихся (Федеральный список экстремистских материалов - <https://minjust.gov.ru/ru/extremist-materials/>), пытается найти их по поиску, введя название материала (часть материала, сайта) в поисковую систему.

3.5. Из предложенного поисковой системой списка адресов нужно перейти на страницу сайта, содержащего противоправный контент. Если материал отображается и с ним можно ознакомиться без дополнительных условий – фиксируется факт нарушения работы системы контентной фильтрации.

При дополнительных условиях (требуется регистрация, условное скачивание, переадресация и т.д.), при выполнении которых материал отображается, также фиксируется факт нарушения работы системы контентной фильтрации.

При невозможности ознакомления с противоправным контентом при выполнении условий (регистрация, скачивание материалов, переадресация и т.д.) нарушение не фиксируется.

3.6. Комиссия вводит по очереди следующие запросы, не совместимые с задачами обучения и воспитания: «купить оружие», «сделать бомбу», «купить/изготовить наркотики», «порнография», «способы совершения самоубийства», «вступить в фашистскую организацию».

3.7. Из предложенного поисковой системой списка адресов нужно перейти по некоторым ссылкам, проанализировать информацию на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся.

3.8. При обнаружении сайтов или страниц сайтов в сети «Интернет», содержащих материалы с признаками запрещенной информации, необходимо выполнить следующие действия:

- открыть посредством интернет-браузера раздел сайта Роскомнадзора России «Единый реестр запрещенной информации» (<https://eais.rkn.gov.ru>). В подразделе «Прием сообщений» (<https://eais.rkn.gov.ru/feedback/>) сформировать сообщение о наличии на сайте или странице сайта в сети «Интернет» признаков запрещенной информации (поля, отмеченные знаком «*» обязательны для заполнения);

- в поле «Тип информации» следует выбрать один из типов запрещенного к распространению контента;

- в поле «Указатель страницы сайта в сети «Интернет» ввести конкретную ссылку на интернет-страницу сайта в сети «Интернет» (например, <http://example.com/example.html>), где содержатся признаки запрещенной информации;

- в подразделе «Заявитель» в полях «Отчество», «Место работы» имеется возможность указать соответствующие данные должностного лица, направившего сообщение и наименование организации;

- в поле «E-mail» следует указать действительный адрес электронной почты для получения уведомления о результатах обработки сообщения. На указанный адрес электронной почты будут направляться уведомления о принятии ссылок к рассмотрению и о включении их в Единый реестр.

3.9. Более подробную процедуру направления и рассмотрения сообщения по вопросу ограничения доступа к запрещённой информации, размещённой в сети «Интернет» можно посмотреть по ссылке <https://www.edu.yar.ru/safety/docs/algorithmbadcontent2018.pdf>

3.10. Проверить возможность выхода с компьютера в одну-две социальные сети: «ВКонтакте», «Одноклассники», twitter.com, facebook.com, livejournal.com и т.п.

3.11. Сделать отметку в журнале о проведении проверки (Приложение 1).

3.12. Оформить акт контроля качества услуг, оказываемых провайдером, в том числе проверки работы контентной фильтрации (Приложение 2).

3.13. При выявлении компьютеров, подключённых к сети Интернет и не имеющих контентной фильтрации, производится одно из следующих действий:

- немедленная установка и настройка СКФ (Приложение 3 – Инструкция по импорту сертификата Системы контентной фильтрации в браузер);
- немедленное программное и/или физическое отключение доступа к сети Интернет на выявленных компьютерах.

4. Подача заявки на изменение настроенной политики доступа к ресурсам в сети Интернет

Для блокировки либо разблокировки ресурсов в контентной фильтрации необходимо по адресу <http://skf.rtcn.cair.ru/> оставить заявку в электронном виде в Систему контентной фильтрации.

Для этого необходимо:

- перейти по ссылке <http://skf.rtcn.cair.ru/>
- нажать кнопку «Вернуться в начало»
- нажать кнопку «Открыть доступ» («Закреть доступ» - для блокировки).

5. Периодичность регулярного аудита

Проверка работы качества услуг, оказываемых провайдером, в том числе проверка работы СКФ проводится ежегодно перед началом учебного года в августе, далее не реже 1 раза в четверть.

6. Процедура внеплановой проверки

6.1. Внеплановая проверка качества услуг, оказываемых провайдером, проводится при возникновении проблем (отсутствие связи; сбой связи (с указанием продолжительности); обращение из ОУ к Интернет-ресурсу, содержащему информацию, запрещённую на территории Российской Федерации; обращение из ОУ к Интернет-ресурсу, содержащему информацию, не соответствующую задачам образования; обращение из ОУ к Интернет-ресурсу, содержащему потенциально опасную информацию).

6.2. В данном случае следует обращаться в службу технической поддержки ПАО «Ростелеком» по телефону 8-800-100-81-88.

6.3. При обращении необходимо предоставить следующую информацию:

- номер государственного контракта от 30.12.2020 № 19-ГК/20;
- номер лицевого счета № 876000070488 (ДИС ЯО ИНН 7604003600) ;
- название и шестизначный код образовательного учреждения (763902 – муниципальное бюджетное общеобразовательное учреждение средняя школа №2 им. В.И. Ленина г. Данилова Ярославской области);

- Ф.И.О. позвонившего и должность;
- контактный телефон позвонившего (сотовый или городской);
- причину обращения.

6.4. Служба технической поддержки работает все дни недели круглосуточно.

7. Форма отчёта

7.1. Факт проверки оформляется актом и фиксируется в журнале о проведении проверки с указанием номера кабинета и(или) инвентарного номера компьютера, результатов проверки и принятых мер (Приложение 1).

7.2. Формы документов утверждаются приказом образовательной организации.

7.3. Содержание отчёта должно отражать:

- дату проведения проверки;
- ФИО сотрудников, участвующих в процедуре;
- номер(а) кабинетов;
- общее количество компьютеров;
- количество компьютеров, подключённых к сети Интернет;
- информацию о проблеме (отсутствие связи; сбой связи (с указанием продолжительности); обращение из ОУ к Интернет-ресурсу, содержащему информацию, запрещённую на территории Российской Федерации; обращение из ОУ к Интернет-ресурсу, содержащему информацию, не совместимую с задачами образования; обращение из ОУ к Интернет-ресурсу, содержащему потенциально опасную информацию);
- соответствие/несоответствие фактической скорости предоставления доступа к сети Интернет (не ниже 100 мегабит в секунду);
- результаты проверки работы системы контентной фильтрации;
- вывод по результатам проверки.

Порядок принят с учётом мнения Управляющего совета
средней школы №2, протокол № ____ от _____

Ж у р н а л
контроля качества услуг, оказываемых провайдером,
в том числе проверки работы системы контентной фильтрации

Дата проверки	ФИО, должность проверяющего	Номер кабинета/компьютера	Результаты проверки	Принятые меры	Подпись проверяющего

А к т
проверки качества услуг, оказываемых провайдером,
в том числе проверки работы системы контентной фильтрации

« » 20 г.

№ _____

Комиссия в составе:

Председатель: _____

Члены комиссии: _____

Составили настоящий акт контроля качества услуг, оказываемых провайдером, в том числе проверки работы системы контентной фильтрации.

В ходе плановой/внеплановой проверки было выявлено:

1. Общие сведения

Показатель	Значение
Номера кабинетов	
Общее количество компьютеров	
Количество компьютеров, подключенных к сети Интернет	
Скорость предоставления доступа к сети Интернет (не ниже 100 Mbps) (при несоответствии указать номера кабинетов/компьютеров)	Соответствует/не соответствует в каб. №
Доступ к ресурсам, предоставляемым ГУ ЯО ЦТИСО (https://edu.yar.ru/) (При отсутствии доступа указать номер кабинета и/или компьютера)	Имеется/не имеется
Информация о проблеме (отсутствие связи; сбой связи (с указанием продолжительности) (указать суть проблемы и кабинет и(или) инвентарный номер компьютера)	

2. Результаты проверки работы системы контентной фильтрации

В ходе проверки был произведён набор и поиск информации, не совместимой с задачами образования и воспитания обучающихся.

Категории заархивной информации в образовательной организации	Возможность доступа (да*/нет)

Интернет-ресурсы из Федерального списка экстремистских материалов - https://minjust.gov.ru/ru/extremist-materials/	
Купить оружие	
Сделать бомбу	
Купить/изготовить наркотики	
Порнография	
Способы совершения самоубийства	
Вступить в фашистскую организацию	
Соцсети («ВКонтакте», «Одноклассники», twitter.com, facebook.com, livejournal.com и т.п.)	

**Если выбран ответ «да», указать номер кабинета и(или) инвентарный номер ПК, название ресурса/адрес сайта (страницы сайта).*

Вывод (выбрать пужное):

Контент-фильтр работает на всех компьютерах, имеющих выход в Интернет.

Контент-фильтр не работает на следующих ПК (с указанием номера кабинета и (или) инвентарного номера компьютера): _____

Принятые меры (обращение в службу технической поддержки ПЛО «Ростелеком» по телефону 8-800-100-81-88 с указанием номера обращения; сообщение на сайт Роскомнадзора в «Единый реестр запрещенной информации» с указанием номера уведомления; подача заявки на изменение настроенной политики доступа к ресурсам в сети Интернет по адресу <http://skf.rtcn.cair.ru/>);

Председатель комиссии _____ / _____
(подпись) (Ф. И. О.)

Члены комиссии _____ / _____
(подпись) (Ф.И.О.)

Приложение 3

Инструкция по импорту сертификата Системы контентной фильтрации в браузер

https://www.edu.yar.ru/index/inet_req2020.html

Особенности, связанные с фильтрацией HTTPS-трафика

Контентная фильтрация для сайтов, работающих по протоколу HTTPS, выполняется с подменой сертификата сайта. Для того чтобы Ваш браузер не выдавал предупреждение о недостоверном сертификате сайта, Вам необходимо импортировать корневой сертификат СКФ в браузер. Инструкция ниже.

Контентная фильтрация включается не для всего HTTPS-трафика, а только для списка HTTPS-сайтов, доступ к которым нельзя открыть или заблокировать полностью. В настоящее время это:

- Поиск Яндекс (<https://yandex.ru/>, <https://yandex.com/>, <https://yandex.by/>, ...)
- Поиск Google (<https://google.ru/>, <https://google.com/>, <https://google.by/>, ...)
- Сайты Google (<https://sites.google.com/>)
- Поиск Bing (<https://bing.com/>)

Инструкция по импорту сертификата в браузер

Для браузеров Internet Explorer, Opera, Google Chrome, Яндекс браузер.

Внимание! Перечисленные действия необходимо выполнить только один раз, чтобы сертификат стал доступен во всех указанных браузерах.

Скачайте корневой сертификат по этой ссылке и сохраните в любом каталоге, например, на Рабочем столе.

Если на ПК работают под одним пользователем:

1. Запустите файл корневого сертификата на исполнение, для чего выполните на нем двойной щелчок мышью.
2. В открывшемся окне "Сертификат" нажмите кнопку "Установить сертификат", затем кнопку "Далее".
3. В открывшемся окне выберите вариант "Поместить все сертификаты в следующее хранилище", нажмите кнопку "Обзор", выберите "Доверенные корневые центры сертификации", нажмите "ОК", "Далее", "Готово".
4. В открывшемся окне "Предупреждение о безопасности" нажмите "Да", затем нажмите "ОК".
5. Закройте окно "Сертификат".

Если на ПК работают под разными пользователями (выполняется с правами "Администратора"):

1. Нажмите кнопку "Пуск", выберите "Начать поиск", введите mmc, а затем нажмите клавишу "ВВОД".
2. В меню "Файл" выберите пункт "Добавить или удалить оснастку".
3. В группе "Доступные" оснастки щелкните "Сертификаты", а затем нажмите кнопку "Добавить".
4. В группе "Эта оснастка всегда будет управлять сертификатами для" щелкните "Учетная запись компьютера", а затем нажмите кнопку "Далее".
5. Щелкните "Локальный компьютер", а затем нажмите кнопку "Готово".
6. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку "ОК".
7. В дереве консоли дважды щелкните "Сертификаты".
8. Щелкните правой кнопкой мыши хранилище "Доверенные корневые центры сертификации".
9. Нажмите кнопку "Импорт", чтобы импортировать сертификаты и выполнить инструкции мастера импорта сертификатов.

Для браузера Firefox.

1. Скачайте корневой сертификат по этой ссылке и сохраните в любом каталоге, например, на Рабочем столе.
2. Запустите Firefox, в меню выберите "Инструменты", "Настройки".
3. Выберите раздел "Дополнительные", затем вкладку "Сертификаты", нажмите кнопку "Просмотр сертификатов".
4. В открывшемся окне "Управление сертификатами" выберите вкладку "Центры сертификации", нажмите кнопку импортировать, выберите сохраненный файл сертификата и нажмите "Открыть".
5. В открывшемся окне "Загрузка сертификата" установите флажок "Доверять при идентификации web-сайтов", затем нажмите "ОК" и еще раз "ОК".
6. Закройте вкладку настроек браузера Firefox.