

Министерство образования Ярославской области государственное
профессиональное образовательное автономное учреждение Ярославской области
Ярославский колледж сервиса и дизайна

УТВЕРЖДЕНО
приказом и.о. директора
ГПОАУ ЯО
Ярославского колледжа
сервиса и дизайна
№ 01-07/401а от 01.09.2023

**ПОРЯДОК
КОНТРОЛЯ КАЧЕСТВА УСЛУГИ ПОДКЛЮЧЕНИЯ К СЕТИ
ИНТЕРНЕТ**

г. Ярославль

2023

1 Общие положения

1. Для обеспечения доступа общеобразовательных организаций в сеть «Интернет» посредством Единой сети передачи данных (далее - ЕСПД) Минцифрой РФ заключен федеральный Государственный контракт Актуальный контракт Минцифры РФ и ПАО «Ростелеком» от 31.08.2023 № 071/23/89 на оказание услуг ЕСПД образовательным организациям и объектам ЦИК в период с 01.09.2023 по 31.12.2023:

Актуальная версия контракта размещается по адресу:

<https://zakupki.gov.ru/epz/contract/contractCard/common-info.html?reestrNumber=1771047437523000107>

2. Контроль скорости интернет осуществляется 1 раз в месяц с записью в журнал «Контроля предоставления интернет услуг».

Контроль осуществляется на компьютерах:

- Скорость интернет - компьютеры директора, бухгалтерии, заместителей директора;
- Контентной фильтрации - компьютерные классы для занятий по информатике, информационным технологиям, компьютерному моделированию и графическому дизайну – три раза в течение учебного года.

3. При возникновении проблем производятся действия в обращении в Ситуационный Центр Минцифры РФ по поводу проблем со скоростью или отсутствия Интернет. При обращении указывается:

- Название социально-значимого объекта;
- Адрес социально-значимого объекта;
- ФИО, должность и контактные данные (телефон, эл. адрес);
- Дата и время возникновения проблемы;
- Описание проблемы (недоступность или ухудшение качества);
- Наличие электропитания в здании;
- Наличие электропитания в помещении;
- Наличие электропитания на оконечном оборудовании;
- Информация о перезагрузке оборудования.

Служба технической поддержки работает все дни недели круглосуточно.

4. Организация работы по защите данных, по ограничению доступа к информации, распространение которой в РФ запрещено, к информации, причиняющей вред здоровью и (или) развитию детей оговаривается действующим контрактом.

4.1. Проверку эффективности использования систем контентной фильтрации Интернет ресурсов в ГПОАУ ЯО Ярославском колледже сервиса и дизайна проводит ответственный за информационную безопасность системный администратор - три раза в течение учебного года.

4.2. Ответственный за информационную безопасность системный администратор проверяет работоспособность системы контентной фильтрации на всех компьютерах образовательной организации путем ввода в поле поиска любого браузера ключевые слова из списка информации, запрещенной для просмотра обучающимися, с последующими попытками загрузки сайтов из найденных. В том числе ответственный за информационную безопасность проверяет, загружается ли информация, причиняющая вред здоровью и развитию обучающихся, не имеющая отношения к образовательному процессу, в социальных сетях и общедоступных сайтах.

4.3. Чтобы провести проверку, ответственный за информационную безопасность системный администратор выбирает три-четыре ресурса с информацией, причиняющей вред здоровью и (или) развитию обучающихся, а также не соответствующей задачам образования.

4.4. В качестве проверочных ресурсов ответственный за информационную безопасность системный администратор использует сайты в том числе из списка экстремистских материалов <https://shinjust.gov.ru/ru/extremist-materials>

4.5. Ответственный за информационную безопасность вносит название материала (части материала, адрес сайта) в поисковую строку браузера. Из предложенного списка адресов переходит на страницу сайта, содержащего негативный контент.

4.6. Если материал отображается и с ним можно ознакомиться без дополнительных условий, ответственный за информационную безопасность фиксирует факт нарушения работы системы контентной фильтрации.

4.7. Если ресурс требует дополнительных действий (регистрации, условного скачивания, переадресации и т. д.), при выполнении которых материал отображается, ответственный за информационную безопасность также фиксирует факт нарушения работы системы контентной фильтрации.

4.8. Если невозможно ознакомиться с негативным контентом при выполнении дополнительных условий (регистрации, скачивания материалов, переадресации и т. д.), нарушение не фиксируется.

4.9. Ответственный за информационную безопасность системный администратор составляет три - четыре запроса в поисковой строке браузера, состоящих из слов, которые могут однозначно привести на запрещенные для несовершеннолетних ресурсы, например по темам: экстремизм, проявление жестокости, порнография, терроризм, суицид, насилие и т. д. К примеру, вводятся фразы («изготовление зажигательной бомбы», «издевательства над несовершеннолетними», «способы суицида»).

4.10. Из предложенного поисковой системой списка адресов ответственный за информационную безопасность переходит на страницу двух-трех сайтов и знакомится с полученными материалами.

4.11. Ответственный за информационную безопасность дает оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся.

4.12. Если обнаруженный материал входит в перечень запрещенной для детей информации (Приложение № 1 к Методическим рекомендациям 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, утв. Минкомсвязи 16.05.2019), ответственный за информационную безопасность фиксирует факт нарушения с указанием источника и критериев оценки.

4.13. Если найденный материал нарушает законодательство Российской Федерации, то ответственный за информационную безопасность направляет сообщение о противоправном ресурсе в Роскомнадзор через электронную форму на сайте <https://eais.rkn.gov.ru/feedback/>.

4.14. По итогам мониторинга ответственный за информационную безопасность оформляет акт проверки контентной фильтрации в образовательной организации по форме из приложения к Порядку (приложение 1).

4.15. Если ответственный за информационную безопасность выявил сайты, которые не входят в Реестр безопасных образовательных сайтов, то перечисляет их в акте проверки контентной фильтрации в образовательной организации.

АКТ
Проверки контентной фильтрации
№ _____ от _____

1. Общие сведения

Показатель	Количество компьютеров	Значение
Компьютерные классы		
№		
№		
№		
№		
№		
№		
№		
Количество компьютеров в локальной сети		
Корпус 1 ул. Автозаводская д. 5/1		
Корпус 2 ул. Большая Федоровская д.119		
Количество компьютеров подключенных к сети Интернет		
Корпус 1 ул. Автозаводская д. 5/1		
Корпус 2 ул. Большая Федоровская д.119		
Провайдер		
Скорость передачи данных		

2. Информация о контент фильтре

Действия необходимые для обеспечения контентной фильтрации Интернет ресурсов	Выполнение (да/нет)
Контент – фильтр работает на всех ПК где есть доступ к сети Интернет	

3. Результаты проверки работы системы контентной фильтрации

Категории запрещенной информации в образовательной организации	Возможность доступа
Перечень видов информации запрещенной к распространению, Ресурсы Интернет не включенные в реестр безопасных образовательных сайтов	

Системный администратор _____