Утверждаю
Директор ГОУ ЯО «Ярославская школа-интернат имени Э.Н. Макшшанцевой»

А.Л. Саватеева
«02» сентября 2024 г.

Порядок контроля качества услуги подключения к сети интернет

1. Для обеспечения доступа общеобразовательных организаций в сеть «Интернет» посредством Единой сети передачи данных (далее - ЕСПД) Минцифрой РФ заключен контракт с ПАО «Ростелеком» на оказание услуг ЕСПД образовательным организациям.

2. Контроль скорости Интернет-соединения осуществляется 1 раз в месяц на всех компьютерах ОУ.

3. Контроль контентной фильтрации осуществляется 1 раз в четверть на компьютерах в компьютерном классе, а также на всех компьютерах, к которым имеют доступ обучающиеся.

4. При возникновении проблем, связанных с низкой скоростью или отсутствием Интернет-соединения осуществляется обращении в Ситуационный Центр Минцифры РФ. 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.

5. 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.

5.1 Проверку эффективности использования систем контентной фильтрации Интернет-ресурсов в ГОУ ЯО «Ярославская школа-интернат имени Э.Н. Макшанцевой» проводит ответственный за информационную безопасность – два раза в течение учебного года.

5.2 Ответственный за информационную безопасность 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.

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

5.4 В качестве проверочных ресурсов ответственный за информационную безопасность использует сайты в том числе из списка экстремистских материалов https://minjust.gov.ru/ru/extremist-materials/.

5.5 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.

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

5.7 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.

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

5.9 Ответственный за информационную безопасность 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».

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

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

5.12 Если обнаруженный материал входит в перечень запрещенной для детей информации, ответственный за информационную безопасность фиксирует факт нарушения с указанием источника и критериев оценки. 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/.

5.13 По итогам мониторинга ответственный за информационную безопасность делает запись в журнале регистрации случаев обнаружения сайтов, причиняющих вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.