|  |  |
| --- | --- |
| РАССМОТРЕНО:  На педагогическом совете  Протокол от 11.11.2024г. № 2 | УТВЕРЖДЕНО:  Приказом директора № 589 о/д от 11.11.2024г. |

ПОРЯДОК

контроля качества услуги, оказываемой провайдером Ростелеком

муниципальному общеобразовательному учреждению

Ишненская средняя общеобразовательная школа

1. Для обеспечения доступа общеобразовательных организаций в сеть «Интернет» по средствам Единой сети передачи данных (далее — ЕСПД) Минцифрой РФ заключен федеральный Государственный контракт с ПAO «Ростелеком».
2. Контроль скорости интернет осуществляется 1 раз в 2 недели с записью в журнал «Контроля предоставления интернет услуг».

Контроль осуществляется на компьютерах:

* Скорость интернет — компьютеры директора, заместителей директора;
* Контентной фильтрации — компьютерный класс, три раза в течение учебного года.

1. При возникновении проблем производятся действия в соответствии с Регламентом технической поддержки при оказании Услуги. Контактные данные технической поддержки: телефон 8-800-301-34-14. 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 конечном оборудовании
* Информация о перезагрузке оборудования

Служба технической поддержки работает все дни недели круглосуточно.

1. 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.
   1. Проверку эффективности использования систем контентной фильтрации Интернет- ресурсов в МОУ Ишненская СОШ проводит ответственный за информационную безопасность три раза в течение учебного года.
   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 детей, не имеющая отношения к образовательному процессу, в социальных сетях: ВКонтакте, Одноклассники, Твиттер, Фейсбук, Инстаграм, Живой Журнал и др.
   3. В качестве проверочных ресурсов ответственный за информационную безопасность использует сайты в том числе из списка экстремистских материалов
   4. 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 конвент.
   5. Если материал отображается и с ним можно ознакомиться без дополнительных условий, ответственный за информационную безопасность фиксирует факт нарушения работы системы контентной фильтрации.
   6. Если pecypc 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.
   7. Если невозможно ознакомиться с негативным контентом при выполнении дополнительных условий (регистрации, скачивания материалов, переадресации и т. д.), нарушение не фиксируется.
   8. Ответственный за информационную безопасность составляет три-четыре запроса в поисковой строке браузера, состоящих из слов, которые *мог*ут 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».
   9. Из предложенного поисковой системой списка адресов ответственный за информационную безопасность переходит на страницу двух—трех сайтов и знакомится с полученными материалами.
   10. Ответственный за информационную безопасность дает оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся.
   11. Если обнаруженный материал входит в перечень запрещенной для детей информации, ответственный за информационную безопасность фиксирует факт нарушения с указанием источника и критериев оценки.
   12. Если найденный материал нарушает законодательство Российской Федерации, то ответственный за информационную безопасность направляет сообщение о противоправном pecypce в Роспотребнадзор через электронную форму.
   13. По итогам мониторинга ответственный за информационную безопасность оформляет акт проверки контентной фильтрации в образовательной организации по форме из приложения к Порядку.
   14. 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.

ПРИЛОЖЕНИЕ 1

АКТ

проверки контентной фильтрации в МОУ Ишненской СОШ

№ ОТ

1. Общие сведения

|  |  |
| --- | --- |
| Показатель | Значение |
| Количество компьютерных классов |  |
| Общее количество компьютеров |  |
| Количество компьютеров в локальной сети |  |
| Количество компьютеров, подключенных к сети Интернет |  |
| Провайдер |  |
| Скорость передачи данных |  |

1. Информация

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

1. Результаты проверки работы системы контентной фильтрации

|  |  |
| --- | --- |
| Категории запрещенной информации в образовательной организации | Возможность доступа |
| Перечень видов информации, запрешенной к распространению  посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования согласно Методическим рекомендации 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 |  |
| Интернет-ресурсы, не включенные в Реестр безопасных  образовательных сайтов |  |

Ответственный за информационную безопасность

Директор школы