

РОССИЙСКАЯ ФЕДЕРАЦИЯ
УПРАВЛЕНИЕ ОБРАЗОВАНИЯ БРЯНСКОЙ ГОРОДСКОЙ АДМИНИСТРАЦИИ
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №11 ИМЕНИ П.М.КАМОЗИНА» Г.БРЯНСКА
(МБОУ СОШ №11 г.Брянска)

ПРИНЯТО
на заседании педагогического совета
МБОУ СОШ №11 г. Брянска
Протокол № 2
от 05 февраля 2024 года

УТВЕРЖДАЮ:
Директор МБОУ СОШ №11 г. Брянска
_____ А.Н.Семигулин
Приказ № 69В
от 05 февраля 2024 года

**ПОРЯДОК
ПРОВЕДЕНИЯ ПРОВЕРКИ ЭФФЕКТИВНОСТИ
ИСПОЛЬЗОВАНИЯ СИСТЕМ КОНТЕНТНОЙ ФИЛЬТРАЦИИ
ИНТЕРНЕТ-РЕСУРСОВ**

**Муниципального бюджетного общеобразовательного учреждения «Средняя
общеобразовательная школа № 11 имени П.М.Камозина» г.Брянска**

1. Общие положения

- 1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации интернет - ресурсов в МБОУ СОШ № 11 г.Брянска (далее - Порядок) определяет процедуру проверки работы системы контентной фильтрации в МБОУ СОШ № 11 г.Брянска (далее - школа).
- 1.2. Порядок разработан в соответствии с Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», 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, утвержденными Минкомсвязи 16.05.2019, и использует терминологию, которая введена ранее перечисленными правовыми актами.

2. Порядок проверки системы контентной фильтрации

- 2.1. Проверку эффективности использования систем контентной фильтрации интернет - ресурсов в МБОУ СОШ № 11 г.Брянска проводит ответственный за информационную безопасность 6 раз в год (один раз в два месяца).
- 2.2. 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, Телеграм, и др.
- 2.3. Чтобы провести проверку, ответственный за информационную безопасность выбирает три-четыре ресурса с информацией, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в том числе ищет информационную продукцию, запрещенную для детей, в форме сайтов, графических изображений, аудиовизуальных произведений и других форм информационной продукции.
- 2.4. В качестве проверочных ресурсов ответственный за информационную безопасность использует сайты в том числе из списка экстремистских материалов -

<http://miniust.ru/nko/fedspisok>.

- 2.5. 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.
- 2.6. Если материал отображается и с ним можно ознакомиться без дополнительных условий, ответственный за информационную безопасность фиксирует факт нарушения работы системы контентной фильтрации.
- 2.7. 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.
- 2.8. Если невозможно ознакомиться с негативным контентом при выполнении дополнительных условий (регистрации, скачивания материалов, переадресации и т. д.), нарушение не фиксируется.
- 2.9. 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».
- 2.10. Из предложенного поисковой системой списка адресов ответственный за информационную безопасность переходит на страницу двух-трех сайтов и знакомится с полученными материалами.
- 2.11. Ответственный за информационную безопасность дает оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся.
- 2.12. 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.
- 2.13. Если найденный материал нарушает законодательство Российской Федерации, то ответственный за информационную безопасность направляет сообщение о противоправном ресурсе в Роскомнадзор через электронную форму на сайте <http://eais.rkn.gov.ru/feedback/>.
- 2.14. По итогам мониторинга ответственный за информационную безопасность оформляет акт проверки контентной фильтрации в образовательной организации по форме из приложения к Порядку.
- 2.15. 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.
- 2.16. При выявлении компьютеров, подключенных к сети интернет и не имеющих системы контентной фильтрации, производится одно из следующих действий:
 - немедленная установка и настройка системы контентной фильтрации;
 - немедленное программное и/или физическое отключение доступа к сети интернет на выявленных компьютерах.

*Приложение
к Порядку проведения проверки эффективности
использования систем контентной фильтрации
Интернет-ресурсов в МБОУ СОШ № 11 г.Брянска*

Акт проверки контентной фильтрации в

« ____ » _____ 20__ г.

№ _____

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 | |

2. Информация о контент-фильтре

| Действия, необходимые для обеспечения контентной фильтрации Интернет-ресурсов | Выполнение (да/нет) |
|--|----------------------------|
| Установлен контент-фильтр | |
| Название контент-фильтра | |
| Контент-фильтр работает на всех компьютерах, где есть доступ в сеть Интернет | |

2. Результаты проверки работы системы контентной фильтрации

| Категории заращённой информации в образовательной организации | Возможность доступа (да/нет) |
|--|-------------------------------------|
| Перечень видов информации, запрещенной 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 включённые в Реестр безопасных образовательных сайтов | |

Члены комиссии по проведению проверки работы системы контентной фильтрации в образовательной организации:

Председатель комиссии

_____/_____
(подпись) (Ф. И. О.)

Члены комиссии

_____/_____
(подпись) (Ф.И.О.)

_____/_____
(подпись) (Ф.И.О.)

С актом ознакомлен.

Директор _____/_____
(подпись) (Ф.И.О.)

"__" _____ 20__ г.

