



Утверждаю
Директор МОАУ СОШ № 7
Н.Л.Байрузова
Приказ № 405 от 29.08.2025г.

**Порядок
проведения проверки эффективности использования
системы контентной фильтрации интернет-ресурсов
в муниципальном общеобразовательном автономном учреждении средняя
общеобразовательная школа № 7
ГО г.Нефтекамск Республики Башкортостан**

1. Общие положения

1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов в муниципальном общеобразовательном автономном учреждении средняя общеобразовательная школа № 7 ГО г.Нефтекамск Республики Башкортостан (далее – Порядок) определяет процедуру проверки работы системы контентной фильтрации в муниципальном общеобразовательном автономном учреждении средняя общеобразовательная школа № 7 (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 16.05.2024, и использует терминологию, которая введена ранее перечисленными правовыми актами.

2. Порядок проверки системы контентной фильтрации

2.2. Проверку эффективности использования систем контентной фильтрации интернет-ресурсов в Школе проводит ответственный за информационную безопасность ежемесячно в течение учебного года.

2.3. Ответственный за информационную безопасность проверяет работоспособность системы контентной фильтрации на всех компьютерах Школы путем ввода в поле поиска любого браузера ключевые слова из списка информации, запрещенной для просмотра учащимися, 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 и др.

2.4. 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.

2.5. В качестве проверочных ресурсов ответственный за информационную безопасность использует сайты в том числе из списка экстремистских материалов – <http://minjust.ru/nko/fedspisok>.

2.5.1. 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.

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

2.5.3. 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.

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

2.6. 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».

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

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

2.6.3. 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.

2.7. 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/>.

2.8. Ответственный за информационную безопасность проверяет работоспособность журнала, фиксирующего адреса сайтов, посещаемых с компьютеров Школы.

2.9. По итогам мониторинга ответственный за информационную безопасность оформляет акт проверки контентной фильтрации в Школе по форме из приложения к Порядку.

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

2.11. 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.

Акт проверки контентной фильтрации в _____
 " ____ " _____ 20__ г.

1. Общие сведения

Количество компьютерных классов: _____. Общее количество ПК в этих классах: _____.

Количество ПК, подключенных к сети Интернет, к которым имеют доступ обучающиеся: _____.

Провайдер: _____.

Скорость доступа к Интернету, замеренная при проверке (Мбит/сек): _____.

2. Информация о контент-фильтре

Действия, необходимые для обеспечения контентной фильтрации интернет-ресурсов	Выполнение (да/нет)
Название установленного контент-фильтра	
Выполнены установки контент-фильтра, блокирующие выход к Интернет-ресурсам, не совместимым с задачами образования и воспитания учащихся, во исполнении положений Федерального закона от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющий вред их здоровью и развитию»	
Контент-фильтр работает на всех компьютерах, где есть доступ в сеть Интернет для обучающихся	

3. Информация о наличии нормативной документации

Наименование документов	Наличие (да/нет)
Наличие приказа (или пункта в приказе) о назначении ответственного за контентную фильтрацию	
Инструкция ответственного по работе с программой контентной фильтрации	
Журнал регистрации случаев обнаружения интернет-ресурсов, не совместимых с задачами образования и воспитания учащихся.	

4. Результаты проверки работы системы контентной фильтрации

Наименования запросов	Возможность доступа (да/нет)
Купить оружие	
Сделать бомбу, сделать взрывное устройство	
Купить наркотики, изготовить наркотики	
Порнография, секс	
Самоубийство, суицид	
Способы самоубийства	
Вступить в фашистскую организацию	
<...>	

Члены комиссии по проведению проверки работы системы контентной фильтрации в ОО:

Должность и ФИО проверяющего _____ / _____ / _____
 (должность) (Ф. И. О.) (подпись)

С актом ознакомлен:

Ответственный за работу контентной фильтрации _____ / _____
 (подпись) (Ф.И.О.)

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