

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №12»
ГОРОДА ОБНИНСКА**

249039, Калужская область, г. Обнинск, ул. Калужская, д. 5
тел. (484)393-92-64, эл. почта: office@school012.ru сайт <http://school012.ru>

ПРИНЯТО:
Педагогическим советом
протокол № 10 от 11.01 2022

УТВЕРЖДАЮ:
Директор МБОУ «СОШ № 12»
_____ И.М. Титова
приказ № 10-р от 11.01.2022

**Порядок проведения проверки
эффективности использования системы контентной фильтрации
интернет-ресурсов в МБОУ «СОШ №12»**

1. Общие положения

1.1. Порядок проведения проверки эффективности использования контентной фильтрации интернет-ресурсов в МБОУ «СОШ №12» (далее- Порядок) определяет процедуру проверки работы системы контентной фильтрации в МБОУ «СОШ №12» (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 Школе проводит ответственный за информационную безопасность не реже 1 раза в квартал.

2.2. 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 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» и др.

2.3. Для проведения проверки, ответственный за информационную безопасность выбирает 3-4 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://minjust.ru/nko/fedspisok>.

2.4.1. 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.

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

2.4.3. 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.

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

2.5. Ответственный за информационную безопасность составляет 3-4 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».

2.5.1. Из предложенного поисковой системой списка адресов ответственный за информационную безопасность переходит на страницу 2-3 сайтов и знакомится с полученными материалами.

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

2.5.3. 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.

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

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

2.8. По итогам мониторинга ответственный за информационную безопасность оформляет акт проверки контентной фильтрации.

2.9. 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.

2.10. 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.