

Муниципальное общеобразовательное бюджетное учреждение

«Шопшинская сш»



**Порядок проведения проверки эффективности использования  
Системы контентной фильтрации Интернет-ресурсов  
в МОБУ «Шопшинская сш»**

**1. Общие положения**

1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации Интернет-ресурсов в МОБУ «Шопшинская сш» (далее-Порядок) определяет процедуру проверки работы системы контентной фильтрации в МОБУ «Шопшинская сш» (далее- образовательная организация).

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, причиняющий вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утверждёнными Минкомсвязи 16.05.2019.

**2. Порядок проверки системы контентной фильтрации**

2.1. Проверку эффективности использования систем контентной фильтрации Интернет-ресурсов в образовательной организации проводят ответственный за информационную безопасность в течение учебного года не реже 4-х раз.

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 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, Твиттер, Фейсбук, Инстаграм, Живой Журнал (livejournal. Com) 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, запрещённую для детей в форме сайтов, графических изображений, аудиовизуальных произведений и других форм информационной продукции.

2.4. В качестве проверочных ресурсов ответственный за информационную безопасность и 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 так же фиксирует факт нарушения работы системы контентной фильтрации.

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

2.4.5. Ответственный за информационную безопасность составляет три-четыре запроса в поисковой строке браузера, состоящих из слов, которые могут однозначно привести на запрещённые для несовершеннолетних ресурсы, например по темам: экстремизм, проявление жестокости, порнографии, терроризм, суицид, насилие и т.д. К примеру, вводятся фразы «изготовление зажигательной бомбы», «издевательства над несовершеннолетними», «способы суицида».

2.5.1. Из предложенного поисковой системы списка адресов ответственный за информационную безопасность переходит на страницу двух-трёх сайтов и знакомится с полученными материалами.

2.5.2. Ответственный за информационную безопасность даёт оценку материалом на предмет возможного нанесения ущерба физическому и психологическому здоровью учащихся.

2.5.3. Если обнаруженный материал входит в перечень запрещённой для детей информации ( Приложение №1 к Методическим рекомендациям по ограничению образовательных организациях доступа, обучающихся к видам информации, распространяемой посредством сети интернет, причиняющей вред здоровью и (или) развитию детей, а так же 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 форму на сайте <http://eais/rkn.gov.ru/feedback/>.

2.7. По итогам мониторинга ответственный за информационную безопасность оформляет акт проверки контентной фильтрации в образовательной организации.

2.8. 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.

2.9. При выявлении компьютеров, 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.