

УТВЕРЖДАЮ:

Директор МКОУ «СОШ №2»

им. генерала армии В.И. Исакова

В.Г. Майоров

Приказ от 31.08.2021 г. № 100



ПОРЯДОК

проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов в муниципальном казенном общеобразовательном учреждении «Средняя общеобразовательная школа №2» имени генерала армии В.И. Исакова

1. Общие положения

1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов (далее - Порядок) определяет процедуру проверки работы системы контентной фильтрации в МКОУ «СОШ №2» им. генерала армии В.И. Исакова (далее - образовательная организация).

2. Порядок проверки системы контентной фильтрации

1.1. Проверку эффективности использования систем контентной фильтрации интернет-ресурсов проводит ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации в течение учебного года.

1.2. Ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации 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 и обеспечение безопасного доступа к сети Интернет в образовательной организации 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.

1.3. Чтобы провести проверку, ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации 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.

1.4. В качестве проверочных ресурсов ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации использует сайты в том числе из списка экстремистских материалов.

1.4.1. Ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации вносит название материала (части материала, адрес сайта) в поисковую строку браузера. Из предложенного списка адресов переходит на страницу сайта, содержащего негативный контент.

1.4.2. Если материал отображается и с ним можно ознакомиться без дополнительных

условий, ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации фиксирует факт нарушения работы системы контентной фильтрации.

1.4.3. Если ресурс требует дополнительных действий (регистрации, условного скачивания, переадресации и т. д.), при выполнении которых материал отображается, ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации также фиксирует факт нарушения работы системы контентной фильтрации.

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

1.5. Ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации 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».

1.5.1. Из предложенного поисковой системой списка адресов ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации переходит на страницу двух-трех сайтов и знакомится с полученными материалами.

1.5.2. Ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации дает оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся. 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 и обеспечение безопасного доступа к сети Интернет в образовательной организации фиксирует факт нарушения с указанием источника и критериев оценки.

1.6. Если найденный материал нарушает законодательство Российской Федерации, то ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации направляет сообщение о противоправном ресурсе в Роскомнадзор через электронную форму на сайте <http://eais.rkn.gov.ru/feedback/>. Ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет проверяет работоспособность журнала, фиксирующего адреса сайтов, посещаемых с компьютеров образовательной организации.

1.7. По итогам мониторинга ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации оформляет акт проверки контентной фильтрации в образовательной организации по форме из приложения к Порядку.

1.8. Если ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации выявил сайты, которые не входят в Реестр безопасных образовательных сайтов, то перечисляет их в акте проверки контентной фильтрации в образовательной организации.

1.9. 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
МКОУ «СОШ №2» им. генерала армии В.И. Исакова**

« ___ » _____ 20__ г.

№ _____

1. Общие сведения

Количество компьютерных классов: _____

Общее количество компьютеров: _____

Количество компьютеров в локальной сети: _____

Количество компьютеров, подключенных к сети Интернет: _____

Провайдер: ОАО «Ростелеком»

Установленный СКФ «UserGate Web Filter»

Скорость передачи данных: _____

2. Информация о контент-фильтре

Действия, необходимые для обеспечения контентной фильтрации интернет-ресурсов	Выполнение (да/нет)
Установлен контент-фильтр	
Выполнены установки контент-фильтра, блокирующие выход к Интернет-ресурсам, не совместимым с задачами образования и воспитания учащихся	
Вручную и автоматически запрещены выходы на сайты общественных и религиозных объединений, иных некоммерческих организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25.07.2002 № 114-ФЗ "О противодействии экстремистской деятельности"	
Контент-фильтр работает на всех компьютерах, где есть доступ в сеть Интернет	

3. Информация о наличии нормативной документации

Наименование документов	Наличие (да/нет)
Приказ о назначении ответственного за работу точки доступа к сети Интернет	
Инструкция ответственного за работу точки доступа к сети Интернет	
Правила пользования сети Интернет в МКОУ «СОШ №2» им. генерала армии В.И. Исакова	
Журнал учёта доступа в сеть Интернет	
Журнал контроля контентной фильтрации	
Регламент работы педагогов и учащихся в сети Интернет	

4. Результаты проверки работы системы контентной фильтрации

Наименования запросов	Возможность доступа (да/нет)
Нелегальное видео	
Купить оружие	
Сделать бомбу	
Купить наркотики	
Секс	
Порнография	
Суицид	

