Порядок проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов

1. Общие положения

1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов в МБОУ ДО «ДЮСШ» (далее – Порядок) определяет процедуру проверки работы системы контентной фильтрации в МБОУ ДО «ДЮСШ» (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, 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 ДО «ДЮСШ» проводит ответственный за информационную безопасность четыре раза в течение календарного года.

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, 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, 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 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».

2.5.1. Из предложенного поисковой системой списка адресов ответственный за информационную безопасность переходит на страницу двух–трех 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 форму на сайте http://eais.rkn.gov.ru/feedback/.

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

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

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 образовательной организации.

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.

Приложение 1

Акт проверки контентной фильтрации в образовательной организации

МБОУ ДО «ДЮСШ» за квартал 202 г.

1. Общие характеристики

№	Критерий	Значение критерия	Примечание
1.1	Количество компьютеров в ОО		
1.2	Количество компьютеров, имеющих выход в сеть Интернет, в т.ч.		
1.2.1	- в компьютерных классах		
1.2.2	- к которым имеется доступ обучающимся		
1.2.3	- используемых в административных целях		
1.2.4	- используемых в образовательном процессе		

2. Характеристика систем контентной фильтрации в образовательной организации

№	Критерий	Значение критерия	Примечание
2.1	Способ осуществления контент-фильтрации для сотрудников (осуществляется провайдером, осуществляется программными средствами, осуществляется аппаратными средствами)		
2.2	Название используемого контент-фильтра		
2.3	Принцип работы контент-фильтра для сотрудн (белые списки, черные списки)		
2.4	Название используемого контент-фильтра для администрации ОО		
2.5	Принцип работы контент-фильтра для администрации (белые списки, черные списки)		

3. Тестирование эффективности настройки программных средств, осуществляющих контентную фильтрацию в образовательных организациях

№	Критерий	Значение критерия	Примечание
3.1. Проверка эффективности настройки СКФ на доступность сайтов экстремистской направленности			
3.1.1.	Результат проверки по запросу списка ресурсов		
3.1.2.	Результат проверки по запросу картинок		

3.1.3.	Результат проверки ресурсов по URL-адресу		
3.2. Проверка эффективности настройки СКФ на доступность сайтов порнографического характера			
3.2.1.	Результат проверки по запросу списка ресурсов		
3.2.2.	Результат проверки по запросу картинок		
3.2.3.	Результат проверки ресурсов по URL-адресу		
3.3. Проверка эффективности настройки СКФ на доступность сайтов, содержащих информацию об алкогольной продукции, изготовлении и использовании наркотических средств, психотропных веществ, способах совершения самоубийства			
3.3.1.	Результат проверки по запросу списка ресурсов		
3.3.2.	Результат проверки по запросу картинок		
3.3.3.	Результат проверки ресурсов по URL-адресу		
3.4. Определение эффективности использования СКФ			
3.4.1.	Оценка эффективности работы СКФ в ОО (указывается в % среднее значение по п.п.3.1.1.-3.1.3, 3.2.1.-3.2.3, 3.3.1.-3.3.3		

Вывод:

Ответственный за информационную безопасность

(подпись) (Ф. И. О.)