ПРИНЯТО:
Педагогическим советом №1
Протокол №1
От 28 августа 2019 г.

УТВЕРЖДЕНО:
Заведующий
МАДОУ «Детский сад №380»
_____ Н.С. Урусова
Приказ №_____
От «29» 08 2019 г.

Порядок
проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов
в Муниципальном автономном дошкольном образовательном учреждении «Детский сад №380 комбинированного вида» Ново-Савиновского района г. Казани

1. Общие положения

1.1. Порядок проведения проверки эффективности использования системы конте фильтрации интернет-ресурсов в Муниципальном автономном дошко образовательном учреждении «Детский сад 3380 комбинированного вида» Савиновского района г. Казани (далее - Порядок) определяет процедуру проверки р системы контентной фильтрации в Муниципальном автономном дошко образовательном учреждении «Детский сад №380 комбинированного вида» Савиновского района г. Казани (далее - Учреждение).

1.2. Порядок разработан в соответствии с Федеральным законом от 29.12.2010 №4 «О защите детей от информации, причиняющей вред их здоровью и разви Методическими рекомендациями по ограничению в образовательных организ доступа обучающихся к видам информации, распространяемой посредством интернет, причиняющей вред здоровью и (или) развитию детей, а так соответствующей задачам образования, утвержденными Минкомсвязи 16.05.20 использует терминологию, которая введена ранее перечисленными правовыми актам

2. Порядок проверки системы контентной фильтрации

2.1. Проверку эффективности использования систем контентной фильтрации инт ресурсов в Учреждении проводит ответственный за информационную безопасност раза в течение учебного года.

2.2. Ответственный за информационную безопасность проверяет работоспосо системы контентной фильтрации на всех компьютерах образовательной орган путем ввода в поле поиска любого браузера ключевые слова из списка инфор запрещенной для просмотра обучающимися, с последующими попытками загрузки из найденных. В том числе, ответственный за информационную безопасность про загружается ли информация, причиняющая вред здоровью и развитию детей, не им отношения к образовательному процессу, в социальных сетях: Вконтакте, Одноклас Твиттер, Фейсбук, Инстаграм, Живой Журнал) И др.

2.3. Чтобы провести проверку, ответственный за информационную безопасность вы три-четыре ресурса с информацией, причиняющей вред здоровью и (или) развитию а также не соответствующей задачам образования, в том числе ищет информаци продукцию, запрещенную для детей, в форме сайтов, графических изобра аудиовизуальных произведений и других форм информационной продукции.

2.4. В качестве проверочных ресурсов ответственный за информационную безопа использует сайты в том числе из списка экстремистских материалов.

2.5. 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.
2.6. Если материал отображается и с ним можно ознакомиться без дополнительных условий, ответственный за информационную безопасность фиксирует факт нарушения работы системы контентной фильтрации.
2.7. 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.
2.8. Если невозможно ознакомиться с негативным контентом при выполнении дополнительных условий (регистрации, скачивания материалов, переадресации и т. д.), нарушение не фиксируется.
2.9. Ответственный за информационную безопасность составляет три-четыре запроса в поисковой строке браузера, состоящих из слов, которые могут однозначно привести на запрещенные для несовершеннолетних ресурсов, 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».
2.10. Из предложенного поисковой системой списка адресов ответственный за информационную безопасность переходит на страницу двух-трех сайтов и знакомится с полученными материалами.
2.11. Ответственный за информационную безопасность дает оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся. Если обнаруженный материал входит в перечень запрещенной для детей ответственный за информационную безопасность фиксирует факт нарушения с указанием источника и критериев оценки.
2.12. Если найденный материал нарушает законодательство Российской Федерации, то ответственный за информационную безопасность направляет сообщение о противоправном ресурсе в Роскомнадзор через электронную форму на сайте.
2.13. Ответственный за информационную безопасность проверяет работоспособность журнала, фиксирующего адреса сайтов, посещаемых с компьютеров образовательной организации.
2.14. По итогам мониторинга ответственный за информационную безопасность оформляет акт проверки контентной фильтрации в образовательной организации по форме из приложения к Порядку.
2.15. 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.
2.16. 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.

3. Заключительные положения

3.1.Срок действия Положения неограничен.
3.2.Положение может быть изменено или дополнено только принятием новой редакции Положения в полном объеме путем утверждения нового.