

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВО-ТУЗЛОВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА»
РОДИОНОВО-НЕСВЕТАЙСКОГО РАЙОНА
(МБОУ «АЛЕКСЕЕВО-ТУЗЛОВСКАЯ СОШ»)**

УТВЕРЖДЕНО
Приказом директора
МБОУ «Алексеево-Тузловская СОШ»
Приказ № 77-2 от 19.09.2019г.

**Порядок проведения проверки эффективности использования системы
контентной фильтрации Интернет-ресурсов в муниципальном бюджетном
общеобразовательном учреждении Родионово-Несветайского района
«Алексеево-Тузловская средняя общеобразовательная школа»**

1. Общие положения

1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации Интернет-ресурсов в муниципальном бюджетном общеобразовательном учреждении Родионово-Несветайского района «Алексеево-Тузловская средняя общеобразовательная школа» (далее – Порядок) определяет процедуру проверки работы системы контентной фильтрации в муниципальном бюджетном общеобразовательном учреждении Родионово-Несветайского района «Алексеево-Тузловская средняя общеобразовательная школа» (МБОУ «Алексеево-Тузловская СОШ») (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 образовательной организации проводит ответственный за информационную безопасность три раза в течение учебного 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 1 к настоящему 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.

**Акт проверки контентной фильтрации
в МБОУ « Алексеево-Тузловская СОШ»**

№ _____

_____ /
(дата)

_____ /
(номер)

1. Общие сведения

Показатель

Значение

Количество компьютерных классов
Общее количество компьютеров
Количество компьютеров в локальной сети
Количество компьютеров, подключенных к сети
Интернет
Провайдер
Скорость передачи данных

2. Информация о контент-фильтре

**Действия, необходимые для обеспечения контентной
фильтрации Интернет-ресурсов**

**Выполнение
да/нет**

Установление контент-фильтра
Название контент-фильтра
Контент-фильтр работает на всех компьютерах, где есть
доступ к сети Интернет

3. Результаты проверки работы системы контентной фильтрации

**Категории запрещенной информации в
образовательной организации**

**Возможность
доступа (да/нет)**

Перечень видов информации, запрещенной к
распространению посредством сети интернет,
причиняющей вред здоровью и (или) развитию детей, а
также не соответствующей задачам образования согласно
Методическим рекомендации по ограничению в
образовательных организациях доступа обучающихся к
Документ подписан электронной подписью. видам
информации, распространяемой посредством сети
интернет, причиняющей вред здоровью и (или) развитию
детей, а также не соответствующей задачам образования
Интернет-ресурсы, не включенные в Реестр безопасных
образовательных сайтов

Ответственный за информационную безопасность: _____ / _____ /
(подпись) (Ф.И.О.)

С актом ознакомлен:

Директор: _____ / _____ /
(подпись) (Ф.И.О.)

