

**Частное дошкольное образовательное учреждение  
«Детский сад № 198 открытого акционерного общества  
«Российские железные дороги»**

**Рассмотрено**

Протокол педагогического совета  
от 31.08.2020 № 1

**Утверждено**

Заведующим ЧДОУ  
«Детский сад № 198 ОАО «РЖД»  
\_\_\_\_\_ Н.А. Овчинникова

Приказ № 204 от 31.08.2020

**Порядок  
проведения проверки эффективности использования  
(системы контентной фильтрации) СКФ интернет-ресурсов в  
частном дошкольном образовательном учреждении  
«Детский сад № 198 открытого акционерного общества  
«Российские железные дороги»**

**1. Общее положение**

1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации (далее – СКФ) интернет-ресурсов в частном дошкольном образовательном учреждении «Детский сад № 198 открытого акционерного общества «Российские железные дороги» (далее - Порядок) определяет процедуру проверки работы системы контентной фильтрации в частном дошкольном образовательном учреждении «Детский сад № 198 открытого акционерного общества «Российские железные дороги» города Красноярска (далее – Учреждение).

1.2. Порядок разработан в соответствии с Федеральным законом от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и (или) развитию», Методических рекомендаций по ограничению в образовательных организациях доступа к видам информации, распространяемой посредством сети интернет, причиняющей вред здоровью и (или) развитию детей, а также несоответствующей задачам образования, утвержденных Минкомсвязи 16.05.2019 г.

**2. Порядок СКФ**

2.1. Проверку эффективности использования СКФ интернет-ресурсов в Учреждении проводит ответственный за информационную безопасность три раза в течение учебного года.

2.2. Ответственный за информационную безопасность проверяет работоспособность СКФ на всех компьютерах образовательной организации

путем ввода в поле поиска любого браузера ключевые слова из списка информации, запрещенной для просмотра обучающими, 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: В контакте, 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.

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 СКФ.

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 СКФ.

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 ресурсы, на пример по темам: экстремизм, проявление жестокости, терроризм, суицид и т.д.

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 информации (Приложение N 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.

2.12. Если найденный материал нарушает законодательство РФ, то ответственный за информационную безопасность направляет сообщение о противоправном ресурсе в Роскомнадзор через электронную форму на сайте. <http://eais.rkn.gov.ru/feedback/>.

2.13. 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.