

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ШКОЛА-ИНТЕРНАТ С ПРЕДОСТАВЛЕНИЕМ ДОШКОЛЬНОГО ОБРАЗОВАНИЯ
ГОРОДСКОГО ОКРУГА ГОРЛОВКА» ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

(ГБОУ «ШИДО г. о. Горловка»)

РАССМОТРЕНО
на заседании педагогического
совета ГБОУ «ШИДО г.о.
Горловка»

Протокол № 18
от « 27 » 12 2024 г.

УТВЕРЖДЕНО
приказом директора
ГБОУ «ШИДО г.о. Горловка»



от « 28 » декабря 2024 г. № 402

**ПОРЯДОК ПРОВЕДЕНИЯ ПРОВЕРКИ ЭФФЕКТИВНОСТИ
ИСПОЛЬЗОВАНИЯ СИСТЕМЫ КОНТЕНТНОЙ ФИЛЬТРАЦИИ
ИНТЕРНЕТ-РЕСУРСОВ
ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ
«ШКОЛА – ИНТЕРНАТ С ПРЕДОСТАВЛЕНИЕМ ДОШКОЛЬНОГО
ОБРАЗОВАНИЯ ГОРОДСКОГО ОКРУГА ГОРЛОВКА»
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ**

Горловка, 2024

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов в ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБЩЕОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ «ШКОЛА – ИНТЕРНАТ С ПРЕДОСТАВЛЕНИЕМ ДОШКОЛЬНОГО ОБРАЗОВАНИЯ ГОРОДСКОГО ОКРУГА ГОРЛОВКА» ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ (далее учреждение) определяет процедуру проверки работы системы контентной фильтрации.

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 учреждении проводит ответственный за информационную безопасность два раза в течение учебного года.

2.2. Ответственный за информационную безопасность проверяет работоспособность системы контентной фильтрации на всех компьютерах учреждения 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, 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 учреждения.

2.8. По итогам мониторинга ответственный за информационную безопасность оформляет акт проверки контентной фильтрации в учреждения 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 учреждения.

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 об эффективной (неэффективной) работе контентной фильтрации

(наименование образовательной организации (полностью))

1. Общие сведения:

- количество компьютерных классов – _____
- количество компьютеров в ОО – _____
- количество компьютеров в локальной сети – _____
- количество компьютеров, подключенных к сети Интернет – _____
- провайдер, предоставляющий доступ в сеть Интернет, номер и дата заключения договора – _____
- скорость передачи данных (как прописано в договоре) – _____

2. Контент-фильтр:

Действия, необходимые для обеспечения контентной фильтрации интернет-ресурсов	да/нет
Установлен контент-фильтр	
Название контент-фильтра	
Контент-фильтр работает на всех компьютерах, к которым есть доступ учащихся и подключенных к сети Интернет	

3. Результаты проверки работы системы контентной фильтрации

Наименования запросов	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 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	
Интернет-ресурсы, не включенные в Реестр безопасных образовательных сайтов	

Ответственный за информационную безопасность:

подпись

Ф.И.О.

С актом ознакомлен: _____

подпись

Ф.И.О.

дата

Директор