Муниципальное бюджетное учреждение дополнительного образования «ЦЕНТР ВНЕШКОЛЬНОЙ РАБОТЫ»

ПРИКАЗ

от 09 октября 2019 года № 352 - о

«Об информационной безопасности в МБУ ДО «Центр внешкольной работы»

В целях осуществления ограничения доступа обучающихся к ресурсам и материалам сети Интернет, не имеющих отношения к образовательному процессу, **приказываю:**

1. Назначить ответственным за обеспечение безопасного доступа к сети «Интернет» в учреждении Меньшакова Владимира Васильевича, электроника муниципального бюджетного учреждения дополнительного образования «Центр внешкольной работы» (далее- МБУ ДО ЦВР).
2. Утвердить:

2.1. Акт об эффективной (неэффективной) работе контентной фильтрации (Приложение 1).

2.2. Порядок проведения проверки эффективности использования систем контентной фильтрации Интернет-ресурсов в МБУ ДО ЦВР (Приложение 2).

3. Специалисту по кадрам А.В. Сильнягиной внести соответствующие изменения в должностную инструкцию электроника В.В. Меньшакова.
4. Секретарю К.А. Тариковой ознакомить сотрудников учреждения с данным приказом и его приложениями.
5. Контроль за выполнением приказа оставляю за собой.

Директор И.В. Семенов

Приложение №1

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:

	да/нет
Наличие технических средств контентной фильтрации	
Выполнены установки контент-фильтра, блокирующего выход к интернет-ресурсам, не совместимым с целями образования и воспитания	
Наличие в договоре с провайдером пункта о предоставлении услуг по контентной фильтрации – «черные» и «белые» списки	
Вручную и автоматически запрещены выходы на сайты общественных и религиозных объединений, иных некоммерческих организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом «О противодействии экстремисткой деятельности» (http://minjust.ru/nko/fedspisok)	
Контент-фильтр работает на всех компьютерах, к которым есть доступ учащихся и подключенных к сети Интернет	

2.1. Название технических средств контентной фильтрации – указать название.

2.2. Способ осуществления контентной фильтрации - установлен на каждом компьютере (ноутбуке), используемом в учебной деятельности.

3. Нормативная документация образовательной организации по проведению организационных мер по ограничению доступа в сеть Интернет:

	да/нет	реквизиты утвержденного документа (дата и номер)
Наличие положения о Совете ОО по вопросам регламентации доступа к информации в Интернете		
Наличие положения об ответственных лицах за функционирование средств контентной фильтрации доступа к сети Интернет в образовательной организации		
Наличие правил использования сети Интернет в образовательной организации		
Наличие порядка действий для сотрудников ОО и членов Совета при осуществлении контроля за использованием учащимися сети Интернет		
Наличие классификатора информации, не имеющей отношения к образовательному процессу		
Назначение ответственного за организацию работы с ресурсами сети Интернет и ограничение доступа		

4. Результаты проверки работы системы контентной фильтрации:

Все виды информации, перечисленной в приложении «Перечень видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования» Методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет, разработанных Министерством образования и науки РФ,

_____ (*доступны, недоступны*) обучающимся в процессе учебной деятельности.

При проверке были использованы следующие запросы в поисковых системах (Yandex.ru, Mail.ru и т.д. указать каких):

- запрос _____ наличие доступа: (*да/нет*) _____
- запрос _____ наличие доступа: (*да/нет*) _____
- запрос _____ наличие доступа: (*да/нет*) _____
- запрос _____ наличие доступа: (*да/нет*) _____

Дата составления акта _____

Члены комиссии по проведению проверки образовательной организации по контентной фильтрации:

ФИО, должность _____ подпись _____

ФИО, должность _____ подпись _____

ФИО, должность _____ подпись _____

ФИО, должность _____ подпись _____

М.П.

Приложение № 2

Порядок проведения проверки эффективности использования
систем контентной фильтрации Интернет-ресурсов
в образовательных организациях

1. В организации приказом руководителя образовательной организации должна быть создана комиссия по проверке эффективной работоспособности школьной системы контентной фильтрации (не менее 4-х человек вместе с председателем).

2. Выбрать 3-4 материала, содержание которых может причинить вред здоровью и развитию обучающихся (Федеральный список экстремистских материалов - http://minjust.ru/nko/fedspisok). Проверить конкретный сайт можно в едином реестре доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено - http://zapret-info.gov.ru/, http://eais.rkn.gov.ru/.

3. Внести название материала (части материала, адрес сайта) в поисковую систему.

4. Из предложенного поисковой системой списка адресов перейти на страницу сайта, содержащего противоправный контент. Если материал отображается и с ним можно ознакомиться без дополнительных условий – фиксируется факт нарушения работы системы контентной фильтрации.

5. При дополнительных условиях (требуется регистрация, условное скачивание, переадресация и т.д.), при выполнении которых материал отображается, также фиксируется факт нарушения работы системы контентной фильтрации. При невозможности ознакомления с противоправным контентом при выполнении условий (регистрация, скачивание материалов, переадресаций и т.д.) нарушение не фиксируется.

6. Выбрать 3-4 противоправных материала по определенной теме (экстремизм, проявление жестокости, порнография, терроризм, суицид, насилие и т.д.).

7. Запросить через поисковую систему материал по заданной теме (Например: «изготовление зажигательной бомбы», «издевательства над несовершеннолетними», «способы суицида» и т.д.).

8. Из предложенного поисковой системой списка адресов перейти на страницу 2-3 сайтов и ознакомиться с полученными материалами.

9. Дать оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающимся.

10. При признании материала условно противоправным – зафиксировать факт нарушения с указанием источника и мотивов оценки, а также направить адрес материала на проверку в единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено - http://zapret-info.gov.ru/, http://eais.rkn.gov.ru/.

11. Комиссия должна проверить работоспособность системы контент-фильтрации на всех компьютерах образовательной организации путем ввода в поле поиска любой поисковой системы ключевых слов из списка информации, запрещенной для просмотра учащимися, с последующими попытками загрузки сайтов из найденных. ***Необходимо, в том числе, проверить загружается ли информация, причиняющая вред здоровью и развитию детей, не имеющая отношения к образовательному процессу, в социальных сетях: «В контакте», «Одноклассники», twitter.com, facebook.com, Живой Журнал livejournal.com и т.д.***

Замечание:

Если учреждение не использует перечисленные выше ресурсы в образовательных целях, то доступ к ним необходимо отключить.

12. Комиссия должна проверить работоспособность журнала, фиксирующего адреса сайтов, посещаемых с компьютеров школы.

13. По итогам мониторинга сформировать заключение (акт) об эффективной (неэффективной) работе контентной фильтрации. При неэффективной работе контент-фильтра, в п.4 приложения №1 необходимо указать выявленные проблемы, пути их решения и сроки исправления.

14. При выявлении компьютеров, подключенных к сети Интернет и не имеющих СКФ, производятся одно из следующих действий:

- немедленная установка и настройка СКФ,
- немедленное программное и/или физическое отключение доступа к сети Интернет на выявленных компьютерах.