БЮДЖЕТНОЕ УЧРЕЖДЕИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА-ЮГРЫ
«ЛАНГЕПАССКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

УТВЕРЖДАЮ
Директор
_____ Н.В. Горбунова
Приказ № 68-12
«12» 08 2024 г.

ПОРЯДОК ПРОВЕДЕНИЯ ПРОВЕРКИ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ КОНТЕНТНОЙ ФИЛЬТРАЦИИ ИНТЕРНЕТ-РЕСУРСОВ В БУ «ЛАНГЕПАССКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

Лангепас

1. Общие положения

1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов (далее – Порядок) определяет процедуру проверки работы системы контентной фильтрации в БУ «Лангепасский политехнический колледж» (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 проводят члены Комиссии по контентной фильтрации под руководством ответственного за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации ежегодно до 30 августа, а также в конце каждого квартала.

2.2. Ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации формирует каталог ссылок из Реестра запрещенных сайтов, опубликованных на сайте Роскомнадзора https://www.ruzapret.com/, включая ссылки из списка экстремистских материалов – http://minjust.ru/nko/fedspisok.

Каталог ссылок – это документ Word, содержащий гиперссылки на указанные сайты. Члены комиссии проверяют работоспособность системы контентной фильтрации на всех компьютерах образовательной организации путем клика по гиперссылкам в каталоге. Затем путем ввода в поле поиска любого браузера проверяют ответ поисковика на ключевые слова из списка информации, запрещенной для просмотра обучающимися, с последующими попытками загрузки сайтов из результатов поиска.

Следующим этапом члены комиссии проверяют, загружается ли информация, причиняющая вред здоровью и развитию детей, не имеющая отношения к образовательному процессу, в социальные сети ВКонтакте, Одноклассники, Твиттер и др.

2.3. Если в результате проверки запрещенный материал отображается и с ним можно ознакомиться без дополнительных условий, секретарь Комиссии по контентной фильтрации фиксирует факт нарушения работы системы контентной фильтрации.

2.4. Если ресурс требует дополнительных действий (регистрации, условного скачивания, переадресации и т. д.), при выполнении которых материал отображается, ответственный за информационную безопасность и

обеспечение безопасного доступа к сети Интернет в образовательной организации также фиксирует факт нарушения работы системы контентной фильтрации.

2.5. Если невозможно ознакомиться с негативным контентом при выполнении дополнительных условий (регистрации, скачивания материалов, переадресации и т. д.), нарушение не фиксируется.

2.6. Ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации 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».

2.6.1. Из предложенного поисковой системой списка адресов ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации переходит на страницу двух–трех сайтов и знакомится с полученными материалами.

2.6.2. Ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации дает оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся.

2.6.3. 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), секретарь Комиссии по контентной фильтрации фиксирует факт нарушения с указанием источника и критериев оценки.

2.7. Если найденный материал нарушает законодательство Российской Федерации, то ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет в образовательной организации направляет сообщение о противоправном ресурсе в Роскомнадзор через электронную форму на сайте http://eais.rkn.gov.ru/feedback/.

2.8. Ответственный за информационную безопасность и обеспечение безопасного доступа к сети Интернет проверяет работоспособность журнала, фиксирующего адреса сайтов, посещаемых с компьютеров образовательной организации.

2.9. По итогам мониторинга секретарь Комиссии по контентной фильтрации заполняет акт проверки контентной фильтрации в образовательной организации по форме из приложения к Порядку.

2.9. Если в процессе проверки выявлены сайты, которые не входят в Реестр безопасных образовательных сайтов, а также в Белый список сайтов,

сформированный преподавателями колледжа, то их перечисляют 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.