

РОССИЙСКАЯ ФЕДЕРАЦИЯ
АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ПРИОЗЕРСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН ЛЕНИНГРАДСКОЙ ОБЛАСТИ

КОМИТЕТ ОБРАЗОВАНИЯ

ПРИКАЗ

от 29.07.2014 года

г. Приозерск

№ 201

Об утверждении методических
рекомендаций по организации системы
контентной фильтрации в
образовательных организациях
муниципального образования
Приозерский муниципальный район
Ленинградской области

В соответствии с требованиями Федерального закона от 29.12.2010 № 436-ФЗ (ред. от 02.07.2013) "О защите детей от информации, причиняющей вред их здоровью и (или) развитию", в целях исключения доступа обучающихся образовательных организаций к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания учащихся, в соответствии с Федеральным законом "Об образовании в Российской Федерации" от 29 декабря 2012 г. № 273-ФЗ, на основании приказа комитета образования МО Приозерский муниципальный район № 198 от 25.07.2014 г. «Об организационных мерах, обеспечивающих исключение доступа обучающихся образовательных организаций к ресурсам сети Интернет, содержащим информацию, причиняющую вред здоровью и (или) развитию детей»,

ПРИКАЗЫВАЮ:

1. Утвердить методические рекомендации по организации системы контентной фильтрации в образовательных организациях муниципального образования Приозерский муниципальный район Ленинградской области.
2. Контроль за исполнением данного приказа возложить на заместителя председателя комитета образования Кравченко И.И.

Председатель комитета образования

Г.Ф. Тысячная

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по организации системы контентной фильтрации
в образовательных организациях муниципального образования
Приозерский муниципальный район
Ленинградской области**

Согласно пункту 4 статьи 29 Конституции Российской Федерации каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Ограничения прав на свободное получение информации, способной принести вред детям, их здоровью и развитию установлены Федеральным законом от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в редакции Федерального закона от 28.07.2012 г. № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации».

Решение задач по ограничению доступа к ресурсам сети Интернет, не совместимых с образовательным процессом и способным причинить вред здоровью и развитию детей, путем организации системы контентной фильтрации возлагается, в первую очередь, на образовательные организации, как на основной уровень практического осуществления мероприятий по ограничению доступа обучающихся к запрещенным ресурсам сети Интернет.

Правовой базой для организации системы контентной фильтрации в общеобразовательных организациях муниципального образования Приозерский муниципальный район Ленинградской области являются:

1. Федеральный закон от 29.12.2010г. №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в редакции Федерального закона от 28.07.2012 г. № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные Законодательные акты Российской Федерации»;
2. Федеральный закон от 24.07.1998 г. №124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
3. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет Министерства образования и науки Российской Федерации от 11.05.2011г.;
5. Приказ Минобрнауки РД от 02 сентября 2013 г. № 2553 «О мерах по исключению доступа к интернет-ресурсам, не совместимым с задачами образования и воспитания обучающихся».

Категории запрещенной информации для распространения среди детей:

- информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- информация, способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и

спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

- информация, обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

- информация, отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

- информация, оправдывающая противоправное поведение;

- информация, содержащая нецензурную брань;

- информация, содержащая информацию порнографического характера.

- информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

- информация, вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

- информация, представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

- информация, содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Система контентной фильтрации (СКФ) - это программный комплекс, основными задачами которого являются управление доступом учащихся к ресурсам сети Интернет, ограничения доступа к интернет - ресурсам, содержание которых несовместимо с задачами воспитания и образования, и мониторинг использования интернет - ресурсов.

Системы контентной фильтрации, используемые в общеобразовательных организациях должны отвечать **следующим требованиям:**

1. Обеспечивать беспрепятственный доступ к информации, распространение к которой в Российской Федерации в соответствии с законодательством Российской Федерации не ограничивается или не запрещается;

2. Обеспечить мониторинг использования интернет ресурсов в образовательном процессе в целях обучения и воспитания учащихся;

3. Обеспечить возможность адаптации к изменяющимся угрозам, условиям эксплуатации, требованиям законодательства Российской Федерации, предписаниям надзорных органов;

4. Обеспечить фильтрацию контента по спискам категорий, рекомендованным Министерством образования и науки Российской Федерации России и размещенным в сети Интернет на сайте Единой системы контент фильтрации доступа к сети Интернет по адресу: <http://www.skf.edu.ru>.

Для подключения к единой системе контент-фильтрации доступа к сети Интернет общеобразовательные организации используют системы контентной фильтрации, рекомендованные Министерством образования и науки Российской Федерации, заключив договор с провайдером, либо системы контентной фильтрации приобретаются самостоятельно.

Сравнительный анализ программных продуктов, осуществляющих контент-фильтрацию на их соответствие с Правилами подключения общеобразовательных организаций к Единой системе контент-фильтрации доступа к сети Интернет, реализованных Министерством образования и науки Российской Федерации:

Характеристики	Internet Censor	NetPolice pro	Content Keeper	KidGid	ChildWebG uardian
-----------------------	----------------------------	--------------------------	---------------------------	---------------	------------------------------

Обеспечивать беспрепятственный доступ к информации, распространение к которой в Российской Федерации в соответствии с законодательством Российской Федерации не ограничивается или не запрещается	+	+	+	+	+
Обеспечить возможность адаптации к изменяющимся угрозам, условиями эксплуатации, требованиям законодательства Российской Федерации предписаниям надзорных органов	+	+	+	+	+
Обеспечить фильтрацию контента по спискам категорий, рекомендованным Министерством образования и науки Российской Федерации и размещенным в сети Интернет на сайте единой системы контент фильтрации доступа к сети Интернет по адресу http://www.skf.edu.ru	+	+	+	-	+
Обеспечить мониторинг использования интернет ресурсов в образовательном процессе в целях обучения и воспитания учащихся	+	+	-	-	+
Возможность установки на каждый компьютер	+	+	+	+	+
Интерфейс (язык)	русский	русский	русский	русский	русский
Операционная система	Windows XP, Linux	Windows XP, Vista, Linux	Windows 7, XP, Vista, Linux	Windows XP, Vista, Linux	Windows 7, XP, Vista, Linux
Сайт программы	http://icenter.ru/	http://www.netpolice.ru	www.contentkeeper.com	http://www.kidgid.com/	http://www.childwebguardian.ru/

Сравнительный анализ DNS-фильтров:

Показатель	SkyDNS	Rejector	OpenDNS
Явная блокировка сайтов, запрещенных законодательством РФ	+	+	+
Безопасный поиск с защитой от экстремизма, порнографии, наркотиков	+	+	+
Принудительное перенаправление всех поисковых систем на безопасный поиск	+	+	+
Блокировка неизвестных сайтов	+	+	+
Режим работы только по белому списку	+	+	+

Обязательно наличие	+	+	+
Централизованное управление	+	+	+
Режим защиты всей сети и отдельных компьютеров	+	+	+
Операционная система	Windows 7, XP, Vista, Linux	Windows 7, XP, Vista	Windows 7, XP, Vista, Linux
Стоимость	платный	бесплатный	бесплатный
Интерфейс (язык)	русский	русский	русский
Сайт программы	https://www.skydns.ru/	http://rejector.ru/	http://www.opendns.com/

Установка программного обеспечения ограничения доступа должна производиться на всё компьютерное оборудование общеобразовательных организаций, имеющих доступ к сети Интернет.

Помимо установки и настройки системы контентной фильтрации в образовательных организациях должен реализовываться комплекс мер по обеспечению безопасного доступа обучающихся образовательных организаций к ресурсам сети Интернет:

1. В образовательной организации приказом руководителя должен быть назначен ответственный за доступ к сети Интернет и организацию контентной фильтрации. В качестве ответственного за организацию доступа к сети Интернет может быть назначен заместитель руководителя образовательной организации по учебно-воспитательной работе, заместитель руководителя образовательной организации по информатизации, преподаватель информатики, другой сотрудник образовательной организации.

В учреждении приказом руководителя образовательной организации должны быть приняты и введены в действие:

- Положение о совете образовательной организации по вопросам регламентации доступа к информации в сети Интернет (приложении № 1).
- Классификаторы информации, не имеющей отношения к образовательному процессу. (Он обязательно должен содержать перечень из Классификатора информации, распространение которой запрещено в соответствии с законодательством Российской Федерации - Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".)
Рекомендации по разработке и применению системы классификации информации, не имеющей отношения к образовательному процессу, приведены в приложении № 2.
- Регламент по созданию и организации точки доступа к сети Интернет в образовательной организации (приложение № 3).
- Регламент образовательной организации по работе с электронной почтой (приложение № 4).
- Инструкция по организации антивирусной защиты компьютерной техники в образовательных организациях (приложение № 5).
- Правила использования сети Интернет в образовательных организациях (приложение № 6).

- Инструкция для сотрудников образовательных организаций о порядке действий при осуществлении контроля использования обучающимися сети Интернет (приложение № 7).
- Должностная инструкция сотрудника образовательной организации, ответственного за использование преподавателями и обучающимися доступа к сети Интернет (приложение № 8).
- Инструкция пользователя по компьютерной безопасности (приложение № 9).
- Инструкция по осуществлению мониторинга эффективности работы системы контентной фильтрации в образовательных организациях (приложение 10).

2. В учреждении должен быть создан Совет по вопросам регламентации доступа к информации в сети Интернет.

3. В должностные инструкции отдельных работников образовательной организации должны быть внесены изменения по использованию сети Интернет работником.

4. В образовательных организациях должны вестись журналы проверок антивирусной защиты и контроля за контентной фильтрацией.

5. Должен регулярно осуществляться контроль использования учащимися сети Интернет с помощью программно-технических средств и визуального контроля. С этой целью также рекомендуется создание комиссии по проверке работоспособности школьной системы контент-фильтрации (не менее 4-х человек вместе с председателем).

Комиссия должна проверить работоспособность системы контент-фильтрации на всех компьютерах учреждения 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 и т.д.

**ПРИМЕРНОЕ ПОЛОЖЕНИЕ
о совете образовательной организации по вопросам регламентации
доступа к информации в сети Интернет.**

1. В соответствии с настоящим Положением о Совете по вопросам образовательной организации по вопросам регламентации доступа к информации в сети Интернет. (далее — Совет) целью создания Совета является обеспечение разработки и принятия мер по ограничению доступа обучающихся к ресурсам сети Интернет, содержащим информацию, не совместимую с целями воспитания и образования обучающихся.

2. Задачами Совета являются:

- обобщение опыта работы общеобразовательной организации, разработка предложений по совершенствованию данной работы;
- разработка предложений по учету основных социокультурных особенностей конкретной организации при формировании легальных механизмов ограничения доступа обучающихся к информации, не имеющей отношения к образовательному процессу;
- разработка предложений, позволяющих на уровне общеобразовательной организации решать вопросы регулирования доступа обучающихся к некоторым видам ресурсов с учетом социокультурных особенностей данного региона Российской Федерации;
- подготовка предложений по совершенствованию применения классификатора информации, доступ к которой обучающихся общеобразовательной организации должен быть ограничен.

3. Совет создается при образовательной организации и является независимым экспертно-консультативным органом.

4. Совет создается из педагогических работников, представителей родительской общественности и ученического самоуправления.

5. Очередные собрания Совета проводятся с периодичностью, установленной Советом.

6. Принятие решений по вопросам политики доступа к ресурсам/группам ресурсов сети Интернет осуществляется Советом самостоятельно либо с привлечением экспертов, в качестве которых могут выступать:

- преподаватели школы и других образовательных учреждений;
- лица, имеющие специальные знания, либо опыт работы в соответствующих областях;
- представители систем информационно-методических центров;
- представители органов местного самоуправления, осуществляющих управление в сфере образования;

7. При принятии решений Совет и эксперты должны руководствоваться:

- законодательством Российской Федерации;
- целями региональных и муниципальных программ развития образования;
- специальными познаниями, в том числе полученными в результате профессиональной деятельности по рассматриваемой тематике;
- интересами обучающихся, целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

РЕКОМЕНДАЦИИ
по разработке и применению системы классификации информации,
не имеющей отношения к образовательному процессу

1. Классификатор информации, запрещенной законодательством Российской Федерации к распространению, применяется в единообразном виде на всей территории Российской Федерации.

2. Классификатор информации, не имеющей отношения к образовательному процессу, может содержать как части (разделы), рекомендуемые к применению в единообразном виде на всей территории Российской Федерации, так и части (разделы), рекомендуемые к использованию экспертно-консультативными органами (советами) регионального и (или) муниципального уровня.

3. Экспертно-консультативные органы (советы), создаваемые при органах управления образованием различных уровней, являются независимыми органами.

4. В соответствии с законодательством Российской Федерации образовательное учреждение свободно в выборе и применении классификаторов информации, не имеющей отношения к образовательному процессу, а также несет ответственность за невыполнение функций, отнесенных к его компетенции.

Рекомендации по формированию Классификатора информации, распространение которой запрещено в соответствии с законодательством Российской Федерации, разработаны в соответствии с проведенным анализом законодательства Российской Федерации и международных договоров Российской Федерации.

№	Тематическая категория	Содержание
1	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	<ul style="list-style-type: none">• Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды;• информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение
2	Злоупотребление свободой СМИ — экстремизм	Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы
3	Злоупотребление свободой СМИ — наркотические средства	Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
4	Злоупотребление свободой СМИ — информация с ограниченным доступом	Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций
5	Злоупотребление свободой СМИ — скрытое воздействие	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская деятельность	А) Экстремистские материалы, то есть предназначенные для обнародования документы или информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие

№	Тематическая категория	Содержание
	(экстремизм)	<p>необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии; публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы;</p> <p>Б) экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков:</p> <ul style="list-style-type: none"> • насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; • подрыв безопасности Российской Федерации, захват или присвоение властных полномочий, создание незаконных вооруженных формирований; • осуществление террористической деятельности либо публичное оправдание терроризма; • возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию; • унижение национального достоинства; • осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; • пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности; • воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения; • публичная клевета в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, сопровождаемая обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке; • применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; • посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения

№	Тематическая категория	Содержание
		его государственной или иной политической деятельности либо из мести за такую деятельность; <ul style="list-style-type: none"> • нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением
7	Вредоносные программы	Программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети
8	Преступления	<ul style="list-style-type: none"> • Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию); • оскорбление (унижение чести и достоинства другого лица, выраженное в неприличной форме); • публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма; • склонение к потреблению наркотических средств и психотропных веществ; • незаконное распространение или рекламирование порнографических материалов; • публичные призывы к осуществлению экстремистской деятельности; • информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также социального, расового, национального и религиозного неравенства; • публичные призывы к развязыванию агрессивной войны
9	Ненадлежащая реклама	Информация, содержащая рекламу алкогольной продукции и табачных изделий
10	Информация с ограниченным доступом	Информация, составляющая государственную, коммерческую, служебную или иную охраняемую законом тайну

Приводимый далее перечень категорий Классификатора информации, не имеющей отношения к образовательному процессу, носит рекомендательный характер и может быть дополнен, расширен или иным образом изменен в установленном порядке, в том числе с учетом специфики образовательного учреждения, социокультурных особенностей конкретного региона и иных обстоятельств.

№	Тематическая категория	Содержание
1	Алкоголь	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию
2	Баннеры и рекламные программы	Баннерные сети, всплывающая реклама, рекламные программы
3	Вождение и автомобили (ресурсы данной категории, не имеющие отношения к	Не имеющая отношения к образовательному процессу информация об автомобилях и других транспортных средствах, вождении, автозапчастях,

№	Тематическая категория	Содержание
	образовательному процессу)	автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям
4	Досуг и развлечения (ресурсы данной категории, не имеющие отношения к образовательному процессу)	<p>Не имеющая отношения к образовательному процессу информация:</p> <ul style="list-style-type: none"> • фотоальбомы и фотоконкурсы; • рейтинги открыток, гороскопов, сонников; • гадания, магия и астрология; • ТВ-программы; • прогнозы погоды; • тесты, конкурсы онлайн; • туризм, путешествия; • тосты, поздравления; • кроссворды, сканворды, ответы к ним; • фантастика; • кулинария, рецепты, диеты; • мода, одежда, обувь, модные аксессуары, показы мод; • тексты песен, кино, киноактеры, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.; • о дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними; • о рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании; • о службах знакомств, размещении объявлений онлайн; • анекдоты, «приколы», слухи; • о сайтах и журналах для женщин и для мужчин; • желтая пресса, онлайн-ТВ, онлайн-радио; • о знаменитостях; • о косметике, парфюмерии, прическах, ювелирных украшениях.
5	Здоровье и медицина (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иные материалы на тему «Здоровье и медицина», которые, являясь академическими, по сути, могут быть также отнесены к другим категориям (порнография, трупы и т.п.)
6	Компьютерные игры (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу компьютерные онлайн-овые и оффлайн-овые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты
7	Корпоративные сайты, интернет-представительства негосударственных учреждений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций
8	Личная и немодерируемая	Немодерируемые форумы, доски объявлений и

№	Тематическая категория	Содержание
	информация	конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги
9	Отправка SMS с использованием интернет-ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
10	Модерируемые доски объявлений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты
11	Нелегальная помощь школьникам и студентам	Банки готовых рефератов, эссе, дипломных работ и пр.
12	Неприличный и грубый юмор	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека
13	Нижнее белье, купальники	Сайты, на которых рекламируется и изображается нижнее белье и купальники
14	Обеспечение анонимности пользователя, обход контентных фильтров	Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам; Peer-to-Peer программы, сервисы бесплатных прокси-серверов, сервисы, дающие пользователю анонимность
15	Онлайн-казино и тотализаторы	Электронные казино, тотализаторы, игры на деньги, конкурсы и пр.
16	Платные сайты	Сайты, на которых вывешено объявление о платности посещения веб-страниц
17	Поиск работы, резюме, вакансии (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-представительства кадровых агентств, банки вакансий и резюме
18	Поисковые системы (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-каталоги, системы поиска и навигации в Интернете
19	Религии и атеизм (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Сайты, содержащие, не имеющую отношения к образовательному процессу, информацию религиозной и антирелигиозной направленности.
20	Системы поиска изображений	Системы для поиска изображений в Интернете по ключевому слову или словосочетанию
21	СМИ (ресурсы данной категории, не имеющие отношения к образовательному процессу)	СМИ, содержащие новостные ресурсы и сайты СМИ (радио, телевидения, печати), не имеющие отношения к образовательному процессу.
22	Табак, реклама табака, пропаганда потребления табака	Сайты, пропагандирующие потребление табака; реклама табака и изделий из него
23	Торговля и реклама (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие, не имеющие отношения к образовательному процессу, сайты следующих категорий: аукционы, распродажи онлайн, интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги,

№	Тематическая категория	Содержание
		иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости, покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в Интернете, e-бизнес
24	Убийства, насилие	Сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.
25	Чаты (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу сайты для анонимного общения в режиме онлайн.

ТИПОВОЙ РЕГЛАМЕНТ

по созданию и организации точки доступа к сети Интернет в образовательных организациях муниципального образования Приозерский муниципальный район Ленинградской области

Данный регламент определяет порядок пользования Интернетом в образовательных организациях муниципального образования Приозерский муниципальный район Ленинградской области.

Точка доступа к информационным Интернет ресурсам в образовательной организации создаётся в рамках реализации национального проекта «Образование». Пользователями точки доступа к сети Интернет являются преподаватели, обучающиеся и сотрудники образовательного учреждения. Пользователи точки доступа могут бесплатно пользоваться доступом к Интернету, искать необходимую информацию, размещать собственную. Также они могут получать консультации по вопросам, связанным с использованием сети Интернет.

К работе в сети Интернет допускаются лица, прошедшие регистрацию и обязавшиеся соблюдать условия работы.

Права, обязанности и ответственность пользователей:

Пользователи точки доступа к сети Интернет в образовательной организации имеют **право:**

- Работать в сети Интернет в течение одного часа в день. При необходимости время работы может быть увеличено по согласованию с сотрудником образовательной организации, ответственного за использование доступа к сети Интернет и при отсутствии иных лиц, желающих воспользоваться доступом к Интернет-ресурсам.
- Сохранять полученную информацию на съемном диске (дискете, СВ-КОМ, флеш-накопителе). Съемные диски должны предварительно проверяться на наличие вирусов. При необходимости пользователь может напечатать полученную информацию на принтере (по согласованию с администрацией образовательной организации).

Пользователю точки доступа к сети Интернет в образовательной организации **запрещается:**

- Осуществлять действия, не предусмотренные законодательством РФ.
- Посещать сайты, содержащие порнографическую и антигосударственную информацию, информацию со сценами насилия, участвовать в нетематических чатах.
- Передавать информацию, представляющую коммерческую или иную тайну, распространять информацию, порочащую честь и достоинство граждан.
- Устанавливать на компьютерах дополнительное программное обеспечение, как полученное в Интернете, так и любое другое.
- Изменять конфигурацию параметров, в том числе менять системные настройки компьютера и всех программ, установленных на нем (заставки, картинку рабочего стола, стартовой страницы браузера).
- Включать и выключать компьютер без согласования с сотрудником образовательной организации, ответственным за использование доступа к сети Интернет.
- Осуществлять действия, направленные на «взлом» любых компьютеров,

находящихся как в точке доступа к сети Интернет образовательной организации, так и за его пределами.

- Использовать возможности точки доступа к сети Интернет образовательной организации для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации.

Пользователи точки доступа к сети Интернет в образовательном учреждении несут **ответственность:**

- За содержание передаваемой, принимаемой и печатаемой информации.
- Пользователи должны соблюдать тишину, порядок и чистоту в точке доступа к сети Интернет, а также выполнять указания сотрудника образовательной организации, ответственного за использование доступа к сети Интернет по первому требованию.
- Лица, не соблюдающие настоящий регламент работ, лишаются права работы в точке доступа к сети Интернет.
- При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.

ТИПОВОЙ РЕГЛАМЕНТ образовательной организации по работе с электронной почтой

1. Общие положения:

- 1.1. Электронная почта в образовательной организации (далее - ОО) может использоваться только в функциональных и образовательных целях.
- 1.2. Пользователи должны соблюдать правила и инструкции по работе с электронной почтой, этические нормы общения.
- 1.3. Перед отправлением сообщения необходимо проверять правописание и грамматику текста.
- 1.4. Пользователям **запрещено:**
 - 1.4.1. Участвовать в рассылке посланий, не связанных с образовательным процессом.
 - 1.4.2. Пересылать по произвольным адресам' не затребованную потребителями информацию (спам).
 - 1.4.3. Отправлять сообщения противозаконного или неэтичного содержания.
 - 1.4.4. Использовать массовую рассылку электронной почты, за исключением необходимых случаев.
- 1.5. Электронное послание не должно использоваться для пересылки секретной и конфиденциальной информации, поскольку является эквивалентом почтовой открытки.

2. Порядок обработки, передачи и приема документов по электронной почте

- 2.1. По электронной почте производится получение и отправка информации законодательного, нормативно-правового, учебного, учебно-методического характера.
- 2.2. Для обработки, передачи и приема информации по электронной почте в ОО приказом директора назначается ответственное лицо.
- 2.3. При создании электронного ящика, сайта ОО ответственное лицо направляет в управление образования свои электронные реквизиты для формирования базы данных.
- 2.4. ОО должно обеспечить бесперебойное функционирование электронной почты и получение информации не реже двух раз в день.
- 2.5. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет ответственный за электронную почту.
- 2.6. Передаваемые с помощью электронной почты официальные документы должны иметь исходящий регистрационный номер.
- 2.7. Все передаваемые учебно-методические и справочно-информационные материалы должны передаваться с сопроводительным письмом.
- 2.8. При обучении работе с электронной почтой обучающихся ответственность за работу с почтой несет учитель.
- 2.9. Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями, предъявляемыми к оформлению официальных документов, в электронном виде и представляет по локальной сети или на носителе информации ответственному лицу за электронную почту.
- 2.10. **При получении электронного сообщения** ответственное лицо за электронную почту:
 - 2.10.1. Регистрирует документ в папке входящих документов;
 - 2.10.2. Передает документ на рассмотрение директору или в случае указания непосредственно адресату.
 - 2.10.3. В случае невозможности прочтения электронного сообщения уведомляет об этом отправителя.

ИНСТРУКЦИЯ

по организации антивирусной защиты компьютерной техники в образовательных организациях Приозерский муниципальный район Ленинградской области

1. Общие положения

- 1.1 В образовательной организации (далее - ОО) руководителем должно быть назначено лицо, ответственное за антивирусную защиту.
- 1.2 В ОО может использоваться только лицензионное антивирусное программное обеспечение.
- 1.3 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
- 1.4 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

2. Требования к проведению мероприятий по антивирусной защите

- 2.1 В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.
- 2.2 Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.
- 2.3 Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен **выполняться**:
- 2.4 Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах ОО.
- 2.5 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).
- 2.6 При отправке и получении электронной почты пользователь обязан проверить электронные письма на наличие вирусов.
- 2.7 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов или электронных писем **пользователи обязаны**:
 - Приостановить работу.
 - Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в ОО.
 - Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.
 - Провести лечение или уничтожение зараженных файлов.

3. Ответственность

- 3.1 Ответственность за организацию антивирусной защиты возлагается на руководителя ОО.
- 3.2 Ответственность за проведение мероприятий антивирусного контроля в организации и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты.
- 3.3 Периодический контроль за состоянием антивирусной защиты в ОО осуществляется руководителем.

Памятка по использованию ресурсов сети Интернет

1. Пользователь обязан выполнять все требования администратора локальной сети.
2. За одним рабочим местом должно находиться не более одного пользователя.
3. Пользователю разрешается переписывать полученную информацию на личные дискеты. Дискеты предварительно проверяются на наличие вирусов.
4. Разрешается использовать оборудование классов только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения проектов. Любое использование оборудования в коммерческих целях запрещено.
5. Запрещена передача внешним пользователям информации, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан. Правовые отношения регулируются Законом «Об информации, информатизации и защите информации», Законом «О государственной тайне», Законом «Об авторском праве и смежных правах», статьями Конституции об охране личной тайне, статьями Гражданского кодекса и статьями Уголовного кодекса о преступлениях в сфере компьютерной информации.
6. Запрещается работать с объемными ресурсами (video, audio, chat, игры) без согласования с администратором.
7. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.
8. Пользователю запрещено вносить какие-либо изменения и программное обеспечение, установленное как на рабочей станции, так и на серверах, а также производить запись на жесткий диск рабочей станции. Запрещается перегружать компьютер без согласования с администратором локальной сети.
9. Пользователь обязан сохранять оборудование в целостности и сохранности. При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность. В случае нарушения правил работы пользователь лишается доступа в сеть. За административное нарушение, не влекущее за собой порчу имущества, вывод оборудования из рабочего состояния и не противоречащие принятым правилам работы пользователь получает первое предупреждение. При повторном административном нарушении пользователь лишается доступа в Интернет без права восстановления. При возникновении технических проблем пользователь обязан поставить в известность администратора локальной сети.

ТИПОВЫЕ ПРАВИЛА использования сети Интернет в образовательных организациях Приозерский муниципальный район Ленинградской области

1. Общие положения

1.1. Использование сети Интернет в образовательной организации (далее – ОО) направлено на решение задач учебно-воспитательного процесса.

1.2. Настоящие Правила регулируют условия и порядок использования сети Интернет в ОО.

1.3. Настоящие Правила имеют статус локального нормативного акта ОО.

2. Организация использования сети Интернет в образовательной организации

2.1. Вопросы использования возможностей сети Интернет в учебно-образовательном процессе рассматриваются на педагогическом совете ОО. Педагогический совет утверждает Правила использования сети Интернет на учебный год. Правила вводятся в действие приказом руководителя ОО.

2.2. Правила использования сети Интернет разрабатываются педагогическим советом ОО на основе примерного регламента самостоятельно либо с привлечением внешних экспертов, в качестве которых могут выступать:

— преподаватели других образовательных организаций, имеющие опыт использования Интернета в образовательном процессе;

— специалисты в области информационных технологий;

— представители органов управления образованием;

— родители обучающихся.

2.3. При разработке правил использования сети Интернет педагогический совет руководствуется:

— законодательством Российской Федерации;

— опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета;

— интересами обучающихся;

— целями образовательного процесса;

— рекомендациями профильных органов и организаций в сфере классификации ресурсов Сети.

2.4. Руководитель ОО отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в ОО, а также за выполнение установленных правил. Для обеспечения доступа участников образовательного процесса к сети Интернет в соответствии с установленным в ОО правилами руководитель ОО назначает своим приказом ответственного за организацию работы с Интернетом и ограничение доступа.

2.5. Педагогический совет ОО:

— принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет;

— определяет характер и объем информации, публикуемой на интернет-ресурсах ОУ;

— дает руководителю ОО рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в Сети;

2.6. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет преподаватель, ведущий занятие.

При этом преподаватель:

- наблюдает за использованием компьютера и сети Интернет обучающимися;
- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.7. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют работники ОО, определенные приказом его руководителя.

Работник образовательной организации:

- наблюдает за использованием компьютера и сети Интернет обучающимися;
- принимает меры по пресечению обращений к ресурсам, не имеющих отношения к образовательному процессу;

- сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу.

2.8. При использовании сети Интернет в ОО обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношения к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в ОО или предоставленного оператором услуг связи.

2.9. Пользователи сети Интернет в ОО должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов, не имеющих отношения к образовательному процессу и содержание которых противоречит законодательству Российской Федерации. Участникам использования сети Интернет в ОУ следует осознавать, что ОО не несет ответственности за случайный доступ к подобной информации, размещенной не на интернет-ресурсах ОО.

2.10. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в ОО правилами обеспечивается работником ОО, назначенным его руководителем.

2.11. Принципы размещения информации на интернет-ресурсах ОО призваны **обеспечивать:**

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;

- защиту персональных данных обучающихся, преподавателей и сотрудников;

- достоверность и корректность информации.

2.12. Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на интернет-ресурсах, создаваемых ОО, только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и сотрудников ОО размещаются на его интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

2.13. В информационных сообщениях о мероприятиях, размещенных на сайте ОО без уведомления и получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя обучающегося либо фамилия, имя и отчество преподавателя, сотрудника или родителя.

2.14. При получении согласия на размещение персональных данных представитель ОО обязан разъяснить возможные риски и последствия их опубликования. ОО не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

3. Использование сети Интернет в образовательной организации

3.1. Использование сети Интернет в ОО осуществляется, как правило, в целях образовательного процесса.

3.2. По разрешению лица, ответственного за организацию в ОО работы сети Интернет и ограничение доступа, преподаватели, сотрудники и обучающиеся вправе:

- размещать собственную информацию в сети Интернет на интернет-ресурсах ОО;
- иметь учетную запись электронной почты на интернет-ресурсах ОО.

3.3. Обучающемуся **запрещается:**

- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- осуществлять любые сделки через Интернет;
- осуществлять загрузки файлов на компьютер ОО без специального разрешения;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, обучающийся обязан незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за работу локальной сети и ограничение доступа к информационным ресурсам.

Ответственный обязан:

- принять информацию от преподавателя;
- направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток);
- в случае явного нарушения обнаруженным ресурсом законодательства Российской Федерации сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:

- доменный адрес ресурса;
- сообщение о тематике ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо его несовместимости с задачами образовательного процесса;
- дату и время обнаружения;
- информацию об установленных в ОО технических средствах технического ограничения доступа к информации.

ТИПОВАЯ ИНСТРУКЦИЯ
для сотрудников образовательных организаций муниципального образования
Приозерский муниципальный район Ленинградской области
о порядке действий при осуществлении контроля использования обучающимися
сети Интернет

1. Настоящая инструкция устанавливает порядок действий сотрудников образовательных организаций (далее – ОО) при обнаружении:

- 1) обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;
- 2) отказа при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.

2. Контроль использования обучающимися сети Интернет осуществляют:

- 1) во время занятия — проводящий его преподаватель и (или) работник ОО, специально выделенный для помощи в проведении занятий;
- 2) во время использования сети Интернет для свободной работы обучающихся — сотрудник ОО, назначенный руководителем ОО в установленном порядке.

3. Преподаватель:

— определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;

— наблюдает за использованием обучающимися компьютеров и сети Интернет;

— способствует осуществлению контроля объемов трафика ОО в сети Интернет;

— запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

— доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;

— принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

4. При обнаружении ресурса, который, по мнению преподавателя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

5. В случае отказа доступа к ресурсу, разрешенному в ОО, преподаватель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

**ПРИМЕРНАЯ ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
сотрудника образовательной организации,
ответственного за использование преподавателями и
обучающимися доступа к сети Интернет**

1. Общие положения

1.1 Сотрудник образовательной организации (далее – ОО), ответственный за использование преподавателями и обучающимися доступа к сети Интернет, назначается на должность и освобождается от должности директором.

1.2. Сотрудник ОО, ответственный за использование преподавателями и обучающимися доступа к сети Интернет подчиняется непосредственно директору или заместителю директора по информационным технологиям.

1.3. Сотрудник ОО, ответственный за использование преподавателями и обучающимися доступа к сети Интернет, руководствуется в своей деятельности Конституцией и законами РФ, государственными нормативными актами органов управления образования всех уровней; Правилами и нормами охраны труда, техники безопасности и противопожарной защиты; локальными правовыми актами школы, а также настоящей должностной инструкцией.

2. Основные задачи и обязанности

Сотрудник ОО, ответственный за использование преподавателями и обучающимися доступа к сети Интернет, обеспечивает доступ сотрудников школы и учащихся к Интернету, а именно:

2.1. Следит за состоянием компьютерной техники и Интернет - канала точки доступа к сети Интернет. В случае необходимости обращается в ремонтную (сервисную) организацию или к поставщику Интернет - услуг.

2.2. Находится в помещении точки Доступа к сети Интернет на протяжении всего времени ее работы.

2.3. Ведет учет пользователей точки доступа к Интернет. В случае необходимости лимитирует время работы в Интернете пользователя.

2.4. Оказывает помощь пользователям точки доступа к сети Интернет во время сеансов работы в сети.

2.5. Участвует в организации повышения квалификации сотрудников школы по использованию Интернета в профессиональной деятельности.

2.6. Организует оформление стендов наглядными материалами по тематике Интернета: советами по работе с программным обеспечением (электронной почтой), обзорами интересных Интернет - ресурсов новостями педагогического Интернет - сообщества и т.п.

2.7. Осуществляет регулярное обновление антивирусного программного обеспечения. Контролирует проверку на внешних электронных носителях информации (дискет, СО-КОМ, флеш - накопителей) на отсутствие вирусов.

2.8. Следит за приходящей корреспонденцией на школьный ящик электронной почты.

2.9. Принимает участие в создании (реализации) школьной веб-страницы.

3. Права

Ответственный за использование преподавателями сети Интернет имеет право:

- 3.1. Участвовать в административных совещаниях по вопросам, связанным с использованием Интернета в образовательном процессе и управлении школой.
- 3.2. Отдавать распоряжения пользователям доступа к Интернет в рамках своей компетенции.
- 3.3. Ставить вопрос перед директором школы или заместителем директора по информатизации о нарушении точки доступа к сети Интернет, правил техники безопасности; противопожарной безопасности, поведения, регламента работы в Интернет.

4. Ответственность

Сотрудник ОО, ответственный за использование преподавателями и обучающимися доступа к сети Интернет, **несет полную ответственность за:**

- 4.1. Надлежащее и своевременное исполнение обязанностей, возложенных на него настоящей должностной инструкцией.
- 4.2. Соблюдение Правил техники безопасности, противопожарной безопасности и норм охраны труда в ОО.
- 4.3. Состояние делопроизводства по вверенному ему направлению работы.

ТИПОВАЯ ИНСТРУКЦИЯ пользователя по компьютерной безопасности

1. Установить последние обновления операционной системы Windows.
2. Включить режим автоматической загрузки обновлений. (Пуск->Настройка->панель управления->Автоматическое обновление->Автоматически загружать и устанавливать на компьютер рекомендуемые обновления).
3. Активировать встроенный брандмауэр Windows (Пуск->Настройка->панель управления->Брандмауэр Windows->Включить).
4. Установить антивирусное программное обеспечение на каждый компьютер. Включить режим автоматического сканирования файловой системы. Включить режим ежедневной автоматической проверки всей файловой системы при включении компьютера. Активировать функцию ежедневного автоматического обновления антивирусных баз.
5. Ежедневно проверять состояние антивирусного программного обеспечения, а именно
 - a. Режим автоматической защиты должен быть включен постоянно
 - b. Дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты.
 - c. Просматривать журналы ежедневных антивирусных проверок. Контролировать удаление вирусов при их появлении.
6. Не реже одного раза в месяц посещать сайт <http://windowsupdate.microsoft.com> и проверять установлены ли последние обновления операционной системы.
7. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.
8. Контролировать посещение Интернет сайтов пользователями. Не допускать посещения т.н. «хакерских», порно и других сайтов с потенциально вредоносным содержанием.
9. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.
10. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Ethernet сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.

ПРИМЕРНАЯ ИНСТРУКЦИЯ по осуществлению мониторинга эффективности работы системы контентной фильтрации в образовательных организациях

Общие требования:

1. Проверяемое автоматизированное рабочее место (далее – АРМ) должно иметь доступ к сети Интернет и использоваться обучающимися образовательного учреждения.
2. По согласованию на период контрольных мероприятий, может быть приглашен специалист ОАО «Ростелеком».
3. При проведении проверки необходимо обеспечить присутствие представителя образовательной организации (руководитель, заместители руководителя, сотрудник, ответственный за доступ к сети Интернет в ОО).

Мероприятия при общем мониторинге:

1. 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/>.
2. Внести название материала (части материала, адрес сайта) в поисковую систему.
3. 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.
4. 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.

Мероприятия при тематическом мониторинге (при необходимости):

1. Выбрать 3-4 противоправных материала по определенной теме (экстремизм, проявление жестокости, порнография, терроризм, суицид, насилие и т.д.).
2. Запросить через поисковую систему материал по заданной теме (Например: «изготовление зажигательной бомбы», «издевательства над несовершеннолетними», «способы суицида» и т.д.).
3. Из предложенного поисковой системой списка адресов перейти на страницу 2-3 сайтов и ознакомиться с полученными материалами.
4. Дать оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся.

5. 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/>.

По итогам мониторинга сформировать заключение (акт, справку, отчет) об эффективной (неэффективной) работе контентной фильтрации с приложением скриншотов экрана. При неэффективной работе контент- фильтра, в заключении необходимо указать выявленные проблемы, пути их решения и сроки исправления.

(примерный)

Журнал

проверок скорости доступа к сети Интернет и работы системы контентной фильтрации

№	Дата	Средняя скорость	Работа контент-фильтра	Обращение в тех. поддержку (№ и дата заявки)	Дата выполнения заявки	Фамилия ИО, ответственного лица