

Использование контент-фильтра SkyDNS.Школа в комплекте с Ideco ICS

Требования к настройке

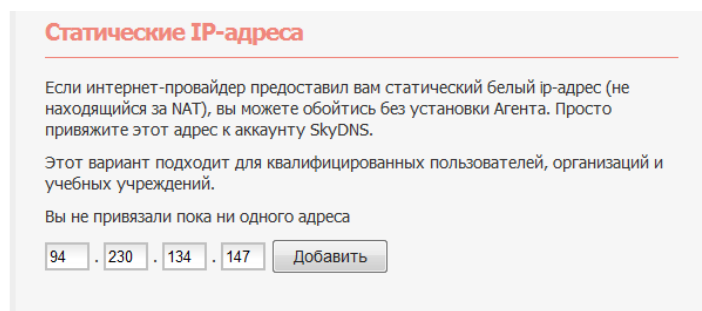
1. Установка контентной фильтрации в учебном заведении
 1. Настройка на интернет-шлюзе Ideco ICS
 2. Использование персонального агента SkyDNS Agent
2. Рекомендуемые правила контентной фильтрации и безопасный поиск
3. Работа только по белому списку
4. Настройки браузеров, установка поиска по умолчанию
5. Организационные меры
6. Как самостоятельно проверить качество фильтрации
7. Что делать, если пришла проверка
8. Правовая справка
9. Техническая поддержка контент-фильтра
10. Техническая поддержка интернет-шлюза
11. Приложение. Лист проверки «Подготовка к проверке контент-фильтрации»
12. Приложение. Примерные формулировки для внесения изменений в должностные инструкции отдельных работников образовательных учреждений
13. Приложение. Типовая инструкция для сотрудников образовательных учреждений о порядке действий при осуществлении контроля использования обучающимися сети Интернет
14. Приложение. Типовые правила использования сети Интернет в общеобразовательном учреждении

1. Установка контентной фильтрации в учебном заведении

В зависимости от схемы организации локальной сети в учебном заведении и схемы подключения учебных классов к интернет существуют разные варианты настройки контентного фильтра:

Настройка на интернет-шлюзе Ideco ICS

1. В случае статичного (неизменного) внешнего IP адреса школы, достаточно на сервере Ideco ICS зайти в раздел Сервер-Интерфейсы-Внешний интерфейс и в поле DNS1 прописать IP-адрес сервера SkyDNS – 193.58.251.251.
2. ОБРАТИТЕ ВНИМАНИЕ! В настройках всех сетевых соединений (как интернет, так и локального) на сервере НЕ должны быть указаны другие DNS серверы. Иначе фильтрация не будет работать.
3. После этого привяжите ваш внешний IP адрес в личном кабинете SkyDNS в разделе «Статические IP-адреса». Привязанный адрес в любой момент можно отвязать и привязать другой адрес, в случае необходимости.



Статические IP-адреса

Если интернет-провайдер предоставил вам статический белый IP-адрес (не находящийся за NAT), вы можете обойтись без установки Агента. Просто привяжите этот адрес к аккаунту SkyDNS.

Этот вариант подходит для квалифицированных пользователей, организаций и учебных учреждений.

Вы не привязали пока ни одного адреса

94 . 230 . 134 . 147

4. После этого можно переходить к настройке правил фильтрации.

Использование персонального агента SkyDNS Agent

Если на некоторых компьютерах необходимы индивидуальные настройки фильтрации, то такие компьютеры НЕ должны использовать веб прокси в составе Ideco ICS и на эти компьютеры необходимо установить программу SkyDNS Agent:

1. На компьютеры под управлением Windows поставьте программу SkyDNS Agent. Загружается данная программа из личного кабинета на сайте www.skydns.ru. При установке на компьютеры указываете ваш логин в SkyDNS (электронная почта) и пароль.
2. ОБРАТИТЕ ВНИМАНИЕ! Чтобы ученики не могли отключить фильтр они должны работать под учетными записями с ограниченными правами.
3. ОБРАТИТЕ ВНИМАНИЕ! Держите пароль от вашего логина в тайне, чтобы никто не мог с его помощью отключить фильтрацию.
4. После этого можно переходить к настройке правил фильтрации. Для индивидуальной настройки правил используются профили фильтрации.

Например, для компьютера директора или учительских можно создать профили с менее строгой фильтрацией или вообще без неё. Как настроить профили фильтрации описано по ссылке <https://www.skydns.ru/info/guides/profiles>

Полезные ссылки:

- Настройка SkyDNS Agent - <https://www.skydns.ru/info/guides/agent>

2. Рекомендуемые правила контентной фильтрации в школе и безопасный поиск

В штатном режиме, когда не ожидается проверка прокуратуры, возможна работа с ограничением по категориям интернет-ресурсов. Список категорий определяется методическими рекомендациями Министерства образования и науки по блокировке не соответствующих задачам образования ресурсов интернет в образовательных организациях.

Мы настоятельно рекомендуем включить фильтрацию следующих категорий (раздел Фильтр в личном кабинете):

- Федеральный список Минюста (в эту категорию входят только явно указанные в федеральном списке сайты, за исключением таких сайтов как vk.com, youtube.com)
- Агрессия, расизм, терроризм
- Грубость, матерщина, непристойность
- Запаркованные домены
- Наркотики
- Реклама и баннеры
- Плагиат и рефераты
- Прокси и анонимайзеры
- Ботнеты
- Сайты, распространяющие вирусы
- Фишинг
- Алкоголь и табак
- Знакомства
- Казино, лотереи, тотализаторы
- Оккультизм и астрология
- Порнография и секс
- Сайты для взрослых
- Радио и музыка онлайн
- Торренты и P2P-сети

- Файловые архивы
- Фотогалереи
- Фильмы и видео онлайн
- Досуг и развлечения
- Компьютерные игры
- Социальные сети
- Новости и СМИ
- Форумы
- Чаты и мессенджеры

Обязательно! Чтобы включить рекомендованные настройки блокировки по категориям в разделе Фильтр личного кабинета нажмите в меню левой колонки кнопку **«Для школ»** и нажмите кнопку Сохранить.

Обязательно! Включите опцию **«Блокировать неизвестные сайты»** (в особых настройках на странице Фильтр), чтобы блокировать все сайты неизвестные для сервиса SkyDNS и не попасть на только что появившийся сайт с неподходящим контентом.

Обязательно! Включите опцию **«Использовать безопасный поиск»**. В этом случае все запросы к поисковым системам будут перенаправляться на безопасный поиск SkyDNS – <http://poisk.skydns.ru>

Выдача этого поиска фильтруется от запрещенной информации (экстремистские материалы, порнография, наркотики, нецензурная речь, фишинговые и вирусные сайты).

ОБРАТИТЕ ВНИМАНИЕ! В категорию «Федеральный список Минюста» входят только явно указанные в федеральном списке экстремистских материалов сайты.

Существующая технология фильтрации не позволяет заблокировать абсолютно все сайты, содержащие произвольно выбранный тестовый, графический, аудио или видео материал из федерального списка экстремистских материалов, указанные без адреса их размещения в интернет. В связи с этим для более надежной защиты от экстремистских материалов можно использовать режим работы «Только по белому списку» и предоставлять доступ только к тем интернет-ресурсам, которые ваше учебное заведение определяет самостоятельно.

ОБРАТИТЕ ВНИМАНИЕ! При использовании исходной поисковой системой шифрованного протокола HTTPS, перенаправление будет работать некорректно. Поэтому необходимо в свойствах браузера поменять поисковую систему по умолчанию на ту которая работает по протоколу HTTP или отключить использование шифрованного протокола.

Полезные ссылки:

- Форма определения категории сайта - <https://www.skydns.ru/check>
- Безопасный поиск SkyDNS - <http://poisk.skydns.ru>
- Инструкции по установке безопасного поиска SkyDNS поиском по умолчанию в браузерах - <http://poisk.skydns.ru/guide>

3. Работа только по белому списку

Как было написано выше, существующая технология не позволяет ограничить доступ к определенным видам запрещенной информации со 100% гарантией. В связи с этим для максимально возможной защиты рекомендуется **использование режима «Работа только по белому списку»**.

В данном режиме доступ предоставляется только сайтам явно включенным вами в белый список (разрешенные ресурсы), а также сайтам входящим в различные каталоги образовательных ресурсов (например <http://window.edu.ru>)

Добавление ресурсов в белый список производится на странице «Домены» в личном кабинете.

Включение режима работы только по белому списку производится на странице «Фильтр» (под списком категорий). Поставьте галочку у опции и нажмите кнопку «Сохранить». Применение настроек занимает от 2 до 3 минут со стороны наших серверов.

Если вам необходимо добавить большой список ресурсов в белый список, то вы можете прислать его нам в техническую поддержку для проверки и мы его добавим в глобальный белый список, чтобы сделать доступным для всех учебных заведений.

4. Настройки браузеров, установка поиска по умолчанию

Часто проверяющие смотрят журналы браузеров на наличие в них посещенных ранее запрещенных сайтов, поэтому рекомендуется принудительно выключать в браузерах ведение журнала и истории, либо включать настройку очистки истории при выходе из браузера.

Кроме этого рекомендуется установить безопасный поиск как поиск по умолчанию, удалив все прочие поисковые системы из браузера или отключив их.

Firefox

1. Зайдите на страницу безопасного поиска poisk.skydns.ru
2. Щелкните на маленький треугольник возле названия текущей выбранной поисковой системы.
3. Выберите пункт «Добавить «Безопасный поиск»».
4. Еще раз нажмите на треугольник для вызова списка поисковых систем и выберите пункт «Управление поисковыми системами».

5. Выберите все прочие поисковые системы и нажмите «Удалить», чтобы «Безопасный поиск» остался единственным элементом в списке.

Chrome

1. Зайдите на страницу безопасного поиска poisk.skydns.ru
2. Щелкните правой клавишей мыши по строке с именем сайта и выберите из списка «Изменить поисковые системы».
3. Наведите мышь на строку «Безопасный поиск» и нажмите на «Использовать по умолчанию».
4. Удалите все прочие поисковые системы. Крестик для удаления появляется справа при наведении мыши на строку с названием поисковой системы.

Internet Explorer

1. Зайдите на страницу безопасного поиска poisk.skydns.ru
2. Щелкните на треугольник рядом с кнопкой с лупой.
3. Выберите пункт «Добавление поставщика поиска» и далее «Безопасный поиск».
4. В открывшемся диалоге поставьте галочку «Сделать поставщиком поиска по умолчанию» и нажмите «Добавить».
5. Снова нажмите на треугольник рядом с кнопкой с лупой и выберите пункт «Управление поставщиками поиска».
6. В открывшемся окне надстроек удалите все прочие поисковые системы.

5. Организационные меры

Не забывайте, что контентная фильтрация - это не только установка фильтра, но и ряд организационных мероприятий.

Согласно требованиям Министерства образования и науки РФ, каждое учебное заведение должно иметь регламент, определяющий порядок доступа в интернет и ответственных за контентную фильтрацию.

Образец регламента и прочих документов можно посмотреть в приложениях.

Удостоверьтесь, что в вашем регламенте четко обозначены:

- ответственные за фильтрацию,
- порядок допуска учеников и третьих лиц к компьютерам для использования интернет,
- обеспечение доступа только к безопасной поисковой системе SkyDNS и запрет на использование других систем,
- порядок действий при обнаружении доступа к сайтам с запрещенной информацией.

Также всегда имейте в школе актуальную копию федерального списка экстремистских материалов (<http://minjust.ru/extremist-materials>) в электронном или печатном виде.

Если в вашем регионе приняты локальные нормативные акты/законы по порядку доступа учебных заведений в интернет и/или контентной фильтрации, то также подготовьте и имейте их печатные копии.

6. Как самостоятельно проверить качество фильтрации

Чтобы самостоятельно проверить правильность настройки фильтра проведите следующую проверку:

Действие	Фильтрация настроена правильно	Фильтрация настроена неправильно
Зайдите на сайт www.yandex.ru	Открывается сайт poisk.skydns.ru	Открывается сайт www.yandex.ru
Зайдите на сайт www.google.com	Открывается сайт poisk.skydns.ru	Открывается сайт www.google.com
Зайдите на сайт huk.ru	Показывается страница блокировки	Сайт открывается
Зайдите на сайт www.vk.com	Показывается страница блокировки	Сайт открывается
В браузере запустите поисковый запрос «Удар русских богов»	Поисковая система выдает, что результатов не найдено	Поисковая система выдает ссылки на сайты
В браузере запустите поисковый запрос «Порно»	Поисковая система выдает, что результатов не найдено	Поисковая система выдает ссылки на сайты
В браузере запустите поисковый запрос «Гитлер Моя борьба»	Поисковая система выдает, что результатов не найдено	Поисковая система выдает ссылки на сайты
В браузере запустите поисковый запрос «Как взорвать школу»	Поисковая система выдает, что результатов не найдено	Поисковая система выдает ссылки на сайты

Поэкспериментируйте с другими запросами и сайтами.

Если для всех действий фильтрация у вас настроена правильно, то вы защищены.

Рекомендуем регулярно, не менее 1 раза в месяц, проводить подобную проверку с различными сайтами и запросами для контроля работы системы фильтрации.

7. Что делать, если пришла проверка

Во-первых, не паникуйте.

Во-вторых, выдайте проверяющим весь пакет документации по контентной фильтрации (регламент, актуальный список федерального списка, копии региональных законов/положений, копию договора с ООО «СкайдНС»).

После этого, выполните все обязательные процедуры по предоставлению допуска третьих лиц (проверяющих) к компьютерам — ознакомление с инструкцией под роспись и т.п.

Обычная процедура проверки заключается в использовании поисковой системы для нахождения запрещенной информации. В случае использования безопасной поисковой системы это будет сделать невозможно, либо очень трудно для определенных редких запросов.

В случае обнаружения проверяющим доступа к запрещенной информации, вы должны обязательно произвести все процедуры требуемые при этом.

Вот пример выдержки из регламента в Свердловской области:

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, Учитель должен предпринять следующие шаги:

4.1. записать адрес ресурса, дату и время его обнаружения;

4.2. закрыть данный ресурс и препятствовать дальнейшим попыткам учащихся зайти на него;

4.3. сообщить информацию о ресурсе в служебной записке на имя Зам руководителя ОУ по ИПК для блокирования доступа к нему;

Вы можете прямо при проверяющих произвести блокировку доступа к найденным ими сайтам, действуя в соответствии с положениями вашего регламента.

Единственно, удостоверьтесь, что после добавления сайтов в черный список, был перегружен браузер, для исключения влияния локального кеша.

ВАЖНО! В случае отказа проверяющих, выполнить установленные в школе процедуры доступа в интернет и доступа к запрещенной информации зафиксируйте это в письменном виде с отметкой проверяющего. Это поможет вам в случае разбирательства в суде.

ВАЖНО! В случае обнаружения проверяющим доступа к запрещенной информации независимо от них зафиксируйте, что именно было найдено, на каких сайтах (ссылки) и по каким поисковым запросам с указанием поисковой системы. Эта информация поможет вам при запросе официального ответа от ООО «СкайдНС» для предоставления в прокуратуру.

Если проверяющие просят дополнительную информацию или объяснительную о причинах доступа к найденным ресурсам с запрещенной информацией, обратитесь к нам на адрес технической поддержки support@skydns.ru или форму обратной связи на нашем сайте и мы предоставим требуемую информацию. При этом рекомендуем максимально подробно описать ситуацию и приложить сканы документов о проверке полученные от проверяющих.

Знайτε законы и выполняйте все законные требования проверяющих!

ОБРАТИТЕ ВНИМАНИЕ! Образовательные заведения не обязаны блокировать сайты входящие в единый реестр запрещенных сайтов (<http://eais.rkn.gov.ru/>). По действующему законодательству доступ к этому реестру имеют только лицензированные операторы связи и они же обязаны производить блокировку сайтов входящих в него.

8. Правовая справка

Фильтрация в учебных заведениях регулируется рядом федеральных законов, приказами и методическими рекомендациями Министерства образования и науки.

В соответствии с федеральными законами №139-ФЗ, №252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» и №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» организации предоставляющие доступ в интернет в местах, где могут быть дети, обязаны применять технические, программно-аппаратные средства защиты детей от информации, причиняющей вред их здоровью и развитию.

Также согласно закону №114-ФЗ "О противодействии экстремистской деятельности" должен быть ограничен доступ к экстремистским материалам. В законе не определяется, что является ответственным за это ограничение и традиционно прокуратуры пользуются этим, проводя проверки непосредственно в учебных заведениях.

Согласно статье 6.17 Кодекса РФ об административных правонарушениях отсутствие средств контент-фильтрации является административным правонарушением и влечет наложение штрафа на юридическое лицо в размере от 20 тысяч до 50 тысяч рублей. Но данное требование распространяется только на фильтры, касающиеся закона №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и не распространяется на требования закона №114-ФЗ "О противодействии экстремистской деятельности".

На уровне Министерства образования и науки установлены:

- Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет от 11.05.2011
- Методические рекомендации 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 от 2.04.2014

В указанных методических материалах содержится списки категорий информации, которые должны быть обязательно отфильтрованы в учебных заведениях и которые рекомендуется блокировать дополнительно к обязательному списку.

9. Техническая поддержка контент-фильтра

Если у вас есть вопросы, вы можете попробовать найти ответ в списке часто задаваемых вопросов - <https://www.skydns.ru/info/faq>

Если вам необходимо проверить к какой категории относится определенный сайт, вы можете сделать это через форму проверки - <https://www.skydns.ru/check>

Все вопросы по технической поддержке контент-фильтра вы можете задать через форму на сайте <https://www.skydns.ru/feedback>, почте support@skydns.ru или телефону 8-800-333-33-72.

Мы проконсультируем вас по всем вопросам связанным с его работой и настройкой.

10. Техническая поддержка интернет-шлюза

Все вопросы по технической поддержке интернет-шлюза Ideco ICS вы можете задать по телефону и электронной почте: +7 (495) 662-87-34, support@ideco.ru

По вопросам расширенной настройки, поиска проблем, и для зарегистрированных пользователей, обращайтесь в <http://helpdesk.ideco.ru/>

Приложение

Лист проверки «Подготовка к проверке контент-фильтрации»

1. Фильтрация ресурсов по настроенным правилам работает _____
2. Настроен белый список разрешенных ресурсов _____
3. Проверена работа безопасного поиска _____
4. В качестве поисковой системы по умолчанию в браузерах поставлен безопасный поиск SkyDNS, а другие поисковики удалены _____
5. Проверена работа в режиме «Только по белому списку» _____
6. Включен режим работы «Только по белому списку» _____
7. Подготовлена папка документов, в составе:
 1. Регламент доступа в интернет и контентной фильтрации _____
 2. Актуальная копия фед. списка экстрем. материалов _____
 3. Копия договора с системой контентной фильтрации _____
 4. Копии локальных законов о контент. Фильтрации _____

Дата проверки _____

Проверил _____

Приложение

Примерные формулировки для внесения изменений в должностные инструкции отдельных работников образовательных учреждений

В должностные инструкции работников образовательных учреждений рекомендуется внести дополнительно следующие положения.

Преподаватель

1. Общие положения

Должен знать:

- дидактические возможности использования ресурсов сети Интернет;
- правила безопасного использования сети Интернет.

2. Должностные обязанности:

- планирует использование ресурсов сети Интернет в учебном процессе с учетом специфики преподаваемого предмета;
- разрабатывает, согласует с методическим объединением, представляет на педагогическом совете образовательного учреждения и размещает в информационном пространстве образовательного учреждения календарно-тематическое планирование;
- получает и использует в своей деятельности электронный адрес и пароли для работы в сети Интернет и информационной среде образовательного учреждения;
- использует разнообразные приемы, методы и средства обучения, в том числе возможности сети Интернет;
- систематически повышает свою профессиональную квалификацию, общепедагогическую и предметную компетентность, включая ИКТ- компетентность, компетентность в использовании возможностей Интернета в учебном процессе;
- соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет.

3. Права

Вправе определять ресурсы сети Интернет, используемые обучающимися в учебном процессе.

4. Ответственность

Несет ответственность за выполнение обучающимися правил доступа к ресурсам сети Интернет в ходе учебного процесса.

Сотрудник образовательного учреждения, назначенный ответственным за работу Интернета и ограничение доступа

Ответственный за работу Интернета и ограничение доступа назначается приказом руководителя образовательного учреждения. В качестве ответственного за организацию доступа к сети Интернет может быть назначен заместитель руководителя образовательного учреждения по учебно-воспитательной работе, заместитель руководителя образовательного учреждения по информатизации,

преподаватель информатики, другой сотрудник образовательного учреждения.

1. Общие положения

Должен знать:

- дидактические возможности использования ресурсов сети Интернет;
- правила безопасного использования сети Интернет.

2. Должностные обязанности:

- планирует использование ресурсов сети Интернет в образовательном учреждении на основании заявок преподавателей и других работников образовательного учреждения;
- разрабатывает, согласует с педагогическим коллективом, представляет на педагогическом совете образовательного учреждения регламент использования сети Интернет в образовательном учреждении, включая регламент определения доступа к ресурсам сети Интернет;
- организует получение сотрудниками образовательного учреждения электронных адресов и паролей для работы в сети Интернет и информационной среде образовательного учреждения;
- организует контроль использования сети Интернет в образовательном учреждении;
- организует контроль работы оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;
- систематически повышает свою профессиональную квалификацию, общепедагогическую и предметную компетентность, включая ИКТ- компетентность, компетентность в использовании возможностей Интернета в учебном процессе;
- обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;
- соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет.

3. Права

Вправе определять ресурсы сети Интернет, используемые обучающимися в учебном процессе на основе запросов преподавателей.

4. Ответственность

Несет ответственность за выполнение правил использования Интернета и ограничения доступа, установленного в образовательном учреждении.

Приложение

Типовая инструкция для сотрудников образовательных учреждений о порядке действий при осуществлении контроля использования обучающимися сети Интернет

1. Настоящая инструкция устанавливает порядок действий сотрудников образовательных учреждений 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 ОУ, специально выделенный для помощи в проведении занятий;
- 2) во время использования сети Интернет для свободной работы обучающихся — сотрудник ОУ, назначенный руководителем ОУ 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 ОУ 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 ОУ, преподаватель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

Приложение

Типовые правила использования сети Интернет в общеобразовательном учреждении

1. Общие положения

1.1. Использование сети Интернет в образовательном учреждении направлено на решение задач учебно-воспитательного процесса.

1.2. Настоящие Правила регулируют условия и порядок использования сети Интернет в образовательном учреждении (ОУ).

1.3. Настоящие Правила имеют статус локального нормативного акта образовательного учреждения.

2. Организация использования сети Интернет в общеобразовательном учреждении

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

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

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

2.5. Педагогический совет ОУ:

- 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 ОУ 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 ОУ, определенные приказом его руководителя.

Работник образовательного учреждения:

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

2.9. Пользователи сети Интернет в ОУ 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 ОУ не несет ответственности за случайный доступ к подобной информации, размещенной не на интернет-ресурсах ОУ.

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 ОУ правилами обеспечивается работником ОУ, назначенным его руководителем.

2.11. Принципы размещения информации на интернет-ресурсах ОУ 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 ОУ, только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и сотрудников ОУ размещаются на его интернет-ресурсах только с письменного согласия лица, чьи

персональные данные размещаются.

2.13. В информационных сообщениях о мероприятиях, размещенных на сайте ОУ 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 ОУ обязан разъяснить возможные риски и последствия их опубликования. ОУ 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 образовательном учреждении

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

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

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

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 ОУ 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 ОУ технических средствах технического ограничения доступа к информации.