Полезная информация и советы по интернет-безопасности

Что такое Malware (Малварь) и как обезопасить себя от кибер-угроз?

Malware или **Малварь**, сокращенно от английского **malicious software** - вредоносное программное обеспечение, имеющее своей целью в той или иной форме нанести ущерб пользователю или компьютеру и его содержимому. **Малварь** - общее название для всех видов кибер-угроз, таких как: вирусы, трояны, шпионские программы, кейлоггеры, adware и др. **Malware** или вредоносы - достаточно распространенный вид кибер-угроз, и столкнуться с вредоносным ПО может каждый.

Какой вред может причинить Malware моему компьютеру?

Вредоносные программы создают множество проблем пользователю - от маленьких почти незаметных неудобств до серьезного финансового вреда:

- Меняют настройки браузера и не дают изменить их пользователю (например, устанавливает новую домашнюю страницу или поиск по умолчанию);
- Тратят ресурсы компьютера, тем самым снижают его быстродействие;
- Устанавливают рекламные программы на компьютер, такие как всплывающие окна и баннеры, которые работают даже без подключения к интернету;
- Используют компьютер и его ресурсы для DDoS-атак или майнинга криптовалют;
- Блокируют доступ к сайтам антивирусов и другим сайтам, содержащим инструменты для борьбы с вредоносным ПО;
- Собирают личные данные пользователя: логины, пароли, номера банковских карт и прочее;
- Без ведома пользователя могут скачивать с интернета и устанавливать другое вредоносное ПО.

Как удалить Malware с компьютера?

Такая программа хорошо маскируется и может ничем не выдавать свое присутствие для пользователя. Сегодня существует множество программных инструментов для того, чтобы очистить компьютер от Malware - антивирусы и специализированные Anti-Malware

программы. Однако очень многие вредоносные программы (Malware) обладают настолько высокой степенью защиты, что их практически невозможно удалить после запуска.

Как SkyDNS блокирует доступ к ресурсам, содержащим Malware?

SkyDNS предлагает альтернативный способ избежать вредоносных программ. Наша система аналитики, основанная на принципах машинного обучения, позволяет с точностью до 98% определять ресурсы, содержащие вредоносное ПО и эффективно блокировать доступ к ним. Предотвратите негативное влияние Malware еще до того, как вредоносное программное обеспечение попадет на ваш компьютер.

Как блокировать интернет-рекламу?

Технологии интернет-маркетинга развиваются с каждым днем, заставляя пользователей пройти по ссылке и купить какой-либо товар или услугу все более изощренными способами. На каждом шагу посетителей сайтов преследуют тонны рекламного «мусора», отвлекающие от основного контента страницы и раздражающие своей навязчивостью.

Как убрать всплывающие окна и другие виды интернет-рекламы?

Сегодня существует множество программ для блокировки рекламы в интернете: от сервисов, встроенных в популярные антивирусы, до отдельных плагинов, устанавливающихся в браузеры. Все они работают с разной степенью эффективности и позволяют блокировать разные типы онлайн-рекламы. Убрать навязчивые интернет-баннеры и всплывающие окна вы можете с помощью сервиса облачной фильтрации SkyDNS.

Это один из самых надежных и эффективных способов — фильтруется до 90% всех видов рекламы: от баннеров и всплывающих окон, до контекстной и видеорекламы. Система рекламного фильтра встроена в сервис контент-фильтрации SkyDNS по умолчанию, как одна из опций тарифов SkyDNS.Домашний и SkyDNS.Школа. Таким образом, вам не придется скачивать и устанавливать программу для блокировки рекламы в интернете. Наше решение позволит убрать онлайн-рекламу без установки дополнительного программного обеспечения на компьютер или плагина для браузера.

Как убрать рекламу из приложений?

Облачный фильтр интернета SkyDNS дает возможность убрать рекламу не только на компьютере, но и на любых устройствах, подключенных к сети Wi-Fi, в том числе и рекламу в играх и приложениях на планшетах и телефонах.

Что такое фишинг и как защититься от кражи паролей в интернете?

Вероятно, в Сети вы часто сталкивались с таким понятием как **Фишинг**. Что такое фишинг и как обезопасить себя от данного вида интернет-угроз? Мы поможем вам разобраться в этом вопросе.

Фишинг — это довольно распространенный вид интернет-мошенничества, основанный на невнимательности пользователей в Сети. Для того, чтобы вытянуть из пользователей личные данные, логины, пароли, номера банковских карт или другую важную информацию, злоумышленники создают поддельные страницы сайтов магазинов, банков, почтовых клиентов и соцсетей. Визуально они не отличаются от оригинальных, поэтому невнимательный посетитель вводит свои данные авторизации, после чего они попадают к мошенникам. Таким образом, мошенники могут взломать страницу вконтакте с помощью фишинга или получить доступ к банковскому аккаунту своей жертвы.

Как же обеспечить себе защиту от фишинга?

Прежде всего, никогда не доверяйте сообщениям, поступающим на вашу электронную почту, и ни в коем случае не переходите по ссылкам, указанным в письме! Следует помнить, что работники банков и администраторы соцсетей не занимаются рассылкой по электронной почте в случае возникновения каких-либо проблем с аккаунтом. Никогда не вводите свои конфиденциальные данные на домены, начинающиеся с http:// (то есть незащищенные домены), следите, чтобы адрес сайта начинался с безопасного протокола https://.

Самым надежным способом защитить себя от фишинговой атаки станет установка контент-фильтра с возможностями защиты от фишинга. Система контент-фильтрации SkyDNS поможет эффективно заблокировать доступ на фишинговые сайты, и обеспечить надежную защиту от подобных интернет-угроз. Благодаря нашему сервису вы всегда можете быть уверены в том, что ваши личные данные и пароли никогда не «утекут» к мошенникам.

Как проверить сайт на фишинг?

Не уверены в безопасности страницы? На сайте SkyDNS вы всегда сможете проверить сайт на фишинг, воспользовавшись нашей специальной формой проверки

https://www.skydns.ru/check/. Просто скопируйте подозрительную ссылку и вставьте ее в

нужное поле: сервис автоматически определит принадлежность сайта к той или иной категории.

Куда сообщить о фишинговом сайте?

Если вы обнаружили подозрительный сайт, отличающийся от оригинала внешне или в адресной строке, обязательно сообщите об этом! Ведь с вашей помощью удастся избежать попадания чьих-то конфиденциальных данных мошенникам и, в конечном итоге, приостановить деятельность фишингового ресурса. Прежде всего, сообщите о сайте-подделке владельцу или администрации ресурса. Обязательно оповестите о подозрительном сайте SkyDNS: https://www.skydns.ru/crime-link-add. Мы включим сайт в список блокировки, а также уведомим о мошенниках правоохранительные органы.

Необходим ли SkyDNS дома?

Многие задаются вопросом — так ли необходима контент-фильтрация дома? Ведь Роскомнадзор не проводит проверки в стенах вашего жилища и никто не обязывает вас соблюдать правила доступа к информации. Рассуждать так может только крайне безответственный родитель, которого не волнует, как его ребенок пользуется интернетом, и что он там может увидеть.

Интернет для семьи предполагает наличие определенных правил пользования и контроля доступного детям контента со стороны родителей. Для того, чтобы обеспечить ребенку безопасный интернет и оградить его от вредоносного и «взрослого» контента сегодня существует множество программных и технических решений. Одним из самых популярных вариантов является использование облачного интернет-фильтра SkyDNS в качестве средства защиты интернета.

Преимущества, которые дает использование контент-фильтра SkyDNS дома

Используя фильтр интернета SkyDNS вы получаете широкий набор возможностей:

- Функция родительского контроля компьютера
- Надежный запрет доступа к онлайн-играм, соцсетям и порно
- Режим **детского интернета**
- Эффективная блокировка рекламы в интернете
- Безопасный режим на YouTube
- Запрет доступа на сайты содержащие потенциальные угрозы
- Блокировка фишинговых страниц
- Контент-фильтрация на всех устройствах, подключенных к домашнему Wi-Fi

Как настроить дома родительский контроль?

Любой родитель знает, что ребенку свойственно любопытство. Исследовать мир, интересоваться тем, как устроены вещи и явления, познавать новое — все это помогает детям получить бесценный опыт, и освоиться в окружающей действительности. Но иногда любопытство оборачивается для ребенка опасностью. Далеко не все, что ребенок увидеть вокруг, предназначено для него и адаптировано под детскую психику.

В особенности это касается интернета. Ведь там очень много вещей, не предназначенных для детских глаз: страницы с эротическим контентом и порнографией, онлайн-игры и казино, экстремистские ресурсы, сайты с оскорбительным содержанием и ругательствами, реклама для взрослых и многое другое. В данных условиях становится очевиден тот факт, что дома просто необходимо установить родительский контроль на компьютере, чтобы оградить ребенка от «взрослого» содержания большинства страниц и обеспечить безопасный интернет для детей и подростков.

Как сделать детский интернет дома?

Защитите своего ребенка от «взрослого» контента с помощью сервиса облачной контент-фильтрации SkyDNS! Специально разработанный пакет для домашнего использования с функцией родительского контроля — SkyDNS.Домашний позволяет ограничить доступ к определенным сайтам и эффективно осуществлять фильтрацию интернета. Подробная статистика позволяет производить контроль посещения сайтов — вы сможете видеть на какие сайты заходили дети, и к каким ресурсам была применена блокировка, пока вас не было дома. Также с помощью нашего сервиса вы можете блокировать соцсети, не позволяя ребенку проводить слишком много времени во ВКонтакте.

Удобная настройка фильтра интернета

Выбирайте блокировку из более, чем 50 категорий сайтов, делайте собственные исключения благодаря черным и белым спискам! Настроить дома родительский контроль особенно легко с помощью специальной программы-агента, устанавливаемой на компьютер. Для того, чтобы обеспечить максимальную безопасность детей в интернете включите фильтр интернета в режиме белого списка. Таким образом, ребенок может зайти только на сайты, внесенные вами в белый список (размер списка ограничен 50 записями), а остальные сайты (да-да, все!) будут заблокированы. Узнать подробнее о других функциях решения SkyDNS.Домашний.

Как влияют соцсети на успеваемость учащихся?

Сегодня интернет занял прочное место в жизни людей. Сложно представить себе молодого человека, который бы хотя бы раз в день не проверял обновления в соцсетях и не листал новостную ленту. Современная действительность требует от нас постоянно оставаться на связи и быть в курсе последних новостей и трендов. Но влияет ли эта тенденция на успеваемость школьников и студентов?

Социальные сети: вред

Зачастую учащемуся не остается времени, чтобы усваивать получаемую на уроках информацию. Ведь в экране телефона или планшета есть вещи гораздо интереснее — переписка со сверстниками, новостные ленты, всевозможные группы социальных сетях, ну и, конечно же, ролики на YouTube. Кроме того, все свободное время ребенок может провести в интернете. Вместо того, чтобы заняться спортом, почитать книжку, пообщаться со своими сверстниками «вживую», подготовиться к урокам или просто погулять, он потратит время на соцсети. Само собой, это негативно сказывается на его физическом и интеллектуальном развитии.

Социальные сети: польза

Несомненно, в социальных сетях есть и полезные для развития ребенка вещи — множество образовательных групп во ВКонтакте и познавательных видео с YouTube. Кроме того, общение со сверстниками через соцсети может помочь ребенку социализироваться, найти новых друзей, обсудить с ними вопросы, связанные с учебой. Кроме того, в соцсетях ребенок может ненадолго расслабиться и отвлечься от повседневной школьной рутины.

Таким образом, можно прийти к выводу, что соцсети оказывают двоякое влияние на успеваемость учащихся, и нужно крайне ответственно подходить к вопросу использования соцсетей детьми и подростками. Ни в коем случае не следует забывать о том, какие негативные последствия может иметь чрезмерное увлечение соцсетями.

Как бороться с пагубным влиянием социальных сетей на школьника?

Конечно же, можно просто отобрать у него телефон или планшет, запретив ему таким образом использовать соцсети вообще или использовать программу для блокировки соцсетей. Но, поверьте, это не выход. Это не просто не даст нужного эффекта, но и значительно ухудшит ваши отношения с ребенком. Лучше всего будет объяснить ребенку,

что не стоит проводить все свободное время, сидя за компьютером, ведь это негативно сказывается на его развитии и здоровье.

Настройте дома родительский контроль

Хорошим вариантом для того, чтобы ограничить время, проводимое ребенком в сосцетях, станет использование системы контент-фильтрации дома и в школе. Компания SkyDNS предлагает эффективное решение для фильтрации интернета. С помощью **SkyDNS.Домашний**, специального решения для домашнего использования, вы сможете заблокировать доступ к соцсетям, а также настроить расписание, чтобы обеспечить ребенку определенные часы для досуга в течение дня.

Что делать, если в школу пришла прокурорская проверка?

Общие положения по прокурорской проверке

Если к вам пришла прокурорская проверка, то для начала, самое главное — не паниковать и не нервничать. Перед проверкой прокурор и его помощники должны обязательно предъявить свои удостоверения и другие документы, дающие им право на проведение проверки. Также работники прокуратуры должны сообщить причину проверки (проверки бывают плановые и внеплановые). Если проверка внеплановая, то она является следствием получения прокуратурой информации о нарушениях (жалобы, сообщения в СМИ). Как правило, прокуратура предупреждает образовательное учреждение заранее о проведении проверки. Однако проверка может быть и внезапной, но для этого нужны веские причины.

Помните, что прокурор вправе требовать документы, связанные только с предметом проверки. Обязательно подготовьте комплект документов по контентной фильтрации заранее. При проверке, касающейся фильтрации интернета в школе, вам будут необходимы следующие документы:

- Регламент, правила или положение о контентной фильтрации в образовательном заведении,
- Актуальная копия федерального списка экстремистских материалов Министерства юстиции,
- Копии региональных законов и положений о контентной фильтрации и защите детей в интернет,
- Договор с ООО «СкайДНС».

Дополнительно у вас могут быть отдельно оформлены:

- Журнал контроля контентной фильтрации,
- Акты о проверке контентной фильтрации,
- Приказ о назначении ответственного за контентную фильтрацию в образовательном заведении,
- Правила пользования интернетом в школе.

Тем самым вы покажете, что относитесь серьезно к исполнению норм законодательства. Ни в коем случае не препятствуйте получению прокурором необходимых документов, это

повлечет за собой возбуждение уголовного дела. **Статьей 294 УК РФ** предусмотрена ответственность за вмешательство в деятельность прокурора. Также, если сотрудник прокуратуры намеревается забрать оригиналы каких-либо документов, необходимо составить список этих документов и передать их под его расписку.

Как проходит проверка?

Часто проверка в школе касается компьютерного оборудования и Согласно законам **«Об образовании»** и **«О защите детей от информации, причиняющей вред их здоровью и развитию» (436-ФЗ)** администрация школы должна обеспечить запрет доступа к экстремистским ресурсам, внесенным в **список Министерства Юстиции РФ** (

http://minjust.ru/ru/extremist-materials). В ходе подобной проверки помощник прокурора в течение некоторого времени пытается найти запрещенные ресурсы через поисковые запросы в браузере на школьном компьютере. Если ему удастся зайти на такую страницу или найти в интернете текст, связанный с экстремизмом, то школе будет записано нарушение.

Что делать, если проверка выявила нарушения?

В случае обнаружения проверяющим доступа к запрещенной информации, вы должны обязательно выполнить все требуемые при этом процедуры. Во-первых, вы должны потребовать от проверяющего описание того, что было найдено и какие федеральные или местные законы оно нарушает, причем в письменном виде, с указанием даты и времени нахождения материала. Во-вторых учитель обязан закрыть данный ресурс и препятствовать любым попыткам учащихся зайти на него. Далее действуйте согласно положениям регламента. Также вы можете включить ресурс в список блокировки прямо при проверяющих. При этом обязательно убедитесь в том, что браузер был перезагружен для очистки локального кэша.

Вот например выдержка 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;

Результатом проверки может стать выявление тех или иных нарушений В любом случае, вы должны отреагировать на результат прокурорской проверки, каким бы он ни был. Если вы согласны с выявленными нарушениями - исправьте их в течение месяца и сообщите о проведенной работе в прокуратуру. Если результаты проверки кажутся вам необъективными, и вы не согласны с решением прокурора - обжалуйте решение через вышестоящего прокурора или обратитесь в суд (заявление подается в течение трех месяцев с момента получения решения). Также обязательно отправьте копию претензии прокуратуры в службу технической поддержки SkyDNS, чтобы мы проверили правильность проверки и выявленных нарушений и выдали вам официальное письмо для передачи в прокуратуру. В большинстве случаев претензии к школе после нашего письма снимаются.

Наиболее экономичным, простым и удобным вариантом успешно пройти прокурорскую проверку станет установка облачного контент-фильтра для блокировки доступа к запрещенным сайтам. Специальное решение для школ - **SkyDNS.Школа** является надежной гарантией успешного прохождения проверки прокуратуры. По доступной стоимости вы получите не только средство управления доступом к интернету, но и целый набор дополнительных функций, таких как блокировка рекламы, безопасный режим на YouTube, режим работы по «белому списку» и многое другое. Нашей системой контент-фильтрации уже пользуются более 6000 учебных заведений в России и странах ближнего зарубежья. Установить и настроить контент-фильтр в школе легко - с этим справится любой учитель информатики.

Виды онлайн-рекламы и как ее заблокировать?

Что раздражает нас в интернете больше всего? Правильно, реклама. Она навязчиво предлагает что-либо купить, поиграть в каком-либо онлайн-казино или потратить время на чтение бесполезных статей о «методе похудения Пугачевой». Здесь мы расскажем вам об основных видах интернет-рекламы и о том как с ней бороться:

1. **Баннеры.** Один из самых простых видов онлайн-рекламы. Представляет собой ссылку на сайт оформленную в виде картинки-баннера.
2. **Всплывающие окна.** Наиболее раздражающий вид рекламы. Иногда закрывают значительное пространство страницы сайта, что затрудняет чтение основного контента. Также могут быть выполнены с использованием технологии flash и иметь звуковую составляющую (зачастую, очень громкую). Не всегда просто закрыть всплывающее окно: разработчики онлайн-рекламы специально помещают кнопку закрытия в самом неподходящем месте и делают ее максимально незаметной.
3. **Контекстная реклама.** Основана на ранее сделанных вами запросах в поисковых системах. Если вы когда-либо искали «где купить пиццу?» в интернете - не удивляйтесь потом, что рекламные предложения пиццерий будут преследовать вас на каждом шагу.
4. **Аудио- и видеореклама.** Видео-ролики, которые вы обязаны просматривать в течение 10-30 секунд, прежде чем вы сможете закрыть их и перейти к основному содержанию страницы. Иногда можно посмотреть рекламный ролик, особенно если он хорошо снят, но когда тебе приходится смотреть по 20-30 роликов за час (возможно, совершенно одинаковых), это, мягко говоря, раздражает.
5. **Реклама в мобильных приложениях и играх.** Особенно раздражает реклама в тех приложениях, которые мы используем ежедневно (например, Скайп или YouTube). Рекламные баннеры в играх, зачастую, достаточно легко убрать, однако за это разработчики потребуют с вас некоторую сумму денег.

Следует помнить, что реклама не только отвлекает вас от непосредственных задач интернет-серфинга, но и значительно замедляет работу браузера и всей системы в целом. Особенно сильно расходует ресурсы компьютера видео-реклама и реклама, использующая flash-технологию. Также следует опасаться того, что кликнув по баннеру (случайно или намеренно), вы можете заразить свой компьютер вредоносным ПО или перейти на фишинговый сайт.

Как заблокировать интернет-рекламу?

Заблокировать онлайн-рекламу можно с помощью специальных программ или плагинов от рекламы для браузера. Однако маркетинговые технологии не стоят на месте, и разработчики онлайн-рекламы находят все новые и новые способы, чтобы обходить блокировку.

SkyDNS поможет эффективно блокировать онлайн-рекламу

Убрать онлайн-рекламу вам помогут технологии облачной фильтрации SkyDNS. Контентная фильтрация является эффективным фильтром против рекламы, гарантируя вам блокировку всех основных видов онлайн-рекламы на большей части сайтов. Вам не придется устанавливать какое-либо дополнительное программное обеспечение или плагины для браузера — все, что вам необходимо — включить блокировку рекламы в личном кабинете.

Блокировка рекламы как одна из опций входит в состав решений SkyDNS.Домашний, SkyDNS.Школа, SkyDNS.Бизнес и SkyDNS.WiFi. Выберите удобное решение, исходя из ваших задач и потребностей, и начните использовать сервис SkyDNS прямо сейчас!

Блокировка по разрешающему и запрещающему спискам

Функция списков исключений, включенная во все продукты для контентной фильтрации SkyDNS, позволяет пользователям осуществлять более гибкую настройку блокировки. Воспользуйтесь возможностью составлять разрешающие и запрещающие списки и настройте фильтрацию так, как вам удобно!

Как работают разрешающие и запрещающие списки?

Запрещающий список позволяет блокировать определенные домены. Так, например, вы можете не блокировать всю категорию «Социальные сети», а заблокировать только какую-нибудь конкретную соцсеть. Разрешающий список действует наоборот — вы блокируете всю категорию целиком, однако вносите исключения из данной категории, которые блокироваться не будут. Таким образом, вы можете настроить фильтрацию интернета исходя из своих предпочтений и задач ограничения доступа в интернет.

Режим работы по разрешающему списку

Особенно полезной для домашних пользователей и школ является функция **Работать по разрешающему списку**. Она позволяет переходить исключительно на сайты, которые содержатся в разрешающем списке, остальные сайты при этом блокируются.

Как добавить сайт в разрешающий или запрещающий список?

Для того, чтобы пользоваться функцией списков исключений, вам необходимо зарегистрироваться на нашем сайте, затем создайте списки и добавьте домены в соответствующие поля по очереди. Системе потребуется до 15 минут, чтобы внести изменения на сервер. После этого список исключений будет работать. Следует помнить, что размер запрещающих и разрешающих списков различается, в зависимости от тарифа.

Требования к настройке контент-фильтрации для образовательных учреждений и библиотек

Требования к настройке

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 подключения их к сервису контент-фильтрации:

Если есть центральный сервер или маршрутизатор/роутер

Если в школе, есть центральный сервер или маршрутизатор/роутер (ADSL, Wi-Fi), через который выходят в интернет все прочие компьютеры, то наиболее оптимальным вариантом настройки будет настройка подключения к фильтру непосредственно на самом сервере, маршрутизаторе/роутере.

Порядок настройки подключения в этом случае следующий:

В случае статичного (неизменного) внешнего IP адреса школы, достаточно на сервере или маршрутизаторе указать в настройках DNS для сетевого соединения адрес SkyDNS – 193.58.251.251.

> В настройках всех сетевых соединений (как интернет, так и локального) на сервере/маршрутизаторе **НЕ должны** быть указаны другие DNS серверы. Также поле DNS для IPv6 должно быть пустым и отключено автоматическое получение DNS. В противном случае фильтрация не будет работать.

> При использовании в школе прокси (обычного или прозрачного), необходимо указывать DNS сервер SkyDNS в настройках прокси сервера или отключить

проксирование. В противном случае фильтрация работать не будет.

После прописывания DNS в своей системе привяжите ваш внешний IP адрес в личном кабинете SkyDNS в разделе «Настройки — Сети — Статические IPадреса». Привязанный адрес в любой момент можно отвязать, привязать другой адрес, в случае необходимости, или перенести на другой профиль настроек.
После этого можно переходить к настройке правил фильтрации.

Все компьютеры подключены к интернет напрямую или через маршрутизатор провайдера (одноранговая сеть)

В этом случае единственным вариантом будет настройка контентного фильтра непосредственно на каждом компьютере в школе:

На компьютеры под управлением Windows поставьте программу SkyDNS Agent. Загружается данная программа из личного кабинета. При установке на компьютеры указываете ваш логин в SkyDNS (электронная почта) и пароль.

На компьютерах под управлением ОС Linux производится настройка DNS аналогично описанному в предыдущем разделе (центральный сервер) или установкой программы SkyDNS Agent.

Чтобы ученики не могли отключить фильтр они должны работать под учетными записями с ограниченными правами.

Держите пароль от вашего логина в тайне, чтобы никто не мог с его помощью отключить фильтрацию.

После этого можно переходить к настройке правил фильтрации.

В обоих случаях, как при использовании центрального сервера/маршрутизатора, так и одноранговой сети, возможно использование программы SkyDNS Agent для того чтобы предоставить некоторым лицам другие правила фильтрации, отличные от ученических. Например, для компьютера директора или учительских можно создать профили фильтрации с менее строгой фильтрацией или вообще без неё.

Если в вашем учебном заведении используется служба каталога MS Active Directory, то для корректной работы с локальными ресурсами каталога вам необходимо запросить в нашей службе поддержки специальную версию агента с поддержкой локальных ресурсов AD.

Также настройка раздельных правил фильтрации для отдельных компьютеров внутри сети доступна в аппаратном фильтре SkyDNS Школа К.

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 **Категории** в личном кабинете):

- Блокировка по предписанию
- Федеральный список Минюста (в эту категорию входят только явно указанные в федеральном списке сайты, за исключением таких сайтов как vk.com, youtube.com)
- Botnets & C2C
- Cryptojacking
- DGA
- Malware
- Phishing & Typosquatting
- Ransomware
- Запаркованные домены
- VPN, Прокси и анонимайзеры
- Агрессия, расизм, терроризм
- Грубость, матершина, непристойность
- Наркотики
- Плагиат и рефераты
- Алкоголь и табак
- Астрология
- Знакомства
- Казино, лотереи, тотализаторы
- Порнография и секс
- Сайты для взрослых
- Аниме
- Радио и музыка онлайн
- Торренты и P2P-сети
- Файловые архивы
- Фильмы и видео онлайн
- Фотогалереи
- Досуг и развлечения
- Компьютерные игры
- Онлайн-реклама и баннеры

- Социальные сети
- Форумы
- Чаты и мессенджеры
- Новости и СМИ

Чтобы включить рекомендованные настройки блокировки по категориям в разделе **Категории** личного кабинета нажмите в меню сверху кнопку **Настройки по 436-ФЗ** и нажмите кнопку Сохранить.

Включите опцию **Блокировать неизвестные сайты**, чтобы блокировать все сайты неизвестные для сервиса SkyDNS и не попасть на только что появившийся сайт с неподходящим контентом.

Включите опцию **Использовать безопасный поиск**. В этом случае все запросы к поисковым системам будут перенаправляться на безопасный поиск SkyDNS – http://search.skydns.ru Выдача этого поиска фильтруется от запрещенной информации (экстремистские материалы, порнография, наркотики, нецензурная речь, фишинговые и вирусные сайты).

Опция **Использовать безопасный режим Youtube** должна быть выключена!

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 опцию **Работать по разрешающему списку** и предоставлять доступ только к тем интернет-ресурсам, которые ваше учебное заведение определяет самостоятельно.

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.

Работа по разрешающему 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 опции **Работать по разрешающему 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 **Списки** в личном кабинете.

> Для корректной работы "Безопасного поиска" **в "Разрешающие списки" нельзя вносить домены поисковых систем**, так как это нарушит фильтрацию поисковой выдачи от запрещенной информации

Включение режима опции работы по разрешающему списку производится на странице **Категории** (над списком категорий). Включите переключатель у опции и нажмите кнопку **Сохранить**. Применение настроек занимает от 10 до 15 минут со стороны всех наших серверов.

> Если вам необходимо добавить большой список ресурсов в разрешающий 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.

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, вы должны установить безопасный поиск SkyDNS как поиск по умолчанию, удалив все прочие поисковые системы из браузера или отключив их.

Инструкции по установке безопасного поиска SkyDNS поиском по умолчанию в браузерах

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.

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 search.skydns.ru	Открывается сайт www.yandex.ru
Зайдите на сайт www.google.com	Открывается сайт search.skydns.ru	Открывается сайт www.google.com
Зайдите на сайт xuk.ru	Показывается страница блокировки	Открывается сайт xuk.ru
Зайдите на сайт www.vk.com	Показывается страница блокировки	Открывается сайт www.vk.com
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

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.

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 кэша.

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.

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.

Знайте законы и выполняйте все законные требования проверяющих!

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.

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 07.06.2019

В указанных методических материалах содержатся списки категорий информации, которые должны быть обязательно отфильтрованы в учебных заведениях и которые рекомендуется блокировать дополнительно к обязательному списку.
Россия, Екатеринбург, ул. Кулибина 2, офис

Техническая поддержка

Если у вас есть вопросы, вы можете попробовать найти ответ в списке часто задаваемых вопросов.

Рекомендации по усилению защиты от обхода контент-фильтра вы можете получить в этой статье.

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 вы можете задать

- через форму на сайте https://www.skydns.ru/feedback,
- по почте support@skydns.ru
- или телефону 8-800-333-33-72.

> Мы не оказываем услуг по настройке фильтра непосредственно в школе, но проконсультируем вас по всем вопросам связанным с его работой и настройкой, и поможем произвести правильную настройку в удаленном режиме.

Есть вопросы?

Если у вас есть вопросы, вы можете попробовать найти ответ в списке часто задаваемых вопросов.
Или задать свой вопрос нам напрямую по адресам info@skydns.ru или телефону 8-800-333-

33-72.
Обращайтесь к нам по любым вопросам связанным с заключением или продлением договора на контент-фильтрацию, функционалом фильтра (в том числе и пока отсутствующего в нём), категоризацией сайтов, контентной фильтрацией, обращением надзорных органов и т. п., мы постараемся дать вам скорейший ответ на любой ваш вопрос.

Приложение

Лист проверки «Подготовка к проверке контент-фильтрации»

1. Фильтрация ресурсов по настроенным правилам работает _____
2. Настроен белые 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 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 отношения 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 техническим 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.