Антитеррористическая комиссия в Чувашской Республике

Министерство образования и молодёжной политики Чувашской Республики

Методические рекомендации

для образовательных организаций, подключенных к сети Интернет

г. Чебоксары, 2016

1. Введение

Развитие образования во всем мире имеет общие тенденции – повышение доступности, внедрение дистанционных форм, технологизация, подстройка под изменение запросов рынка труда. Все это требует обеспечение доступа к большим объемам быстро меняющейся информации.

В Конституции Российской Федерации (статья 29) провозглашено право каждого человека на свободный поиск, получение и передачу информации законным способом.

Глобальная сеть Интернет, являясь мировым хранилищем всевозможной информации, предоставляет возможности по поиску, получению и передаче информации. Однако, в Интернете, в настоящее время, находится асоциальная информация, которая может нанести вред здоровью и психике ребенка.

В Федеральном законе «Об основных гарантиях прав ребенка в Российской Федерации» № 124-ФЗ от 24.07.1998 (с изменениями) в ст. 14 указано на необходимость принятия всех мер по защите ребенка от информации, наносящий вред его здоровью, нравственному и физическому развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, а также от информации пропагандирующей насилие и жестокость, порнографию, наркоманию, токсикоманию, антиобщественное поведение.

Принятый 29 декабря 2010 года Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает правила медиа-безопасности детей при обороте на территории России продукции СМИ, печатной, аудиовизуальной продукции на любых видах носителей, программ для компьютеров и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи. Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.06.2015) «О защите детей от информации, причиняющей вред их здоровью и развитию» конкретизировал и дополнил требования к свободно доступной информации. В ст. 14. указанного закона особо отмечено, что «...доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, в местах, доступных для детей, предоставляется … при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

Кроме того, принят Федеральный закон Российской Федерации от 21 июля 2011 г. № 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», направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки. Закон устанавливает порядок прекращения распространения продукции средств массовой информации, осуществляемого с нарушением законодательно установленных требований. Он, также, запрещает размещение рекламы в учебниках, учебных пособиях, другой учебной литературе, предназначенных для обучения детей, а также распространение рекламы, содержащей информацию, запрещенную для распространения среди детей, в детских образовательных организациях.

Федеральный закон Российской Федерации от 28 июля 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» конкретизировал ранее принятые нормативные акты и внес дополнительные изменения, связанные, в частности, с развитием сотовой связи.

Учитывая что:

– достаточно большое количество детей, находятся в социально неблагополучных условиях;

– высока уязвимость детей, со стороны лиц, совершающих противоправные действия с применением высоких технологий;

– существенно возросла скорость распространения информации в сети Интернет и все более массовое развитие получили интернет-технологии в России, одной из первостепенных задач образовательного сообщества является необходимость защиты несовершеннолетних от противоправных действий с использованием сети Интернет. Постоянное развитие интернет-технологий и их широкое проникновение в нашу жизнь ставит перед государством и обществом задачу поддержания эффективного комплекса мер по профилактике, предотвращению и преодолению последствий вредоносных действий в отношении несовершеннолетних, совершаемых с применением Интернета или информационно-коммуникационных технологий.

Таким образом, очевидной становится проблема между обязанностью предоставления возможности широкого использования ресурсов Интернет в образовательном процессе и необходимостью контролировать получаемую школьником информацию на соответствие федеральным законам.

Поговорим о контент-фильтрации.

Для полного понимания этого термина приведем определение понятия контент. **Контент** – это наполнение или содержание какого-либо информационного ресурса – текст, графика, музыка, видео, звуки и т.д. (например: контент интернет-сайта); **Мобильный контент** – мультимедийное наполнение (графика, музыка, рингтоны, видео, игры, программное обеспечение), адаптированное для использования в мобильных устройствах (телефоны, смартфоны, коммуникаторы и т.п.).

Информация нежелательного характера, которая несет в себе контентные риски, – это различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию.

К противозаконной, неэтичной и вредоносной информации относится:

– информация о насилии, жестокости и агрессии;

– информация, разжигающая расовую ненависть, нетерпимость по отношению к другим людям по национальным, социальным, групповым признакам;

– пропаганда суицида;

– пропаганда азартных игр;

– пропаганда и распространение наркотических веществ, отравляющих веществ;

– пропаганда анорексии (отказ от приема пищи) и булимии (чрезмерное потребление пищи);

– пропаганда деятельности различных сект, неформальных молодежных движений;

– эротика и порнография;

– нецензурная лексика и т.д.

К сожалению, в сети Интернет такую информацию можно встретить практически везде: в социальных сетях, блогах, торрентах, персональных сайтах, видеохостингах и др. Не являются исключением и мобильные сервисы.

Неэтичный, противоречащий принятым в обществе нормам морали и социальным нормам, контент не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей и оказать вредоносное воздействие. Подобная информация не попадает под действие уголовного кодекса, но может оказать негативное влияние на психику человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, порнография, агрессивные онлайн игры, азартные игры, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей), нецензурная брань, оскорбления, и др.

Неэтичная и вредоносная информация может быть направлена на манипулирование сознанием и действиями различных групп людей, в первую очередь – на молодежь.

Вредоносный контент может привести к заражению компьютера вирусами и потере важных данных, например, просмотр тех или иных видео-материалов через сеть интернет приводит к заражению компьютера вирусами. В последнее время, очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера, получить деньги незаконным способом. Такие действия могут преследоваться по закону в соответствии со статьями Уголовного кодекса Российской Федерации (ст. 272, 273, 274).

В Интернете есть большая доля информации, которую никак нельзя назвать ни полезной, ни надежной, ни достоверной. Молодые пользователи Сети должны мыслить критически, чтобы оценить достоверность, актуальность и полноту информационных материалов; поскольку абсолютно любой может опубликовать информацию в Интернете. В Интернете не существует служб редакторов и корректоров, никто не проверяет информационные ресурсы на достоверность, корректность и полноту.

Поэтому нельзя использовать Интернет как единственный источник информации, необходимо проверять информацию по другим источникам, особенно если эта информация касается жизненно важных моментов в жизни человека, например, здоровья, обучения, нормативных правовых актов и т.п.

На основании положений ч. 1 ст. 14 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в образовательных организациях должна быть установлена и настроена, как минимум, двухуровневая система фильтрации интернет трафика (контент-фильтрация).

Достаточно подробно особенности работы образовательной организации в сети Интернет описаны в письме Министерства образования и науки Российской Федерации от 28 апреля 2014 г. № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет».

Каждая образовательная организация сама несет полную ответственность за работу в сети Интернет, в том числе, за организацию контент-фильрации.

Обычно, **первый уровень контент фильтрации** осуществляется на уровне провайдера (на основании прописанного образовательной организацией договора).

Второй уровень контент-фильтрации осуществляется на уровне образовательной организации, для этого используются как средства контент-фильтрации (далее – СКФ) на базе сервера (ClearOS, Squid), так и средства персональной контент-фильтрации (Интернет-Цензор).

Допускается создания **третьего уровня СКФ** – на уровне рабочего места обучаемого.

В образовательной организации должны быть назначены ответственные за функционирование СКФ лица, соответствующая локальная нормативно-правовая база (положения, инструкции и др.), а также на всех рабочих местах необходимо вести журналы работы пользователей в сети Интернет.

2. Как организовать СКФ в образовательной организации

Контент может фильтроваться на уровне провайдера (на основании заключенного с ним договора), на уровне шлюза в Интернет защищаемой сети и на уровне рабочей станции.

Фильтрация может быть построена на основе внешней обновляемой базы данных запрещенных ресурсов и основана на локальной программе, которая действует по собственным принципам фильтрации («черные», «белые» списки, ключевые слова и т.п.).

При этом фильтрация может быть построена либо по принципу: «запрещаем все, кроме того, что можно», либо «можно все, кроме того, что запрещено».

Конечно, реализовать фильтрацию по принципу «Запрещаем все, кроме того, что можно» построить достаточно просто, подобная форма имеет смысл для младших школьников, но в этом случае Интернет теряет многие свои функции.

Второй вариант требует построения и обновления огромной базы данных (поддерживать ее должен провайдер сервиса), которая постоянно пополняется информацией о запрещенном контенте.

Для полноценной реализации второго вида фильтрации необходимо проиндексировать миллиарды Web-страниц и это под силу только крупным провайдерам подобного сервиса. В частности, по такому принципу работает Proventia Web Filter. Чем больше база, тем качественнее, но и дороже решение.

Сложности фильтрации контента в образовательных организациях.

Каждый день в Интернете появляются тысячи новых сайтов, многие сайты меняют свои местонахождение и адресацию, поэтому, даже используя постоянное обновления баз данных с адресами нежелательных ресурсов, добиться сто процентной гарантии фильтрации невозможно. Это сильно усложняет организацию СКФ в образовательной организации. Практически невозможно долгое время использовать «белый» список сайтов.

Отдельная проблема – это недостаточная фильтрация русскоязычного контента западными программными продуктами. Возможны ошибки когда фильтр будет отсеивать сайты полезного содержания и пропускать нежелательную информацию. В общем, чем более интеллектуален фильтр и чем больше база на которую он опирается, тем дороже решение и тем оно менее доступно для образовательных организаций.

Образовательный процесс требует доступа к множеству различных областей знаний и контент-фильтрация должна быть всеобъемлющей, настраиваемой, а также обеспечивать защиту от новейших постоянно меняющихся угроз.

Если в образовательной организации установлено различное компьютерное оборудование, а так часто бывает, то необходимы продукты фильтрации контента (Web и e-mail), работающие на различных платформах, что требует дополнительных ресурсов.

Мониторинг интернет-активности.

Мониторинг и протоколирование – это во многих случаях первый и важнейший шаг в контролировании интернет-доступа. Данная функция наглядно показывает серфинг-профиль пользователя. Учитель может проверить где находился ученик, что просматривал, в какое время и как долго.

Не контролируемое использование Интренета повышает возможность заражения вирусом, увеличивает возможности инсайдерских угроз, существенно повышает финансовые расходы.

Одним из основных способов контроля действий пользователя является **мониторинг его рабочего стола**. Это реализуется двумя способами – администратор видит всё то, что сейчас видит пользователь, или просматривает сохранённые снимки экрана.

Мониторинг доступа к USB. Съёмные usb-носители представляют серьёзную угрозу сохранности информации, поэтому доступ к ним может контролироваться системой. Большинство систем наблюдения предоставляют возможность блокировки доступа ко всем устройствам, фильтрации устройств и журналирования использования usb-устройств. Это предотвращает как утечку информации, так и проникновение вирусов на рабочий компьютер. Часто при разрешённом доступе информация, копируемая на съёмный носитель, сохраняется в другом месте и может быть использована для расследования нарушений.

В Windows технически это реализуется несколькими способами:

– полное блокирование через реестр;

– полное блокирование, через запрет записи в файлы %SystemRoot%\Inf\Usbstor.pnf , %SystemRoot%\Inf\Usbstor.inf;

– частичная блокировка и фильтрация возможна через написание USB-драйвера.

Мониторинг посещаемых веб-сайтов позволяет выявить не целевое использование компьютерного времени, отслеживать поисковые запросы обучающихся (из них можно отследить – ищет ли он необходимую или не относящуюся к образовательному процессу информацию). Сохраняются Url, заголовки посещённых страниц, время их посещения. Некоторыми системами реализуется возможность наблюдения в режиме реального времени за открытыми сайтами.

Социальные сети. Помимо не целевой траты времени на социальные сети, через них может утекать конфиденциальная информация, а в них может содержаться ассоциальная и запрещенная информация. Поэтому система может сохранять набор данных: просматриваемые профили, переписки, а также отправляемые туда фотографии.

IM. Чтобы предотвратить или потом доказать утечку информации, можно перехватывать и сохранять сообщения большинства популярных IM-протоколов и месседжеров (ICQ, Jabber,IRC, Skype). Это делается как программными средствами, так и через анализ трафика проходящего через шлюз.

Мониторинг электронной почты. По данным Infowatch в первой половине 2013 года почти 30% утечек происходили через Email, поэтому важно контролировать что отсылается/принимается сотрудником и обучаемыми. Для этого ведётся полное журналирование всех сообщений электронной почты. Чаще всего это делается путём перехвата сообщений локального почтового-клиента, однако возможен и перехват сообщений отправляемых через web-клиент.

Технически, такой вид мониторинга может быть реализован двумя способами:

– перехват непосредственно сетевого трафика программно или аппаратно. Это работает до тех пор, пока не используется защищенное интернет соединение, например SSL;

– перехват содержания web-форм, полей ввода и прочего. При таком методе наблюдения, скрыть передаваемое сообщение практически не возможно.

Основные локальные действия пользователя тоже при этом контролируются:

Мониторинг клавиатуры. Система записывает все нажимаемые клавиши, включая системные (CTRL, SHIFT, ALT, CAPS LOCK), кроме этого, могут быть записаны название окна, в которое производился ввод, язык раскладки и т.д. Это позволяет контролировать использование конфиденциальной информации,

восстанавливать забытые пароли, отслеживать объём проделанной работы. Программа, занимающаяся только перехватом нажатий клавиш, называется кейлоггер. Для Windows кейлоггеры создаются с помощью так называемых хуков, когда между нажатием клавиши и отправкой сообщения окну о факте нажатия вклинивается сторонняя функция, которая отмечает факт нажатия клавиши.

Буфер обмена. Система сохраняет всё, что было скопировано в буфер обмена, и почти всегда сопутствующую информацию. Это позволяет предотвратить потерю информации, даёт возможность обнаружить разглашение конфиденциальной информации. Windows предоставляет стандартную функцию для этих целей SetClipboardViewer, для Linux это делается через Xlib. Также есть платформонезависимые средства управления буфером обмена, например Qt. Запоминаются все действия с файлами: копирование, удаление, редактирование и программа, через которую действие совершено. Это позволяет установить, какие файлы использовались и выявить вирусную атаку. Для Windows программно это реализуется подменой стандартных функций чтения/записи файла в соответствующих DLL. В Linux этого можно достичь, перехватывая системные вызовы.

Печать файлов. Через принтер может утечь конфиденциальная информация, поэтому можно сохранять названия печатаемых файлов, время и дата печати. Также печатаемые файлы могут сохраняться как в виде исходного файла, так и в виде графического файла. В Windows для таких целей предусмотрен Print Spooler API, позволяющий управлять очередью печати. Мониторинг дает быструю и точную картину Web серфинга. Данные об интернет активности защищены криптографически и хранятся в недоступном для неавторизованного просмотра виде. Любой посещенный ресурс может быть просмотрен, и впоследствии добавлен в список разрешенных или запрещенных листов.

Отчеты мониторинга (Monitoring Reports) четко показывают: какие Web-страницы посещались, время визита, Web-адрес, и прочая информация.

Фильтры сетевого контента.

Фильтрация сетевого контента – системы позволяющие ограничивать доступ к тем или иным сетевым сервисам или сайтам.

Фильтры системы **CyberPatrol** позволяют учителям контролировать как, когда и кому

интернет-доступ разрешен, (разрешен с ограничением (в виде фильтрации контента) или заблокирован в принципе). Сайт программы: https://www.cyberpatrol.com

Фильтрация или блокирование web-сайтов, групп новостей и результатов, которые выдают поисковые машины, базируются на базе данных, которая может настраиваться путем добавления собственного списка запрещенных или разрешенных сайтов.

Программа позволяет блокировать чаты и программы класса Instant Messaging.

Чат-сессии могут быть также подвергнуты фильтрации для предотвращения утечки важной информации (имена, адреса телефоны и т.п.).

Программа поддерживает Лист разрешенных сайтов (YES List), который ограничивает пользователей серфингом только по заранее заданному разрешенному списку сайтов. Это хорошее решение для младших школьников. Можно выбирать заранее заданные настройки (Preset Filter Strengths). Имеются группы Ребенок (Child), Младшие тинэйджеры (Young Teen), Старшие тинэйджеры (Mature Teen) и т.п.

Имеется также возможность настроить профиль фильтрации, указав какие категории сайтов должны фильтроваться жестко, а какие мягко.

Еженедельные листы обновлений (Weekly List Updates) поступают еженедельно (или 2 раза в неделю), добавляя тысячи новых сайтов.

CyberPatrol поставляется с функцией «ready-to-go filtering» (преднастроенной фильтрацией). Настройки могут быть изменены пользователем.

Защита приватности предотвращает утечку приватной информации (имена, адреса, номера телефонов). Информация фильтруется прежде чем покинуть ваш компьютер.

Доступны ограничения на время проведенное в онлайне и доступ к определенным программам. Временной контроль позволяет ограничить длительное пребывание за компьютером, например, исключить длительное участие в сетевой игре.

Ограничения могут базироваться на времени суток (например, во время уроков или после урока), по дням недели и т.п.

Возможен контроль за скачиванием программ из Сети, поскольку скачивание программ может быть небезопасным, нарушать политику школы в отношении

пользования пиратским ПО. Вы можете заблокировать скачивание без разрешения игр, музыки, графических файлов, видео. Это в свою очередь снизит риск загрузки шпионского ПО вирусов, скачивание пиратской продукции.

CyberPatrol использует многослойную защиту, которая включает следующие технологии:

CyberLIST – постоянно пополняемая база запрещенных сайтов.

CyberPATTERNS – технология контекстной фильтрация по ключевым словам.

Web Page Analysis – контентный анализ Web-страниц на базе динамического посещения сайтов, которые еще не были категоризированы с помощью CyberLIST.

Web Link Analysis – на базе анализа Web-ссылок блокируются изображения непристойного содержания, которые могут возвращаться в ответ на запросы, не содержащие запрещенных ключевых слов.

Мощность Web-фильтрации может варьироваться за счет подключенных методов фильтрации.

SurfControl Web Filter – средство управления доступом в Интернет, позволяющее оптимизировать использование сетевых ресурсов и снизить возможные риски, связанные с использованием Интернета.

Разработчик: SurfControl (www.surfcontrol.com).

Сайт программы: http://www.surfcontrol.ru/web_filter.shtml

Программа предоставляет пользователям доступ к полезной информации в Интернете, одновременно преграждая им доступ к запрещенным Web-сайтам. Кроме того, вероятность потери важных данных или выхода из строя всей сети может быть снижена за счет запрещения загрузки потенциально опасных файлов, которые могут содержать вирусы либо другой разрушительный или опасный программный код (*.doc, *.vbs, *.elm, *.exe и *.zip).

Фильтр пресекает действия, ведущие к увеличению трафика вследствие посещения развлекательных сетевых ресурсов, скачивания музыки или просмотра видеоклипов, и составляет подробный отчет об использовании Интернета.

Продукты SurfControl оптимизированы для обеспечения безопасности процесса образования. SurfControl работает практически при любом способе организации сети, в том числе он может работать совместно с популярными антивирусными программами и брандмауэрами. Решения SurfControl легки в

управлении, что позволяет и специалистам и простым пользователям создавать и поддерживать гибкую политику безопасности. Например легко можно идентифицировать и ограничивать web-контент и e-mail на основе различных критериев (определенный web-сайт или страница; категория web-контента (порнография, расизм, хакерство, и др.); категория e-mail сообщений; конкретный пользователь; имя пользователя; имя группы; время суток; время, проведенное пользователем в сети; создаваемая им нагрузка на сеть).

Стандартные и настраиваемые отчеты позволяют определять эффективность применяемых правил использования Интернет. То есть можно получать данные о посещенных сайтах, кем они были посещены, как часто, как долго и когда. Мониторы реального времени могут информировать администраторов, учителей, родителей и школьников о попытках нарушения политики. Также можно установить правила обращения с определенными типами e-mail сообщений – удаление, изоляция, задержка, пересылка или доставка получателю.

Разносторонняя база данных SurfControl обладает наиболее современной и комплексной базой данных контента, предлагая обширную базу данных, классифицированную по категориям риска, как web, так и e-mail. Кроме того, продукт использует технологии искусственного интеллекта динамически расширяющих определяемый контент, что помогает защитить пользователей от внешних угроз прежде, чем они получили широкое распространение или были помещены в базу данных.

Proventia Web Filter – это блокиратор нежелательного Web-содержимого, который ежемесячно анализирует 120 млн. Web-страниц и ежедневно добавляет в базу 100 тыс. новых и обновленных Web-страниц. Блокиратор отличается гибкостью настройки, так что системный администратор легко может определить, кто будет иметь доступ к какой информации в какое время, а также какое содержимое будет блокироваться.

Разработчик: Internet Security Systems (www.iss.net).

Сайт программы: http://www.iss.net/products/Proventia_Web_Filter/

При анализе того или иного сайта программа принимает решение о том, к какой категории его следует отнести. Всего рассматривается 58 категорий (порнография, откровенное фото, образование, религия и т.п.). Технология фильтрации основана на анализе текста и распознавании графики.

Технология WebLearn позволяет создавать схемы поведения пользователей в Интернете. С ее помощью организации могут оптимизировать и расширять фильтрующую базу данных компании Internet Security Systems для решения своих специфических проблем. Если некоторые Web-сайты, посещаемые пользователями, не будут по какой-либо причине идентифицированы, то их URL-адреса автоматически и анонимно посылаются в Global Data Center для анализа с последующим распределением их по соответствующим категориям базы данных, которая содержит более 20 млн. URL-адресов.

С помощью функции Blocking by Extension (блокирование по расширению файла) руководство может запретить загружать во внутреннюю сеть любые файлы изображений, звуковые и видеофайлы, а также документы больших объемов.

В настоящее время доступны следующие версии Proventia Web Filter:

Proventia Web Filter for ISA – для Windows, устанавливается как встраиваемый модуль к ISA Server; Proventia Web Filter for Windows – для Windows, выполняет функции прокси-сервера; Proventia Web Filter for Linux – для Linux, выполняет функции прокси-сервера. В России указанное программное обеспечение продвигает компания CPS (http://www.cps.ru/content/view/430/58/).

Proventia Mail Filter – это достаточно полное средство антиспама и фильтрации электронной почты, которое позволяет повысить производительность работы, освобождает ресурсы сети и защищает конфиденциальную информацию. Proventia Mail Filter анализирует входящую и исходящую почту для полной защиты от спама и утечки информации. Кроме спама, программа блокирует вирусы, запрещенные сайты и MP3-файлы.

Достаточно совершенные средства анализа в Proventia Mail Filter сочетаются с базой из более чем 200 тыс. наиболее распространенных примеров спама. Продукт не допускает блокирования нужных писем благодаря использованию 10-ступенчатого анализа письма, включая сравнение сообщения с базой спама и сравнение URL в e-mail-сообщениях с адресами Web-сайтов, занесенными в базу.

Процесс 10-ступенчатого анализа Proventia Mail Filter значительно превосходит аналоги, такие как включение в «черный» список и поиск по ключевым словам. Функция Proventia Mail Filter Spam Learn постоянно обновляет

базу, которая четыре раза в день рассылает обновления конечным пользователям для обеспечения защиты в реальном времени.

Proventia Mail Filter анализирует исходящие e-mail-сообщения и блокирует письма с нежелательным содержимым, сохраняя интеллектуальную собственность и конфиденциальные документы. Программа анализирует текст сообщения, изображения и вложенные документы независимо от формата. Кроме того, она позволяет создавать специальные почтовые политики, устанавливать правила для входящих и исходящих e-mail.

CS MIMEsweeper for Web – средство контроля и разграничения доступа к Web, обеспечивающее в том числе защиту от утечки конфиденциальных материалов через бесплатные интернет-сервисы – Web-почту, чаты и доски объявлений.

Разработчик: Clearswift (www.clearswift.com)

Сайт: http://www.clearswift.com/products/msw/web.aspx

Эта программа защищает от распространения вирусов через Web, от потери конфиденциальной информации, от запрещенного серфинга, от нецелевых скачиваний и помещения нелегальной информации на внешние Web-ресурсы.

Это программное обеспечение вписывается в общую схему комплексного обеспечения безопасности в послойной схеме обеспечения безопасности.

Компания FutureSoft предлагает решение для контентной фильтрации, позволяющие снизить риск правовых нарушений, связанных с незаконным контентом, и оптимизировать пропускную способность сети организации. **DynaComm i:filter** генерирует точные отчеты о нарушении правил посещения запрещенных категорий ресурсов. Система может также выдавать предупреждения в режиме реального времени.

Разработчик: FutureSoft (www.futuresoft.com).

Сайт: http://www.dciseries.com/products/ifilter/

Сегодня в базе п рограммы более 9 млн. сайтов, разбитых на категории, в том числе: Adult (для взрослых), Anti-Social Rhetoric (антисоциальная риторика), Chat Rooms, Forums & Online Communities (чат-комнаты, форумы и онлайновые сообщества), Employment & Jobs (поиск занятости и работы), Entertainment (развлечения), Financial Services (финансовые сервисы),

Gambling (азартные игры), Hacker & Cracker Activities/Information (хакерская и крэкерская информация), Health & Medical (здоровье и медицина), News & Weather (новости и погода), Dating & Personal Web Sites (персональные странички знакомств), Political (политика), Potentially Offensive (потенциально оскорбительные ресурсы), Religion & Spirituality (религиозные и духовные материалы), Reproductive Health & Sexuality (вопросы секса и состояния репродуктивных функций), Shopping (покупки), Sports & Hobbies (спорт и хобби) Terrorism (терроризм), Travel & Tourism (путешествия и туризм).

PureSight Content filtering

Разработчик: PureSight, Inc. (www.icognito.com/company)

Сайт программы: http://www.icognito.com/company/index.shtml

Компания PureSight, Inc. предлагает целый набор решений для контентной фильтрации Web-трафика. Фирменная технология Advanced Content Recognition (ACR) позволяет динамически анализировать и классифицировать Интернет-контент в режиме реального времени и обеспечивает надежную фильтрацию постоянно меняющегося содержания Сети.

PureSight Mobile Content filtering служит для фильтрации Интернет-контента для портативных мобильных устройств, имеющих WAP-функциональность. Технология PureSight Active Content Recognition (ACR) может быть легко интегрирована в мобильные решения, обеспечивая услуги контентной безопасности. Продукт Classification Software Development Kit (CSDK) от PureSight позволяет осуществлять бесшовную интеграцию ACR-технологии в различные прикладные решения, предоставляя возможность интегрировать в различные продукты и службы высококачественные технологии распознавания контента на лету. Решение PureSight Mobile Content filtering снимает головную боль у провайдеров беспроводных служб и подписчиков этих служб на базе анализа, фильтрации и, если необходимо, предотвращения доступа к оскорбительному контенту посредством мобильных карманных беспроводных устройств.

PureSight PC for ISP – решение для фильтра Интернет-контента для ISP, позволяющее пользователям ограничить доступ к Web-ресурсам и управлять им на основе пользовательских списков, создавать до 10 пользовательских профилей (каждый с собственным паролем, логином и индивидуальным профилем

фильтрации), определять различные профили фильтрации. Данное решение дает возможность управлять доступом к Web-ресурсам в зависимости от времени суток. Кроме того, составляются отчеты о том, какой пользователь пытался посетить ту или иную страницу.

Webwasher URL Filter

Разработчик: CyberGuard Corporation (www.cyberguard.com).

Применение Webwasher URL Filter резко сокращает нецелевое использование Web-ресурсов за счет блокировки определенных категорий сайтов, например из разделов Shopping и Entertainment. Система также предотвращает возможность скачивания файлов определенных расширений, в частности MP3.

Smartfilter Web filtering 4.1

Разработчик: Secure Computing Corporation

Сайт: http://www.securecomputing.com/index.cfm?skey=85

Программа защищает организации от рисков, связанных с нерегламентированным использованием Интернета, позволяя повысить безопасность, поднять производительность и ограничить трафик. SmartFilter предоставляет базу данных, содержащую миллионы Web-сайтов, на которые следует ограничивать доступ, по более чем 70 категориям. Над базой работает команда аналитиков с помощью многоязычного анализа Web-ресурсов.

SmartFilter отлично вписывается в сетевую среду организации и работает с большинством популярных прокси-серверов, брандмауэров и аппаратных решений в области безопасности.

Используем встроенные возможности Windows

Встроенные средства Windows позволяют вводить некоторые ограничения, касающиеся работы ребенка на компьютере, – устанавливать временной интервал, в течение которого дети могут пользоваться компьютером, а также определять перечень доступных игр и приложений. Этого может оказаться вполне достаточно для ограничения компьютерной деятельности детей младшего возраста, причем как в образовательной организации, так и на домашнем компьютере.

В Windows10 дополнительно предусмотрен функционал для блокирования доступа к некоторым сайтам и другим интернет-сервисам. Операционная система

Windows 7 встроенного веб-фильтра не имеет – по замыслу разработчиков для организации расширенного родительского контроля в этой ОС предназначена программа Family Safety («Семейная безопасность») из пакета Windows Live Essentials 2011. С ее помощью можно блокировать доступ к нежелательным сайтам, определять контакты, с которыми ребенок может общаться через Интернет (только в Windows Live Hotmail и Windows Live Messenger), и просматривать отчеты о действиях чада в Сети.

Для настройки контроля встроенными средствами Windows необходимо иметь отдельную учетную запись с правами администратора, а также одну (или более, если детей несколько и требуется разграничение прав) учетную запись обычного пользователя, под которой ребенок будет заходить в систему. Разумеется, гостевой профиль должен быть отключен, а на профиль администратора установлен пароль – в противном случае ребенок рано или поздно отключит родительский контроль и будет использовать компьютер безо всяких ограничений.

Технология настройки ограничений никаких сложностей не вызывает – достаточно из панели управления открыть модуль «Родительский контроль», выбрать учетную запись, под которой заходит ребенок, и определить требуемые настройки.

Можно, например, настроить расписание работы по дням недели, что позволит ограничить общее время работы на компьютере, поскольку по окончании разрешенного периода времени будет происходить автоматический выход из системы. Не сложнее окажется отрегулировать доступ к играм, установив на них общий запрет либо запретив доступ только к отдельным установленным на компьютере играм, указав их вручную либо путем выбора возрастной категории (рис. 1).

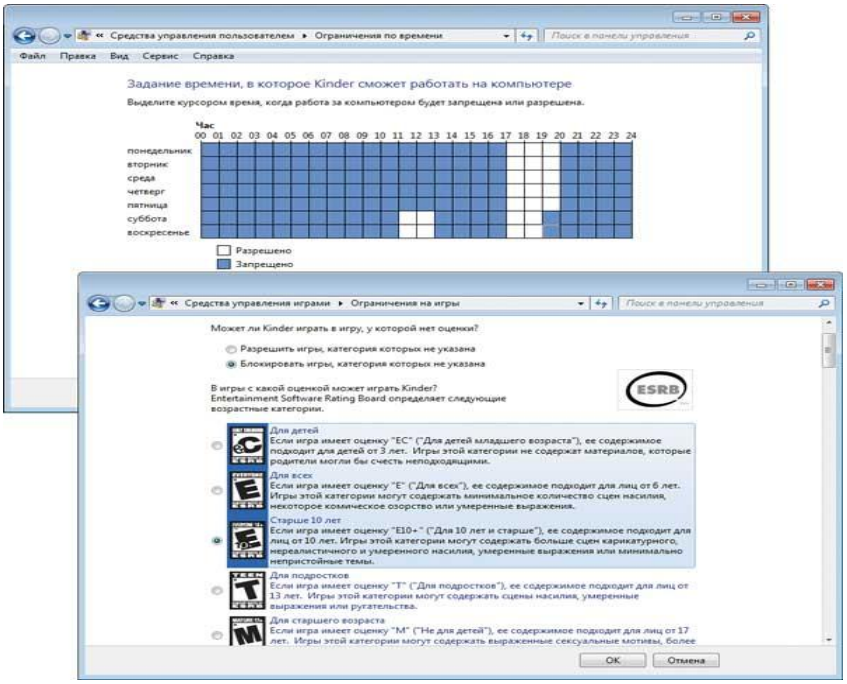

Рис. 1. Установка ограничений на время работы и игры в Windows

Стоит отметить, что полный запрет на игры – вполне разумная мера в образовательной организации, В этом случае у ребенка для работы на компьютере используются два профиля: «Ученик» и «Дополнительное». При этом для профиля «Ученик» полностью запрещен доступ к играм, а для профиля «Дополнительное» установлены четкие временные рамки, что позволяет ограничить время на отдельные компьютерные игры, но разрешить доступ к компьютеру в учебных целях. В дополнение также стоит отметить, что ограничение доступа по времени легко может быть обойдено путем смены компьютерного времени, о чем рано или поздно догадается любой ребенок. Поэтому установка пароля на BIOS – условие обязательное, которое для надежности также может быть подкреплено настройкой синхронизации времени на компьютере с временными серверами в Интернете.

Привлекаем к контролю решения класса Internet Security

Если на компьютере используется комплексный продукт защиты класса Internet Security, то имеет смысл попытаться настроить нужный вариант ограничений с помощью модуля контроля, который сегодня является обязательным компонентом таких решений. Данный вариант тем более привлекателен, что наиболее популярный среди российских пользователей в этом классе инструмент – Kaspersky Internet Security 2012 – недавно был признан лучшим в тестах контроля Anti-Malware.ru в плане эффективности блокирования ресурсов нежелательной тематики.

Kaspersky Internet Security 2012

Сайт: http://www.kaspersky.ru/kaspersky_internet_security

Kaspersky Internet Security – ориентированный на обычных пользователей инструмент для многоуровневой защиты от всех интернет-угроз: вирусов, хакерских атак и спама. Данное решение базируется на параллельном использовании «облачных» и традиционных антивирусных технологий, что позволяет достичь максимального уровня безопасности компьютера. Продукт включает в себя базовые инструменты обеспечения антивирусной безопасности, а также большой набор дополнительных модулей. В их числе – безопасная среда запуска приложений и браузеров, монитор активности программ, сетевой экран, контроль и т.д. Входящий в состав продукта модуль «Родительский контроль»

позволяет регулировать доступ детей к веб-сайтам и их общение в социальных сетях («ВКонтакте», «Одноклассники.ру», Facebook, Twitter и др.) и через программы обмена сообщениями (ICQ и др.), а также ограничивать время доступа к компьютеру и отдельным приложениям.

Несложно ввести ограничения на доступ к веб-сайтам (рис. 2) в зависимости от их содержимого. Настраивается система ограничений путем выбора категорий веб-сайтов, доступ к которым следует заблокировать, формирования списка исключений (при необходимости) и включения/отключения режима безопасного поиска, который будет применяться во время работы пользователя с поисковыми системами (для Google и Bing.com).

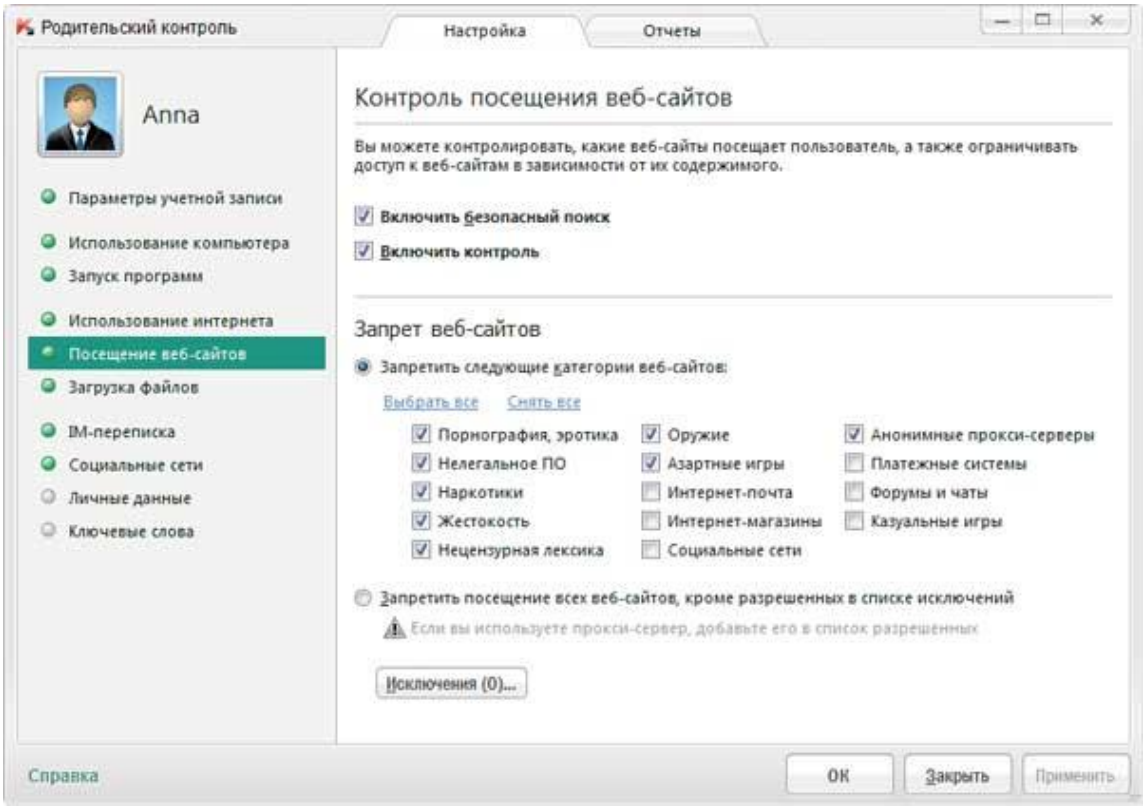

Рис. 2. Настройка контроля посещения веб-сайтов в Kaspersky Internet Security

Кроме того, разрешается ограничивать загрузку определенных типов файлов и осуществлять контроль переписки через интернет-пейджеры и в социальных сетях путем блокирования переписки с контактами, с которыми общение запрещено. Предусмотрен мониторинг переписки с учетом употребления указанных родителем конкретных слов и блокирование пересылки данных, содержащих персональную информацию (например, домашний адрес, номер телефона). Все действия

пользователей, для которых настроен родительский контроль, фиксируются в детальных отчетах по всем категориям контролируемых событий.

Подключаемся к сервисам облачной контентной фильтрации

При необходимости настройки домашнего компьютера на блокирование веб-страниц, содержащих порнографию, рекламу наркотиков, пропаганду расовой ненависти, насилия и пр., возможным вариантом может стать подключение к специализированному сервису фильтрации. Таких сервисов в Сети довольно много, но мы остановимся на ContentKeeper Home и SkyDNS, поскольку эти сервисы также показали в тестах Anti-Malware.ru впечатляющие результаты.

ContentKeeper Home

Разработчик ContentKeeper Technologies

(www.contentkeeper.com)

Сайт: https://home.contentkeeper.com/

ContentKeeper Home – «облачная» система фильтрации веб-контента, которая ориентирована на домашних пользователей. Данная система обеспечивает очень высокое качество фильтрации при минимальной нагрузке на ресурсы компьютера, что является результатом применения технологии SaaS (Software as a Service), в которой основная функциональность выполняется в «облаке» на специальных серверах ContentKeeper. Система фильтрации ContentKeeper Home предлагается на коммерческой основе, для ознакомления доступна бесплатная лицензия сроком на один месяц. Данное решение позволяет родителям легко отслеживать, управлять, контролировать и обеспечивать безопасность работы в Интернете для всех членов семьи. Контроль осуществляется путем блокирования доступа к неподходящему или вредному контенту и ресурсам, содержащим ключевые слова из списка ключевых слов, ограничения доступа к программам чатов (Google Talk, MSN Messenger, Yahoo Messenger и др.) и к определенным типам файлов (аудио и видеофайлы, приложения и пр.). К сожалению, популярные в России программы чатов (ICQ, Miranda, QIP) не поддерживаются, зато список доступных для блокирования типов файлов внушителен.

Администрирование ContentKeeper Home осуществляется через веб-интерфейс и может производиться локально либо в удаленном режиме. Для настройки

параметров фильтрации необходимо зайти на сервис, зарегистрироваться в панели управления под своей учетной записью и установить ограничения. Настройка производится для каждой из имеющихся учетных записей по отдельности, а это значит, что для детей и родителей могут быть определены разные политики доступа. Самый быстрый способ установить ограничения по конкретной учетной записи – выбрать один из предустановленных профилей настроек. Предусмотрена также возможность создания пользовательских наборов фильтров, что позволяет решать конкретные задачи ограничения доступа.

Готовых профилей доступа четыре:

– Education Only – работа только с образовательными ресурсами;

– No Facebook Or MySpace – блокирование доступа к социальным сетям;

– Block All Access – полное блокирование доступа в Интернет;

– Default – блокирование сайтов с порнографией, азартными играми и ресурсов, связанных с наркотиками.

Конфигурация любого из предустановленных профилей может быть изменена. Например, несложно открыть или закрыть доступ к ресурсам конкретных категорий, определить режим работы для программ чатов (запретить, разрешить или разрешить с ведением отчета о сообщениях) и установить для конкретных поисковых систем режим безопасного поиска (Yandex.ru, Rambler.ru и Mail.ru не включены). Можно также создать белый и черный списки ресурсов, включить или отключить блокировку сайтов по ключевым словам и разрешить либо запретить загрузку определенных типов файлов.

SkyDNS

Разработчик: ООО «СкайДНС».

Сайт программы: https://www.skydns.ru/

SkyDNS – «облачный» российский сервис интернет-фильтрации на уровне DNS-запросов, который обеспечивает блокирование опасных и нежелательных для просмотра детьми сайтов. Данный сервис был запущен в 2010 году и в настоящее время работает в нескольких режимах – бесплатном Free (с ограниченным функционалом) и трех коммерческих: «Премиум», «Школа» и «Бизнес». Для настройки блокирования сайтов, нежелательных для просмотра детьми,

предназначены тарифы «Премиум» и «Школа». Тариф «Школа» ориентирован на использование в учебных заведениях и не имеет ограничений на число защищаемых компьютеров. Возможности обоих тарифных планов обеспечивают блокирование разнообразных нежелательных ресурсов (содержащих порнографию, рекламу наркотиков, пропаганду расовой ненависти, агрессии и пр.), а также позволяют защитить компьютер от сайтов, замеченных в распространении вирусов и фишинге, ограничить доступ к социальным сетям, форумам и др.

Настройка защиты компьютера через сервис SkyDNS не совсем очевидна, хотя и занимает в целом немного времени. На первом этапе нужно зарегистрироваться на сервисе, войти на сайт SkyDNS под своим аккаунтом, перейти на вкладку «Фильтр» и указать категории, которые необходимо заблокировать. После этого можно дополнительно отрегулировать доступ на уровне отдельных сайтов (то есть с обходом настроек общего фильтра) на вкладке «Исключения». В принципе сервис может работать и без регистрации, но в анонимном режиме обеспечивается только фильтрация от сайтов, распространяющих вирусы, а также от фишинговых ресурсов. Стоит отметить, что в платных тарифах предусмотрено использование профилей фильтрации, позволяющих устанавливать разные правила фильтрации в рамках одного аккаунта (например, для детей и взрослых).

Альтернативным вариантом организации контроля может стать использование специализированных программных продуктов. Подобных решений на рынке представлено очень много, а их функциональность может быть самой разной. Остановимся на двух разноплановых продуктах от российских разработчиков – Time Boss и KinderGate Родительский контроль.

Time Boss 2.5

Разработчик: компания NiceKit Software (www.nicekit.ru).

Сайт программы: http://nicekit.ru/parental-control/time-boss.php

Time Boss – простая и удобная программа для организации контроля. С ее помощью учителя и родители легко могут ограничивать время компьютерной деятельности ребенка (в том числе в играх и нахождение в Интернете), определять

перечень доступных приложений (включая игры), вводить ограничения на ряд системных операций, запрещать доступ к отдельным папкам, а также регулировать посещение сайтов при интернет-серфинге. Программа обеспечивает контроль для всех зарегистрированных в системе пользователей и потому при необходимости может быть использована для настройки разных вариантов ограничений по различным профилям. В целях защиты от взлома подрастающим поколением разработчики предусмотрели ряд возможностей: использование пароля доступа к программе, работу в скрытом («Стелс») режиме, защиту от удаления приложения при загрузке Windows в безопасном режиме Safe mode и др. Приложение предлагается в двух редакциях: базовой Time Boss и расширенной Time Boss PRO. Редакция Time Boss PRO дополнительно предоставляет функционал для удаленного управления в рамках локальной сети (можно удаленно менять настройки, оперативно добавлять время и пр.) и оснащена защитой от кейлоггеров (чтобы исключить возможность получения ребенком пароля доступа к программе).

Принцип использования Time Boss очень прост – для каждого пользователя Windows создаются профили типов «Учитель» и «Ученик». Пользователям типа «Ученик» настраивается компьютерное расписание, которое позволит четко определить часы для работы на компьютере в целом, а также в Интернете и с конкретными приложениями путем управления белыми и черными списками. Последнее окажется полезным для ограничения игровой деятельности – игры можно вовсе запретить, указав их в черном списке, либо разрешить только по вечерам – то есть после подготовки домашних заданий. В ходе настройки расписания разрешается не только устанавливать временны*е* интервалы, но и указывать общее допустимое количество компьютерного времени на день, а также вводить при работе принудительные перерывы. При необходимости также можно вводить системные ограничения, например, отключить панель управления и заблокировать запуск системного реестра, запретить изменение даты и времени, отключить модуль «Установка и удаление программ», сделать невидимыми отдельные диски, защитить от изменений папки и др.

При желании можно попытаться предотвратить посещение ребенком нежелательных сайтов при интернет-серфинге. Правда, возможности тут ограничены блокированием по ключевым словам (задействованы ключевые слова

для базовых категорий) и с учетом черного и белого списков, что, впрочем, не мешает ограничить ребенку посещение социальных сетей (например, указав для ресурса *.vkontakte.ru максимальный лимит допустимого времени) и пр. К сожалению, интернет-фильтр работает только с IE, запуск других браузеров необходимо отключить.

KinderGate Родительский Контроль 1.2

Разработчик Entensys Corporation (www.entensys.com).

Сайт программы: http://www.kindergate.ru/

Программа «KinderGate Родительский Контроль» – инструмент для организации контроля доступа детей в Интернет, рассчитанный на домашних пользователей и образовательные организации. Данное решение позволяет блокировать нежелательный контент (поддерживается URL-фильтрация по черным или белым спискам и фильтрация по категориям), вредоносные сайты, а также прокси-серверы и сайты анонимайзеры, через которые можно было бы обойти подобную блокировку. В целях защиты от взлома юными хакерами предусмотрено обязательное использование пароля для доступа к программе. Решение включает функционал для мониторинга действий ребенка в Сети: отслеживание посещаемых ресурсов при серфинге, мониторинг сообщений в сетевых мессенджерах (поддерживаются протоколы ICQ, Jabber, MSN, Mail.ru, YMSG) и наблюдение за перепиской ребенка в социальных сетях «ВКонтакте», «Одноклассники» и Facebook. Кроме того, предусмотрен инструментарий для запрета загрузки разных видов контента (видео, аудио, изображения и пр.), настройки расписания доступа в Интернет и блокировки контекстной рекламы и баннеров.

В техническом плане использование программы «KinderGate Родительский Контроль» сложностей не вызывает. Предполагается, что домашний компьютер, на который собираются устанавливать это решение, используется преимущественно ребенком; при необходимости работы учителей и родителей систему контроля временно отключают путем запуска окна программы (естественно, требуется знание пароля). Для настройки ограничений необходимо сделать простые настройки. Например, для настройки фильтрации сайтов по их содержимому достаточно

активировать вкладку «Запрет категорий» и перетащить бегунок на нужный уровень блокирования. Столь же несложно ввести запрет на загрузку определенного типа файлов и конкретных ресурсов, а также настроить режим доступа в Интернет по времени или календарю. Допускается использование и более сложных правил фильтрации – скажем, можно запретить категорию «Веб-почта», но разрешить доступ к ресурсу mail.yandex.ru в качестве исключения. При необходимости можно включить функцию «Безопасный поиск» (позволяет заблокировать запросы сомнительного характера в поисковых системах Яндекс, Google и др.) и режим морфологического анализа ресурсов (обеспечивает блокирование веб-страниц с запрещенными словами), а также настроить запись мгновенных сообщений. Вся деятельность ребенка в Интернете фиксируется в логах и отображается в виде отчетов (посещаемые ресурсы, трафик, заблокированные сайты).

Программа фильтрации Голкипер

Разработчик: Центр Анализа Интернет Ресурсов
(www.cair.ru).

О программе СКФ «Голкипер»:
http://www.dvpt.ru/?page=event016

СКФ «Голкипер» – Российская система контентной фильтрации, использующая эффективные алгоритмы работы и настроенная на русскоязычный контент. Программа, в первую очередь, предназначена для нужд российских образовательных организаций, а также организаций, обеспечивающих публичный доступ в Интернет.

Возможности Голкипера: работа с ресурсами на русском и иностранных языках, наравне с отличной способностью анализировать русскоязычный контент, Голкипер также работает с другими основными языками мира, распределяя ресурсы по 48 категориям, которые охватывают более 200 тем.

Отчеты о доступе пользователей: различные типы отчетов позволяют получить детальную статистику об использовании Интернет от детализированного отчета по сайту до общих отчетов об активности использования Интернет.

Модуль сбора и обработки статистики: Голкипер представляет уникальный инструмент для сбора и представления статистики в больших территориально-распределенных организациях с помощью специализированного модуля сбора и обработки статистики обращений пользователей, собираемых локальными контентными фильтрами, установленными в удаленных подразделениях организации.

Автоматическое обновление базы URL: Голкипер избавляет от дополнительной работы по обслуживанию, производя автоматическое обновление базы URL, списка категорий и других параметров.

Контентная фильтрация почтового трафика на уровне сети: электронная почта является одним из главных Интернет-сервисов (ежедневно в мире отправляется десятки млрд. электронных посланий) и одновременно является источником многочисленных проблем: спам, вирусы, распространение запрещенной информации. Спамеры пытаются обмануть фильтры, придумывают новые формы сообщений, невидимые для фильтров, в надежде сохранить свой бизнес. В результате идет эволюция спам-фильтров и параллельно эволюционируют средства доставки спама, а оплачивается этот процесс на деньги, получаемые от e-mail-пользователей. Проблема состоит еще и в том, что спам тоже разнороден: одни сообщения представляют угрозу заражения вирусами и троянцами, другие просто отвлекают пользователей, поскольку маскируются под важные для них сообщения, третьи, не выдаваемые за что-то другое, не отнимают у получателей много времени.

Таким образом, решение вопроса противодействия антиспаму (как и антивирусу) нельзя создать раз и навсегда – это результат непрерывного процесса накапливания сведений о спаме, его анализа и модернизации улавливающих его фильтров.

3. Регламент по работе в сети Интернет и по работе с электронной почтой

Нормативно-правое обеспечение является основой деятельности образовательной организации по всем направлениям, в том числе и по работе с Интернет. В образовательной организации должен быть сформирован пакет нормативной правовой документации федерального, регионального, муниципального и локального уровней по вопросам информационной безопасности.

К таким документам относятся положения и регламенты по работе в сети Интернет как педагогических работников, так и школьников, документы по контентной фильтрации, по обработке персональной информации, различные положения об организации профилактической работы по медиабезопасности, о формах профилактической работы с детьми и родителями по Интернет-безопасности, правила безопасного поведения в сети Интернет. В образовательной организации приказами должны быть назначены лица, ответственные за организацией работы школьников в сети Интернет, за контентную фильтрацию, за работу с персональными данными и т.д.

В организационном плане по обеспечению информационной и медиабезопасности в образовательной организации должен выполняться ряд **мер технико-технологической направленности**:

– установка только лицензионного программного обеспечения;

– подключение к системе контентной фильтрации;

– установка антивирусных программ;

– установка и настройка программ-фильтров, брандмауэров.

К **организационным внутришкольным мероприятиям** можно отнести:

– разработка и реализация правил Интернет-безопасности, с привлечением заинтересованных лиц: директора школы, классных руководителей, преподавателей информационных технологий, самих учащихся и их родителей, поставщиков услуг интернета;

– организация работы детей в Интернет по расписанию с ограничением по времени под наблюдением педагогических работников;

– регулярная проверка принимаемых мер в области Интернет безопасности в образовательной организации.

Для организации **профилактической работы** по медиабезопасности с детьми и родителями педагогический работник должен знать проблемы и опасности, которые подстерегают пользователя в сети Интернет, и быть готов дать рекомендации по решению данных проблем.

Для организации профилактических мер в образовательной организации необходимо периодически проводить мониторинг, диагностику проблем по Интернет-безопасности среди детей и родителей.

В аспекте **программно-методического обеспечения** в образовательной организации должна быть разработана программа (раздел, модуль комплексной программы по профилактике девиантного поведения детей), в которую должны быть включены темы по медиабезопасности, о безопасном поведении в сети Интернет. Такие же темы и проблемы должны включаться в программы воспитательной деятельности.

Рекомендуемая тематика для организации профилактической деятельности:

– нежелательная информация в Интернете, как ее избежать;

– проблемы достоверности информации в Интернете, как проверить достоверность информации;

– социальные сети: опасности и правила поведения в социальных сетях;

– кибермошенничества, как избежать кибермошенников;

– киберхулиганство, киберзапугивание, правила поведения в опасной виртуальной ситуации;

– вредоносные программы, методы борьбы с ними;

– полезные ссылки, ресурсы, сервисы в Интернете.

Информационная безопасность в Интернете может обсуждаться во время уроков информатики, социологии, ОБЖ, права и др. В образовательной организации рекомендуется проводить день медиабезопасности, уроки по Интернет-безопасности, внеклассные мероприятия и т.п.

Тематика проведения различных школьных мероприятий по интернет-безопасности может быть самой разнообразной, например:

– противозаконная, неэтичная и вредоносная информация в Интернете: как ее избежать;

– достоверность информации в интернете, проблемы и способы проверки информации на достоверность и полноту;

– этика сетевого общения;

– личная информация: нужна ли она в интернете, как защитить личную информацию в блогах, социальных сетях и пр.;

– социальные сети: как общаться в сети и не попасть в сети мошенников и злоумышленников;

– что такое хакерство: этика и основы;

– интернет-зависимость: угрозы, реальность, проблемы, решения;

– Web-серфинг: как не потерять себя и свое время в Интернете;

– как распознать кибермошенничество и не стать жертвой;

– что такое киберхулиганство: как не стать жертвой и киберхулиганом;

– как защитить свою почту от спама и не стать спамером;

– компьютерные вирусы и методы борьбы с ними;

– киберпреступления в законодательстве России;

– безопасность в коммерческих интернет-сервисах: интернет-магазины, услуги различных фирм и др.;

– компьютерные игры, как не стать игроманом;

– мобильные угрозы в современном мире;

– как правильно вести себя с киберхулиганами и защититься от нежелательного общения, и другие.

Большое значение для эффективности мероприятий по интернет-безопасности имеет не только содержание, но и форма его проведения.

Можно рекомендовать следующие формы:

1-4 классов – урок-путешествие, урок-викторину, урок-соревнование, урок-игру, беседу;

5-8 классов – урок-пресс-конференцию, урок-викторину, урок-соревнование, урок-презентацию проектов, урок-практикум, урок-встречу со специалистами медиа-сферы (системными администраторами) и т.д.;

9-11 классов – деловую игру, урок-презентацию проектов, день интернет-безопасности, мозговой штурм, дискуссию, дебаты, встречу со специалистами медиа-сферы (системными администраторами) и т.д.

4. Полезная информация

Зависимость от компьютерных игр (кибераддикция).

Кибераддикция подразделяется на группы в зависимости от характера той или иной игры:

1. Ролевые компьютерные игры (максимальный уход от реальности).
2. Неролевые компьютерные игры

(стремление к достижению цели – пройти игру, азарт от достижения цели, набора очков).

<u>Признаки компьютерной зависимости</u>:

- ✓ значительное улучшение настроения от работы за компьютером;
- ✓ нежелание оторваться от работы или игры на компьютере;
- ✓ если Вы отрываете ребенка от компьютера, он испытывает раздражение, даже проявляет некоторую агрессию по отношению к Вам;
- ✓ неспособность спланировать окончание игры на компьютере;
- ✓ пренебрежение домашними делами в пользу компьютера;
- ✓ пренебрежение личной гигиеной и сном в пользу компьютера;
- ✓ при общении с окружающими сведение любого разговора к компьютерной тематике;
- ✓ отказ от общения с друзьями.

Можно наблюдать и некоторые **физические отклонения ребенка**, страдающего компьютерной зависимостью: нарушение зрения, снижение иммунитета, головные боли, повышенная утомляемость, бессонница, боли в спине, туннельный синдром (боли в запястье).

Так как первопричиной ухода ребенка из реального мира является неудовлетворенность существующей действительностью, необходимо в первую очередь выяснить, что же побудило ребенка уйти «в компьютер».

Неправильно критиковать ребенка, проводящего слишком много времени за компьютером.
Если Вы видите у ребенка признаки компьютерной зависимости, не обостряйте ситуацию, отведите его к психотерапевту.
Можно попытаться вникнуть в суть игры, разделив интересы ребенка, это сблизит ребенка с родителями, увеличит степень доверия к ним.
Рекомендуется ограничивать доступ детей к играм и фильмам, основанным на насилии.

Приложение № 1

**Примерный классификатор информации,
несовместимой с задачами образования и воспитания
в соответствии с законодательством Российской Федерации**

№ п/п	Тематическая категория	Содержание
1.	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	– 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 –	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или)

№ п/п	Тематическая категория	Содержание
	скрытое воздействие	оказывающая вредное влияние на их здоровье
6.	Экстремистские материалы или экстремистская деятельность (экстремизм)	а) экстремистские материалы, то есть предназначенные для обнародования документы или информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие 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; б) экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: – 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

№ п/п	Тематическая категория	Содержание
		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 его государственной или иной политической деятельности либо из мести за такую деятельность; – 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	– 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 ниже 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 образовательной организации.

№ п/п	Тематическая категория	Содержание
1.	Алкоголь	Реклама алкоголя, пропаганда потребления алкоголя. Сайты

№ п/п	Тематическая категория	Содержание
		компаний, производящих алкогольную продукцию
2.	Баннеры и рекламные программы	Баннерные сети, всплывающая реклама, рекламные программы
3.	Вождение и автомобили (ресурсы, не имеющие отношения к образовательному процессу)	Информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям
4.	Досуг и развлечения (ресурсы, не имеющие отношения к образовательному процессу)	– фотоальбомы и фотоконкурсы; – рейтинги открыток, гороскопов, сонников; – гадания, магия и астрология; – 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, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.; – о дачах, участках, огородах, садах; – о рукоделии, студенческой жизни, 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, 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, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу компьютерные онлайновые и оффлайновые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты
7.	Корпоративные сайты, интернет-представительства негосударственных учреждений	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций
8.	Личная и немодерируемая информация	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги

№ п/п	Тематическая категория	Содержание
9.	Отправка SMS с использованием интернет-ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
10.	Модерируемые доски объявлений (ресурсы, 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, 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, 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, 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

№ п/п	Тематическая категория	Содержание
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, 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, е-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.

Приложение № 2

Сравнительный анализ программных продуктов, осуществляющих контент-фильтрацию доступа к сети Интернет, реализованных Министерством образования и науки Российской Федерации

Характеристики	***Internet Censor***	***NetPolice pro***	***Content Keeper***	***KidGid***	***ChildWebGuardian***
Обеспечивать беспрепятственный доступ к информации, распространение которой в РФ в соответствии с законодательством не ограничивается или не запрещается	+	+	+	+	+
Обеспечить возможность адаптации к изменяющимся угрозам, условиями эксплуатации, требованиям законодательства РФ предписаниям надзорных органов	+	+	+	+	+
Обеспечить фильтрацию контента по спискам категорий, рекомендо-	+	+	+	-	+

ванным 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 образователь-ном процессе в целях обучения и воспитания учащихся	+	+	-	-	+
Возможность установки на каждый компьютер	+	+	+	+	+
Интерфейс (язык)	русский	русский	русский	русский	русский
Стоимость	бесплатная	платная	платная	платная	платная
Операционная система	Windows 7, XP, Vista, Linux	Windows 7, XP, Vista, Linux	Windows 7, XP, Vista, Linux	Windows 7, XP, Vista, Linux	Windows 7, XP, Vista, Linux
Сайт программы	**http://icenor.ru/**	**www.netpolice.ru**	**www.contentkeeper.com**	**www.kidgid.com**	**www.childwbguardian.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 выделенного сервера	+	+	+
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	www.skydns.ru	http://rejector.ru	www.opends.com
DNS	193.58.251.251	95.154.128.32 91.196.139.174	208.67.222.222 208.67.220.220

Приложение № 3

Правила использования сети Интернет в образовательной организации
(примерные)

1. Общие положения

1.1. Настоящие Правила регулируют условия и порядок использования сети Интернет в образовательной организации (ОО).

1.2. Настоящие Правила имеют статус локального нормативного акта образовательной организации.

1.3. Использование сети Интернет в образовательной организации направлено на решение задач учебно-воспитательного процесса.

2. Организация использования сети Интернет в общеобразовательной 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 вводится в действие приказом руководителя ОО.

2.2. Правила использования сети Интернет разрабатывается 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 ОО;

– 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 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 ОО следует осознавать, что ОО не несет полной 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 техническим 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 образовательном учреждении

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.

Приложение № 4

Примерная инструкция
для сотрудников образовательной организации о порядке действий при осуществлении контроля использования обучающимися сети Интернет

1. Настоящая инструкция устанавливает порядок действий сотрудников образовательных организаций 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 Интернете 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.