Администрации МР «Табасаранский район»
информационно-аналитический отдел

Методические рекомендации

по защите детей от негативной информации в сети Интернет

с. Хучни 2015 г.

В последнее десятилетие вопросы обеспечения благополучного и защищенного детства стали одними из основных национальных приоритетов Российской Федерации.

В результате значительного повышения обеспеченности россиян компьютерами и подключения в рамках национального проекта школ к сети «Интернет» пользовательская активность российских школьников резко возросла.

Бесспорно Интернет - это наш сегодняшний день и при правильном использовании - это возможность получать новые полезные знания. Однако, всего 44% несовершеннолетних используют Интернет как источник информации для учебы.

В силу отсутствия жизненного опыта, неокрепшей психики, ребенок более других подвержен воздействию через компьютерные игры, мобильную связь, рекламу, и особенно, через всемирную паутину сети «Интернет».

В Федеральном законе от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию, введено понятие информационной безопасности детей, рассмотрены виды информации, причиняющей вред здоровью и (или) развитию детей».

Комплекс мер, направленных на обеспечение информационной безопасности детства, закреплен в «Национальной стратегии действий в интересах детей на 2012-2017 годы», утвержденной указом Президента РФ от 01.06.2012 №761 (далее - Национальная стратегия действий в интересах детей),

С позиций системы образования информационная безопасность обучающихся - это необходимость:

1. обеспечивать достаточные и защищенные информационные ресурсы и информационные потоки для поддержания образовательного процесса на соответствующем уровне;
2. противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику обучающихся;

Таким образом, информационная безопасность детей включает две относительно самостоятельные составляющие - гуманитарную и техническую. *Техническая составляющая* включает организационно-правовые механизмы и технические средства защиты.
Гуманитарная составляющая включает содержание и организацию образовательного процесса, подготовку педагогов.

Проблема защиты детей от информации, причиняющей вред их здоровью и развитию, в Российской Федерации регулируется следующими нормативно правовыми актами:

- Конституция РФ от 12.12.1993;
- Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе»;
- Федеральный закон от 25.07.2002 №114-ФЗ «О противодействии экстремистской деятельности»;
- Указ Президента РФ от 01.06.2012 г. № 761 «О Национальной стратегии действий в интересах детей на 2012-2017 годы»;
- Правила подключения общеобразовательных учреждений к единой системе контент- фильтрации доступа к сети Интернет, реализованной Минобрнауки РФ от 11.05.2011 №АФ-12/07 вн. На уровне Образовательной организации

1. Вопросы использования возможностей сети «Интернет» в образовательном процессе рассмотреть на педсовете;
2. Издать приказы по вопросам обеспечения информационной безопасности обучающихся;
3. *Разработать локальные акты (Регламент доступа в сеть «Интернет», Правила использования сети «Интернет», Положение о Совете образовательной организации по вопросам регламентации доступа к информации в сети «Интернет» и др.);*
4. *Разработать или внести необходимые дополнения в должностные инструкции (сотрудника,*

назначенного ответственным за организацию работы с сетью «Интернет» и контроль доступа в сеть; учителя, допущенного к работе в сети);

5. Разработать и внедрить программы обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет- зависимости, предупреждения рисков вовлечения в противоправную деятельность.

Внешняя защищенность образовательной среды реализуется через:

- Создание системы контентной фильтрации, которая представляет собой программный комплекс, позволяющий ограничить учащимся доступ к интернет-ресурсам;
- Использование различных систем противовирусной защиты;
- Использование специальных настроек операционной системы;
- Установку поисковых систем для детей.

В качестве дополнительных средств контентной фильтрации я предлагаю использовать следующий программный продукт:

Интернет Цензор

Программа «Интернет Цензор» предназначена для предотвращения посещения сайтов, противоречащих законодательству РФ, а также любых сайтов деструктивной направленности лицами моложе 18 лет. Программа обеспечивает родителям полный контроль за деятельностью в сети их детей.

Основной функцией «Интернет Цензора» является блокирование доступа к интернет-сайтам, которые не входят в разрешенную белую базу сайтов, составленную и предложенную компанией-разработчиком, а также в список, составленный самими родителями. База сайтов, разрешённых компанией к посещению, постоянно обновляется. Обновления скачиваются программой с сервера компании автоматически раз в день. В дополнение к этому пользователь может воспользоваться кнопкой «Проверить обновления» в интерфейсе программы.

Белый список в интерфейсе программы родители заполняют самостоятельно после скачивания и установки программы на домашний компьютер. Этот список для программы важнее, чем база компании-разработчика. При работе «Интернет Цензор» сначала обращается к «родительскому» списку разрешённых адресов. Кроме того, владелец программы может создать чёрный список ресурсов и запретить посещение сайтов, доступ к которым разрешён компанией-разработчиком. Таким образом, ваши запреты или разрешения будут приниматься во внимание в первую очередь.

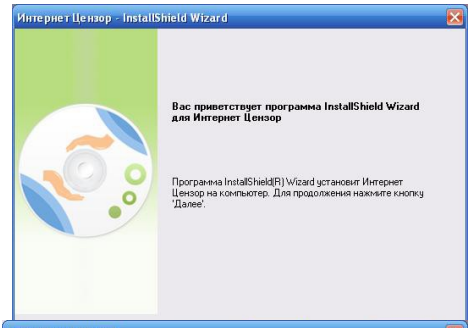
При включении режима фильтрации вместо запрещенных к просмотру ресурсов ваш браузер будет показывать страницу-заменитель. В случае, если на разрешенном ресурсе есть нежелательные элементы, замене подвергнется лишь часть страницы – та, что содержит части, не допущенные к просмотру.

Замечание! В работе программы есть некоторые особенности. Это обстоятельство связано с тем, что мы предоставляем мощную защиту, не допускающую «пробоев» в фильтрации. Во время работы уже установленного «Интернет Цензора» если вы включили или выключили фильтрацию «Интернет Цензора», добавили сайты в чёрный или белый списки, то не забудьте закрыть и открыть заново все окна интернет-браузера (Internet Explorer, Google Chrome, Mozilla Firefox и др.)

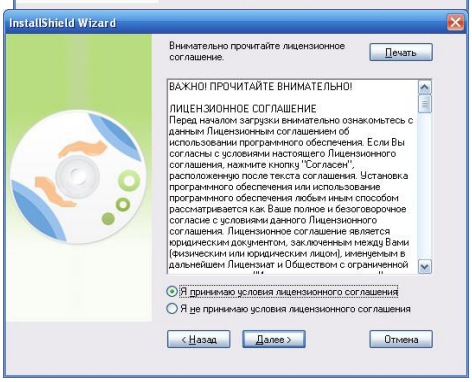
Установка программы

Вы скачали программу «Интернет Цензор» с сайта нашей компании. Для установки программы на вашем компьютере запустите приложение InternetCensor. exe.

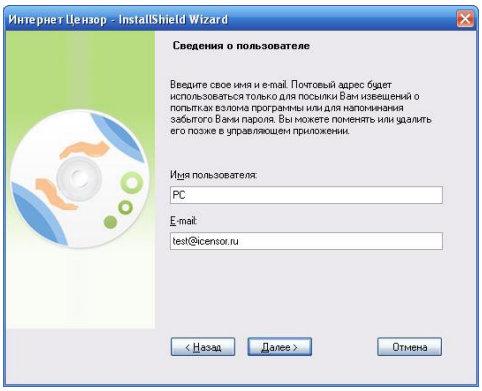
В появившемся окне нажмите кнопку **«Далее»**:



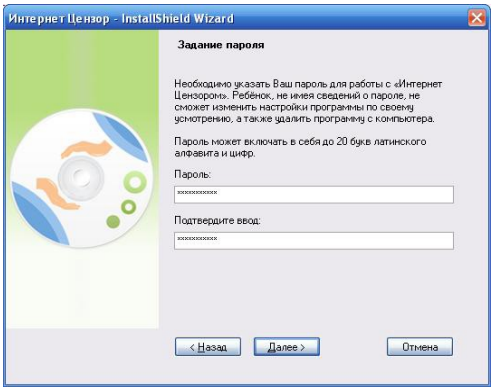
Ознакомьтесь с лицензионным соглашением, выберите пункт «Я принимаю условия лицензионного соглашения» и нажмите кнопку **«Далее»:**



Введите имя пользователя и адрес электронной почты и нажмите кнопку **«Далее»**:
Внимание! Указывайте действительный адрес электронной почты, поскольку данный адрес будет использоваться для напоминания пароля.

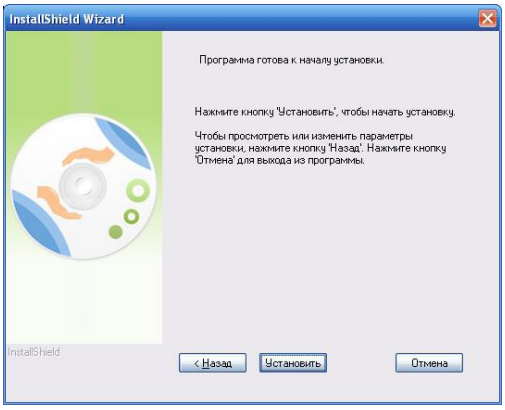


Далее, установите пароль на доступ к программе нажмите кнопку **«Далее»:**



Нажмите кнопку «Далее», что бы установить программу в стандартную папка **Program Files**:

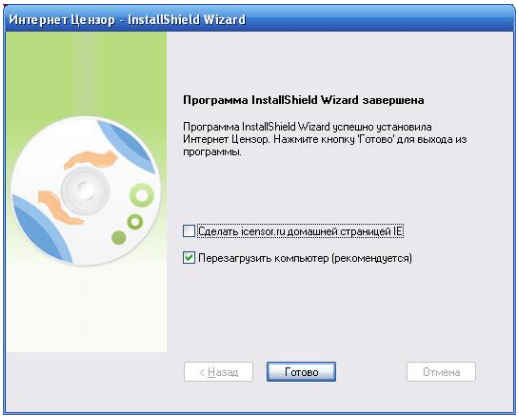
Нажмите кнопку **«Установить»** для запуска установки:



Внимание! В процессе установки программы происходит разрыв интернет соединения. Вы сможете восстановить соединение после установки программы.

Снимите галочку с пункта «Сделать icensor домашней страницей»

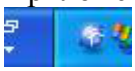
Нажмите кнопку **«Готово»** для перезагрузки компьютера:



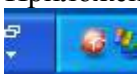
Запуск программы

Приложение запускается по умолчанию при включении компьютера. При «сворачивании» окна с программой её значок остаётся на панели инструментов. Цвет значка указывает на активность программы.

Приложение в «свернутом» виде – фильтрация ВКЛЮЧЕНА.



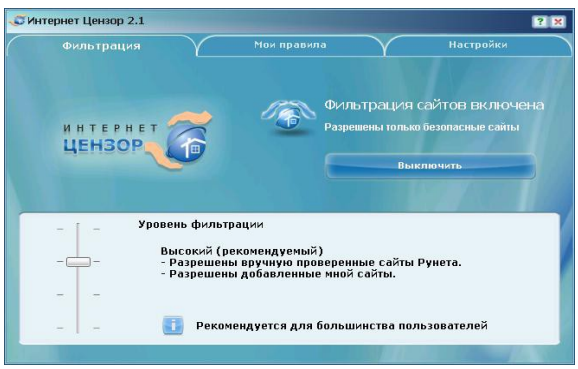
Приложение в «свернутом» виде – фильтрация ВЫКЛЮЧЕНА.



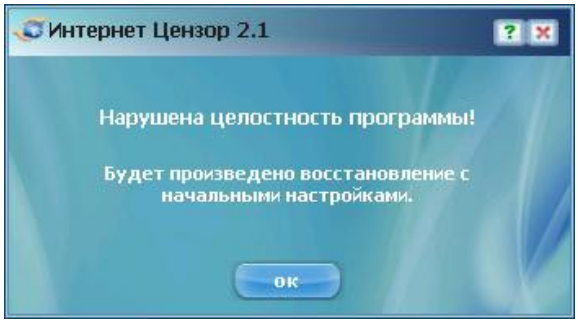
Чтобы открыть управляющее приложение, курсором мыши выберите изображение программы в панели инструментов и сделайте клик левой клавишей.

Перед вами появится окно с вводом пароля:

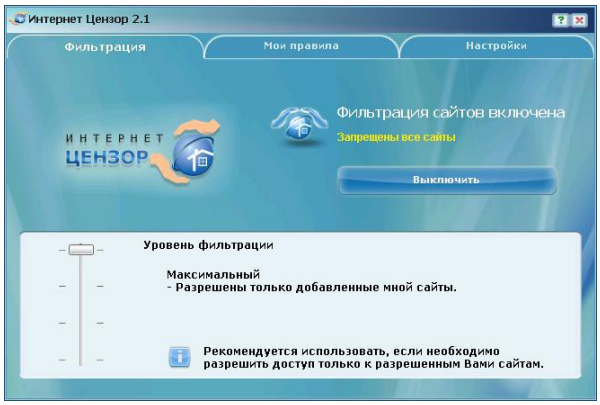
Введите пароль, который вы указали при установке программы.
Если вы забыли пароль, кликните по надписи «Напомнить пароль» для восстановления пароля на электронную почту.
Если введён правильный пароль, откроется окно программы:



Если значок свёрнутой программы мигает, меняя цвет с синего на красный, то это сигнал о том, что была попытка взлома программы (ребёнок пытался удалить или вывести из строя «Интернет Цензор»). В этом случае на почтовый адрес, введённый вами при установке программы, будет отправлено соответствующее оповещение. Если вы кликнете на значок приложения, то откроется такое окно:

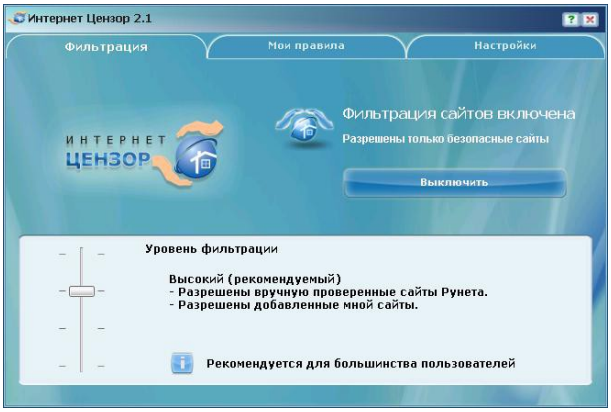


Следуйте инструкции, которую вы видите в окне программы. Управляющее приложение поможет вам настроить программу «Интернет Цензор» под конкретные потребности.



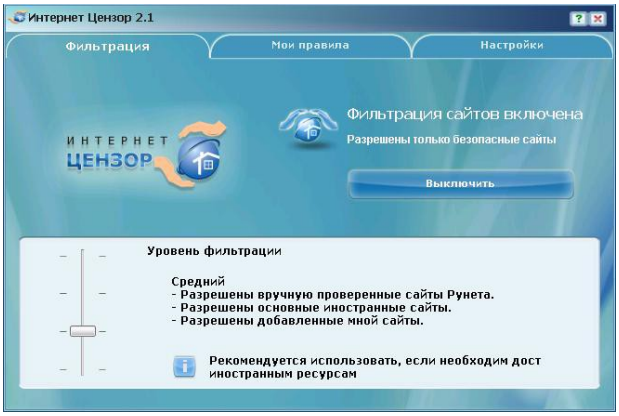
Интерфейс приложения содержит 3 вкладки:
Фильтрация Мои правила Настройки
Рассмотрим каждую из вкладок подробнее.
· Вкладка «Фильтрация».
На этой вкладке вы можете управлять уровнями фильтрации.
Каждый следующий уровень фильтрации (движение ползунка сверху вниз) является расширением предыдущего.
Рассмотрим каждый уровень отдельно.

Максимальный уровень:



На этом уровне фильтрации разрешены только добавленные вами сайты в белый список на вкладке «Мои правила».
Все остальные сайты Интернет будут блокироваться программой.
Высокий уровень:
На этом уровне кроме разрешенных вами сайтов, разрешена вручную проверенная база русского Интернета.
Данный уровень является наиболее оптимальным, и мы рекомендуем использовать его.

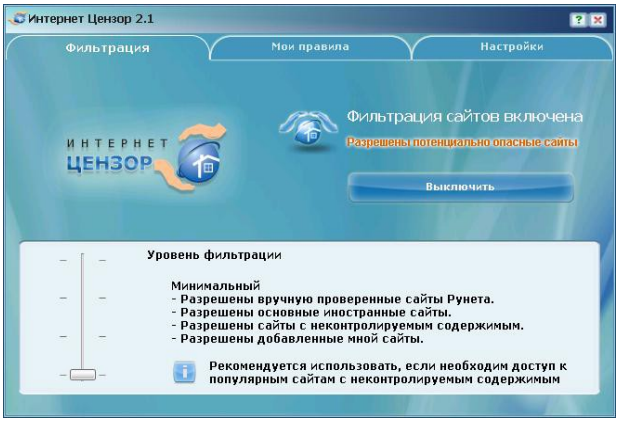
Средний уровень:



На этом уровне то же, что и на Высоком уровне плюс база основных иностранных сайтов.

Минимальный уровень:
На этом уровне разрешено то же, что и на Среднем уровне плюс ресурсы с неконтролируемым содержимым:

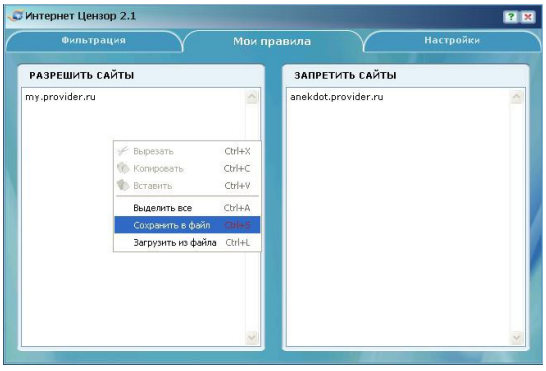
социальные сети, файлообменники и файлораздачи, в том числе сайты пиринговых сетей фото - и видео-хостинги (, ***** и т. д.) блоги (кроме профессиональных и тематических, например, *****) чаты, онлайн-игры



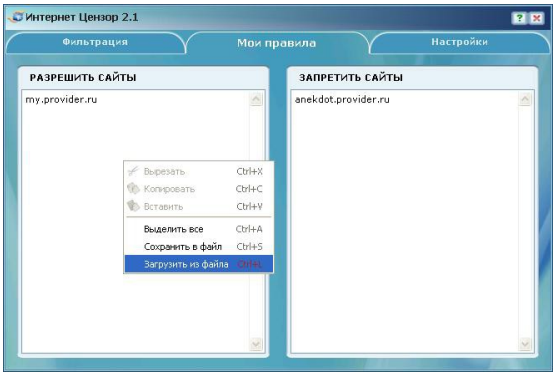
Вкладка «Мои правила».

На этой вкладке вы можете указать адреса интернет-сайтов, к которым должен быть разрешен или запрещён доступ. Внесенные вами изменения вступят в действие немедленно. Если введенные вами данные или часть данных изменит свой цвет на красный, то это значит, что была допущена ошибка в тексте. В этом случае вам следует сделать необходимые исправления.
Замечание. При внесении адресов в списки вы можете использовать адрес целиком или написать лишь его часть. В этом случае будет запущен особый режим проверки. Приведем пример. Добавление в белый список строки «» разрешит работу со всеми адресами, заканчивающимися строкой «»: download. , www. и так далее.
Если вы хотите сделать режим проверки более строгим, то используйте специальный символ «*» перед адресом: при указании в белом списке строки «*» будет разрешен доступ только к адресам «» и «www. ».
Добавление одинаковой строки и в белый список и в черный список приведёт к тому, что доступ на указанный ресурс будет запрещён.
Рекомендация:сайты, которые вы вносите в свои чёрный и белый списки, мы рекомендуем сохранять также и в отдельном текстовом файле. Если вам придётся переустановить программу, все настройки сбросятся. В этом случае вы просто скопируете список ресурсов из текстового файла в списки программы.

Если вы захотите сохранить данные из черного или белого списка в текстовый файл, то при клике правой кнопкой мыши в области списка доступно меню с пунктом «Сохранить в файл»:



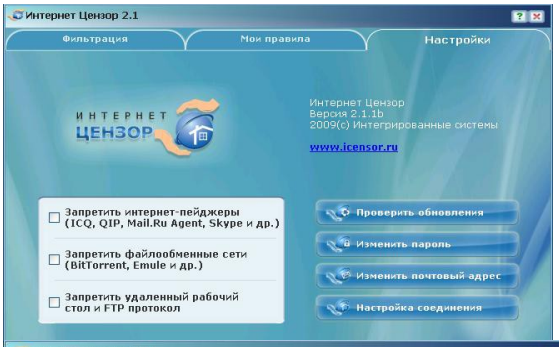
Вы также можете сайты из текстового файла загрузить в список выбрав пункт «Загрузить из файла»:



При загрузке сайтов из текстового файла, сайты добавляются в конец текущего списка.
· Вкладка «Настройки».

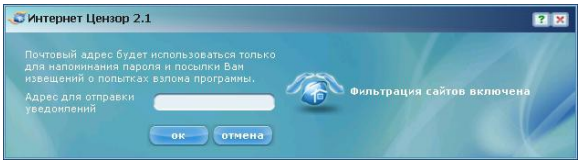
На этой вкладке вы можете:

Проверить обновления базы компании. Изменить текущий пароль. Изменить введённый вами ранее почтовый адрес, который используется для получения вами уведомлений о работе системы Наложить дополнительный запрет на активность в сети

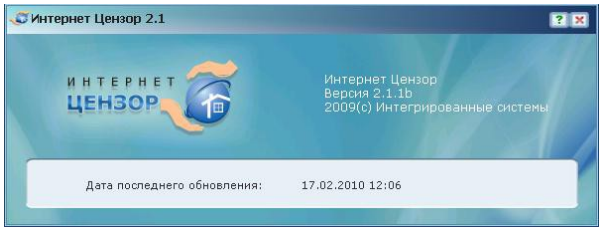


Если вы захотите изменить старый пароль, перед вами откроется окно:

Введите сначала старый пароль, а затем новый. Подтвердите новый пароль и нажмите кнопку «ОК». Окно смены почтового адреса выглядит так:



Введите в поле тот адрес электронный почты, по которому вы хотите в дальнейшем получать сведения о работе программы. Напоминаем, что этот почтовый адрес используется исключительно для отправки на него уведомлений о попытке взлома программы на вашем компьютере.
В окне проверки обновлений вы сможете увидеть дату последнего обновления программы:



Запрет на дополнительную активность в сети. В этом случае, вы можете запретить: использование Интернет-пейджеров, таких как программы обмена мгновенными сообщениями типа ICQ (а также других клиентов сети ICQ, например QIP), ***** Агент использование клиентов файлообменных сетей, например BitTorrent

Если доступ к необходимому Вам ресурсу запрещен фильтрами Вы можете обратиться с заявкой на рассмотрение необходимого интернет ресурса для дальнейшей его проверки и внесение в список разрешенных и проверенных сайтов

Удаление программы

Чтобы удалить программу с вашего компьютера нужно выбрать меню Пуск -> Все программы/Программы -> Интернет Цензор -> Удалить Интернет Цензор. При этом будет запущен процесс удаления приложения с вашего компьютера. Кроме того, программа запросит ваш пароль для того, чтобы удаление не было совершено кем-то другим. После удаления приложения может потребоваться перезагрузка.

Для получения дополнительной информации можно обратиться к **главному специалисту информационно-аналитического отдела Ахмедханову Тельману Сейфутдиновичу тел. 8-872-492-21-68**

В помощь специалистам, отвечающим за информационную безопасность в образовательных учреждениях муниципального образования «Табасаранский район», информационно-аналитический отдел провел анализ, и подготовил список **строго запрещенных ресурсов**.

1	vkontakte.ru	27	ukoz.net	53	imamtv.com	79	rusigra.info
2	odnoklassniki.ru	28	radikal.ru	54	jamaatshariat.com	80	rusigra.livejournal.com
3	video.mail.ru	29	org.ua	55	kavkazcenter.com	81	sbl4.org
4	games.mail.ru	30	ozon.ru	56	chechenpress.org	82	rusinfo.org
5	foto.mail.ru	31	com.ua	57	daymohk.ru	83	dpni-kirov.org
6	video.yandex.ru	32	classniy.ru	58	camagat.com	84	vzagruzke.info
7	images.yandex.ru	33	uooz.ru	59	fank.ru	85	intrukciya.info
8	wikipedia.org	34	vkontakte.ru	60	kavkazcenter.net	86	ru-adena.ru
9	ru.wikipedia.org	35	novoteka.ru	61	kavkazcenter.tv	87	www.liveinternet.ru
10	gazetaolekma.ru	36	rutube.ru	62	kavkaz.org	88	rian.ru
11	detka.com	37	yahoo.com	63	kavkaz.tv	89	belpar.org
12	detka.net	38	nsn.com	64	ufagub.com	90	barbos111.narod.ru
13	detka.ru	39	eiveinternet.ru	65	zhurnal.lib.ru	91	antifa.com.ua
14	devki.com	40	mikimedia.org	66	reinform.livejournal.com	92	anenerbe-org.narod.ru
15	devki.net	41	imgsmail.ru	67	liveinternet.ru	93	akmshalom.com
16	devki.ru	42	caucasuslive.org	68	national-socialist.tk	94	agonoize.beon.ru
17	devok.com	43	chechenpress.info	69	newp.org	95	www.tambov.gov.ru
18	devok.ru	44	daymohk.org	70	punk.nnov.ru	96	mirror.yandex.ru
19	devush.com	45	mon.gov.ru	71	nso.korpus.org	97	ruposik.su
20	dildo.com	46	price.ru	72	vdesyatku.biz	98	volga34.ru
21	dildo.net	47	torg.mail.ru	73	chechentimes.net	99	
22	dildo.ru	48	legal-amin.ru	74	offtop.ru	100	steroidus.ru
23	odnoklassniki.ru	49	voleity.ru	75	livejornal.com	101	
24	gismeteo.ru	50	vashareklama.com	76	velesova-sloboda.org		
25	static.com	51	volgograd-regions.lanet.ru	77	gorodsalavat.ru		
26	gov.ru	52	mirborisa.com	78	rusigra.org		

Рекомендации

Для наилучшего обеспечения безопасности мы рекомендуем вам создать на вашем компьютере несколько учётных записей пользователей. Одну – с правами администратора – для себя, другие – для детей – пользовательские, без администраторских прав. О том, что такое учетные записи и как

управлять ими вы можете посмотреть в справке Windows. Помимо всего прочего, эта мера поможет снизить риск заражения компьютера вирусами, проникающими в систему при прочтении информации с инфицированных сменных носителей.

Следует также помнить, что при любых попытках нарушить работу программы путём удаления или повторной установки (с целью получить новый пароль) на ваш адрес электронной почты, который вы указали в программе, приходит соответствующее уведомление. Таким образом, вы получаете возможность контролировать целостность «Интернет Цензора» на вашем компьютере

Информационно-аналитический отдел рекомендует 1 раз в четверть проводить контроль работы средств контентной фильтрации и сверку библиотечного фонда силами общественности и актировать полученные результаты. Если в ходе проверки удалось выйти на запрещенную информацию, адрес ресурса актируется и направляется провайдеру, предоставляющему услугу доступа в сеть. Особое внимание следует уделить доступу к информации, содержащейся в федеральном списке экстремистских материалов.

Формирование у подростка готовности и способности регулировать информационные опасности вокруг себя одна из задач системы образования.

Оценивая собственную подготовку по вопросам обеспечения информационной безопасности детей 89% педагогов отмечают, что знают о существовании основных законодательных актов, но не знакомы с их основными положениями; почти все участники опроса (98%) уверены, что педагогу необходима специальная подготовка к работе с детьми и родителями по вопросам информационной безопасности. В связи с чем, проблема повышения квалификации педагогов приобретает особую актуальность.

Еще одной мерой, направленной на обеспечение информационной безопасности детства, является создание порталов и сайтов, аккумулирующих сведения о лучших ресурсах для детей и родителей; стимулирование родителей к использованию услуги "Родительский контроль", позволяющей устанавливать ограничения доступа к сети "Интернет".

В целях усиления профилактической работы по вопросу защиты детей от информации, причиняющей врез их здоровью и развитию, рекомендуем руководителям образовательных организаций следующее:

1. Провести родительские собрания на тему **«Защита детей от информации, наносящей вред их здоровью, нравственному и духовному развитию».** Особое внимание уделить разъяснению необходимости подключения домашней услуги «Родительский контроль».
2. Оформить стенд для родителей, разместив на нем материалы по защите детей от информации, приносящей вред их здоровью и развитию, в том числе, информацию об услуге «Родительский контроль».
   2.1. Разместить информацию для родителей (законных представителей) и обучающихся на официальном сайте образовательной организации.

Помимо услуги «Родительский контроль» родителям можно также предложить **NetKids** - сервис, который позволяет контролировать использование сети «Интернет» детьми.

На заре появления социальных сетей основной их аудиторией была молодежь, сейчас же в социальных сетях общаются люди самого разного возраста. Стоит ли говорить, что контент социальных сетей далеко не всегда приемлем для детей, добравшихся до интернета. Эксперты признали "ВКонтакте" самой опасной социальной сетью. Однако есть специальные детские социальные сети, содержание которых соответствует возрасту юных пользователей.

Ответственность образовательной организации по вопросу обеспечения информационной безопасности детей закреплена в Федеральных законах

От №273-ФЗ «Об образовании в Российской Федерации» и от 29.12.2010 №436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию».

В соответствии с п.15 ч.3 ст.28 Федерального закона «Об образовании в Российской Федерации» к компетенции образовательной организации относится создание необходимых условий для охраны и укрепления здоровья обучающихся и работников.

В соответствии со ст.11, ч. 1 ст. 14 Федерального закона № 436-ФЗ образовательные

организации, предоставляя для детей компьютеры, имеющие выход в Интернет, во время образовательного процесса и вне учебного времени, обязаны применять определенные административные и организационные меры, технические и программно-аппаратные средства защиты детей от указанной информации и несут ответственность за доступ к информации, наносящей вред здоровью несовершеннолетнего.

В соответствии с Приказом Генеральной прокуратуры РФ «Об организации прокурорского надзора за исполнением законов о несовершеннолетних и молодежи» от 26 ноября 2007 г.№188, соблюдение законодательства о защите детей от информации, наносящей вред их здоровью, репутации, нравственному и духовному развитию в деятельности средств массовой информации, органов и учреждений образования и культуры проверяется систематически.

В рамках проверок образовательных организаций изучались следующие вопросы:

- Организация доступа в сеть «Интернет»;
- Административные и организационные меры, технические и программно-аппаратные средства защиты детей от вредной информации;
- Внедрение программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность;
- Защита детей от запрещённой для распространения информации в рекламе.

Материал подготовил
Главный специалист
Ахмедханов Т.С.
тел. 8-872-492-21-68