Сервер контентной фильтрации. Инструкция для администратора учреждения.

Оглавление

Введение.

Сервер контентной фильтрации – это кэширующий HTTP-прокси сервер со специальными настройками, позволяющий блокировать доступ к различным категориям сайтов, в том числе работающих по защищенному протоколу HTTPS. Блокировка происходит как на основе чёрных списков сайтов, так и на основе анализа содержимого текста веб-страницы. Блокировка также осуществляется по результатам антивирусной проверки объектов веб-сайтов встроенным в сервер антивирусом ClamAV.

Сервер контентной фильтрации также может выступать в качестве маршрутизатора локальной сети, DNS- и DHCP-сервера.

Уровни фильтрации.

В настоящий момент реализовано 3 уровня фильтрации содержимого веб-страниц:

1. «Без фильтрации» – блокировка сайтов не осуществляется.
2. «Администрация» – действует блокировка сайтов следующих категорий: порнографические материалы, алкоголь, наркотики, онлайн-казино, обход блокировок, социальные сети, сайты знакомств. Анализ текста веб страниц не осуществляется. HTTPS –сертификат не подменяется.
3. «Учащиеся» - действует блокировка сайтов следующих категорий: порнографические материалы, нецензурная лексика, алкоголь, наркотики, онлайн-казино, обход блокировок, социальные сети, сайты знакомств, файлообменные сети, торрент-трекеры, онлайн-кинотеатры, экстремистские организации, изготовление самодельных взрывных устройств, суицидальное поведение, компьютерные игры. Для блокировки поисковых запросов осуществляется анализ содержимого сайтов работающих по HTTPS, путём подмены сертификата сайта (включается по запросу). В поисковых системах Яндекс, Google и видео-хостинге www.youtube.com принудительно включен «детский» режим, не позволяющий осуществлять некоторые виды поисковых запросов.

Уровни фильтрации настраиваются при создании учётных записей пользователей, если включена аутентификация пользователей по паролям, либо указанием принадлежности IP адреса компьютера к группе, если аутентификация по паролям не включена (подробнее в разделах «Аутентификация» и «Настройка браузеров»).

HTTPS сайты.

Все поисковые системы и многие популярные сайты работают по протоколу HTTPS. Это означает, что данные передаются от веб-сервера к веб-браузеру в зашифрованном виде, и не могут быть подвергнуты анализу содержимого. Для решения этой проблемы сервер контентной фильтрации расшифровывает данные HTTPS, анализирует, повторно зашифровывает, и передаёт в браузер пользователю. Но данные зашифрованы сертификатом, выданным неизвестным удостоверяющим центром (сервером контентной фильтрации), поэтому браузер сообщит об ошибке сертификата сайта и откажется открывать сайт (Рис.1):

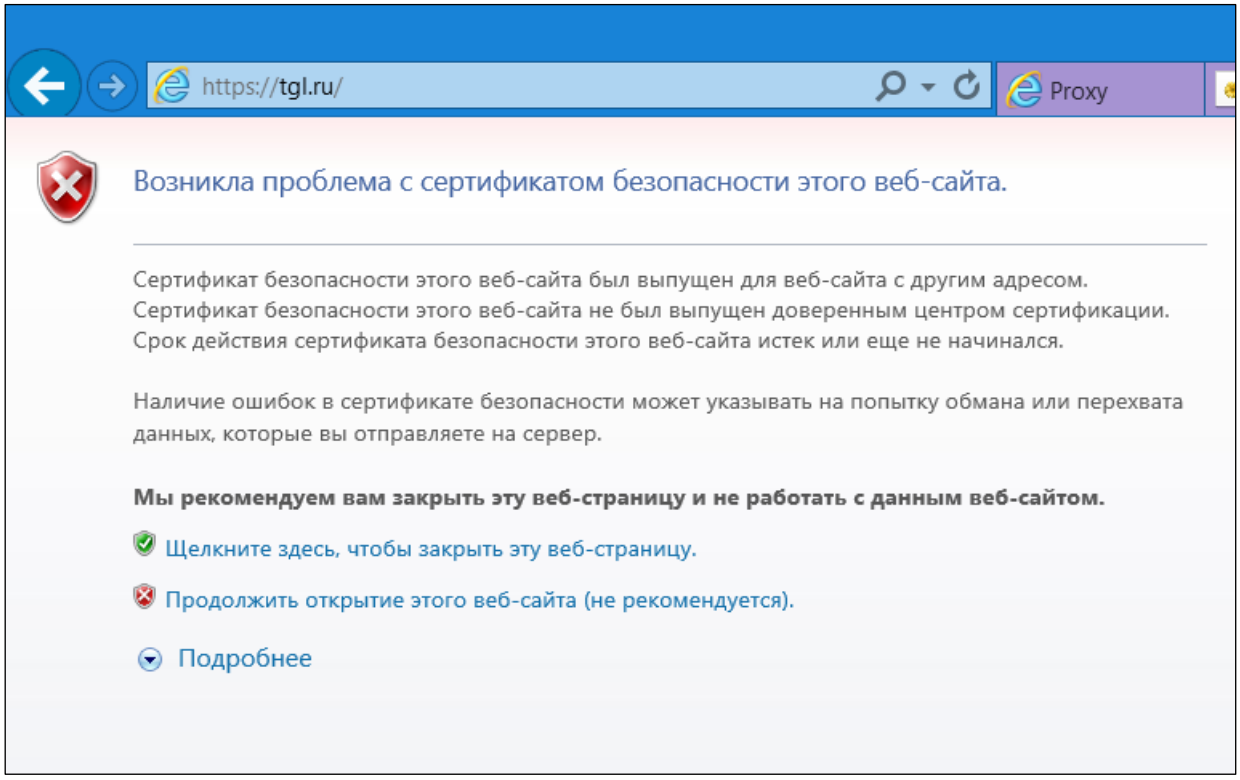


Рисунок 1. Предупреждение о недействительном SSL-сертификате сайта.

Для подавления этой ошибки в браузерах, необходимо установить в хранилище сертификатов операционной системы корневой сертификат сервера контентной фильтрации. Делать это нужно только на ученических компьютерах, т.к. расшифровка HTTPS-трафика с подменой сертификата осуществляется только для уровня фильтрации «Учащиеся». Подробнее об установке сертификата в разделе «Настройка браузеров».

Веб-интерфейс сервера контентной фильтрации.

Чтобы открыть веб-интерфейс СКФ, в браузере необходимо открыть адрес сервера: http://proxy.school.lan (или http://xxx.xxx.xxx.xxx, где xxx.xxx.xxx.xxx адрес СКФ в локальной сети)

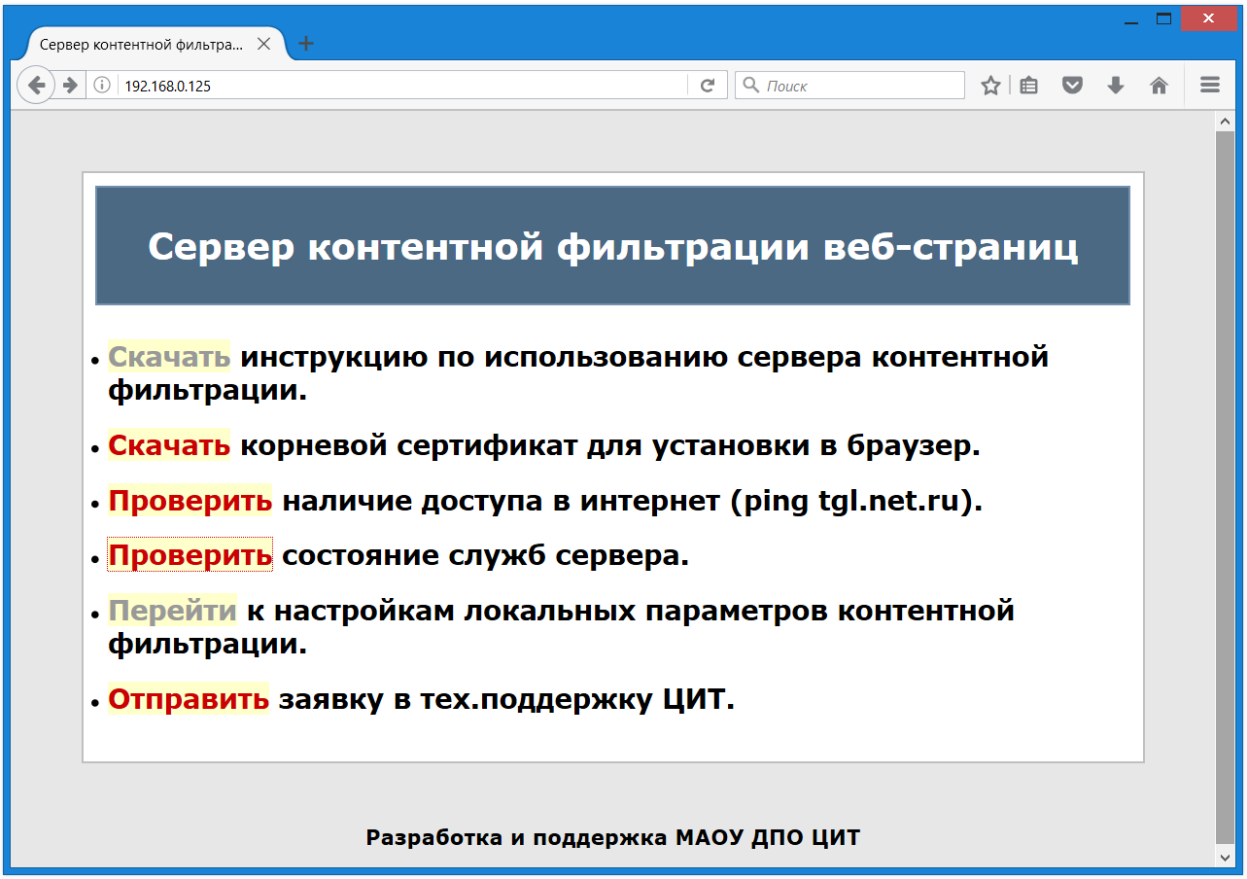


Рисунок 2. Веб-интерфейс сервера контентной фильтрации.

- **Скачать инструкцию …** – скачать данную инструкцию в формате PDF. Файл инструкции автоматически обновляется при необходимости.
- **Скачать корневой сертификат …** – скачать файл сертификата для. См. раздел инструкции «Настройка браузеров»
- **Проверить наличие доступа в интернет** – сервер выводит результаты системной команды ping, если доступ в интернет есть, в конце должны быть строки:

```
--- tgl.net.ru ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.762/0.847/0.928/0.075 ms
```

  Что означает отсутствие потерь пакетов.
- **Проверить состояние служб сервера** – выводится страница с состоянием критически важных служб СКФ, временем их работы с момента запуска, нагрузкой на процессор. В нормальном режиме работы, Status всех служб должен быть Running:

System	Status	Load	
proxy64	Running	[0.00] [0.01] [0.05]	0.0%us,

Process	Status	Uptime
squid	Running	6d 5h 8m
named	Running	6d 5h 8m
e2guardian	Running	8h 4m

Рисунок 3. Проверка состояния сервера.

- **Перейти к настройкам локальных параметров контентной фильтрации** – в этом разделе интерфейса можно управлять некоторыми параметрами контентной фильтрации:

    - Пользователи – управление учётными записями пользователей СКФ. См. раздел «Аутентификация»
    - Журнал доступа в интернет – просмотр и загрузка журнала доступа к веб-сайтам. Данные в журнале сохраняются за последние 365 дней.
    - Белый список. Включение режима «Белый список» позволяет группе пользователей «Учащиеся» работать только с теми сайтами, список которых заранее определён.
    - Разрешенные IP адреса – управление полным доступом в Интернет для определённых компьютеров и устройств. См. раздел «Полный доступ в интернет»

    Если вы считаете, что какой-либо сайт заблокирован ошибочно, вы должны направить заявку в ЦИТ для разблокирования данного сайта. Возможна блокировка/разблокировка сайта для определённой группы пользователей и для определённой школы.
    «Белый список» также будет пополняться по вашим заявкам.
    При обнаружении сайтов с запрещенным содержанием необходимо незамедлительно подать заявку на блокировку.

Аутентификация.

При доступе в интернет рекомендуется включать аутентификацию пользователей с помощью ввода логина и пароля. Это позволит вести электронный журнал доступа в интернет и легко присваивать учётным записям пользователей соответствующие уровни фильтрации. Учётные записи пользователей могут быть локальными (хранящимися на сервере) или доменными (хранящимися на контроллере домена Windows Server или SAMBA Linux). Если прокси-сервер настроен на использование учётных записей домена, то запроса имени и пароля не будет, для авторизации браузер будет использовать имя и пароль, указанные при входе в систему Windows.
Включение и настройка аутентификации производится специалистами ЦИТ по запросу.
Возможен режим работы СКФ без аутентификации, в таком случае запроса логина и пароля не будет, а различные уровни фильтрации выбираются путём назначение IP-адресу или диапазону адресов соответствующего уровня.

Добавление пользователя:

1. Зайти на веб-интерфейс СКФ: http://proxy.school.lan (или http://xxx.xxx.xxx.xxx, где xxx.xxx.xxx.xxx адрес СКФ в локальной сети)
2. Перейти к настройкам локальных параметров контентной фильтрации. Ввести логин и пароль для доступа к настройкам.
3. Перейти в раздел «Пользователи», создать учётные записи пользователей, назначить уровни фильтрации, и применить изменения.

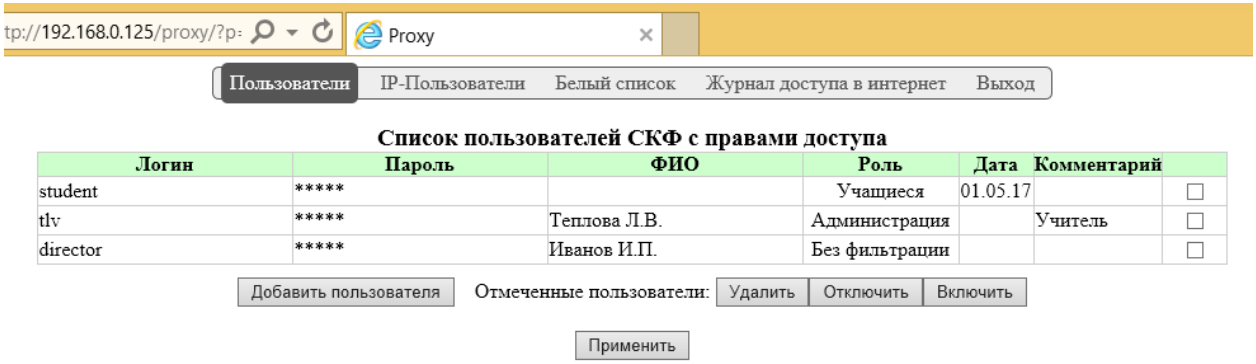


Рисунок 4. Управление пользователями

Если аутентификация по паролям не включена, то по умолчанию всё компьютеры локальной сети работают по максимальному уровню фильтрации «Учащиеся». Для того что бы изменить уровень фильтрации для определённых компьютеров нужно перейти в раздел «IP-Пользователи», добавить адреса, для которых необходимо изменить уровень фильтрации.

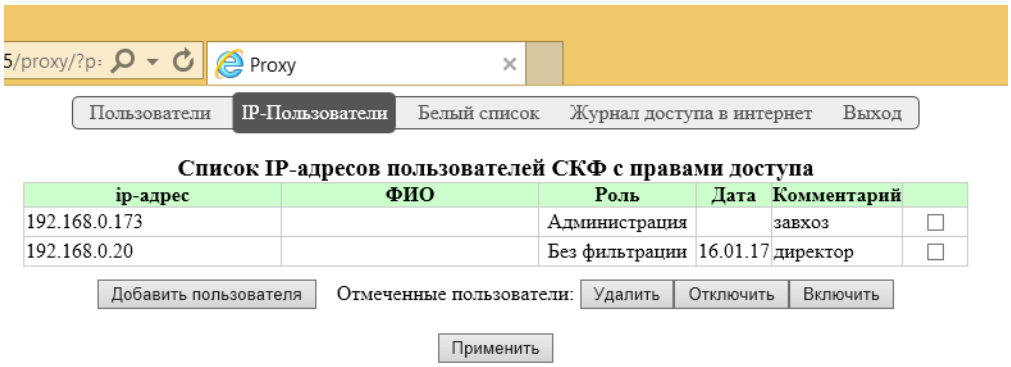
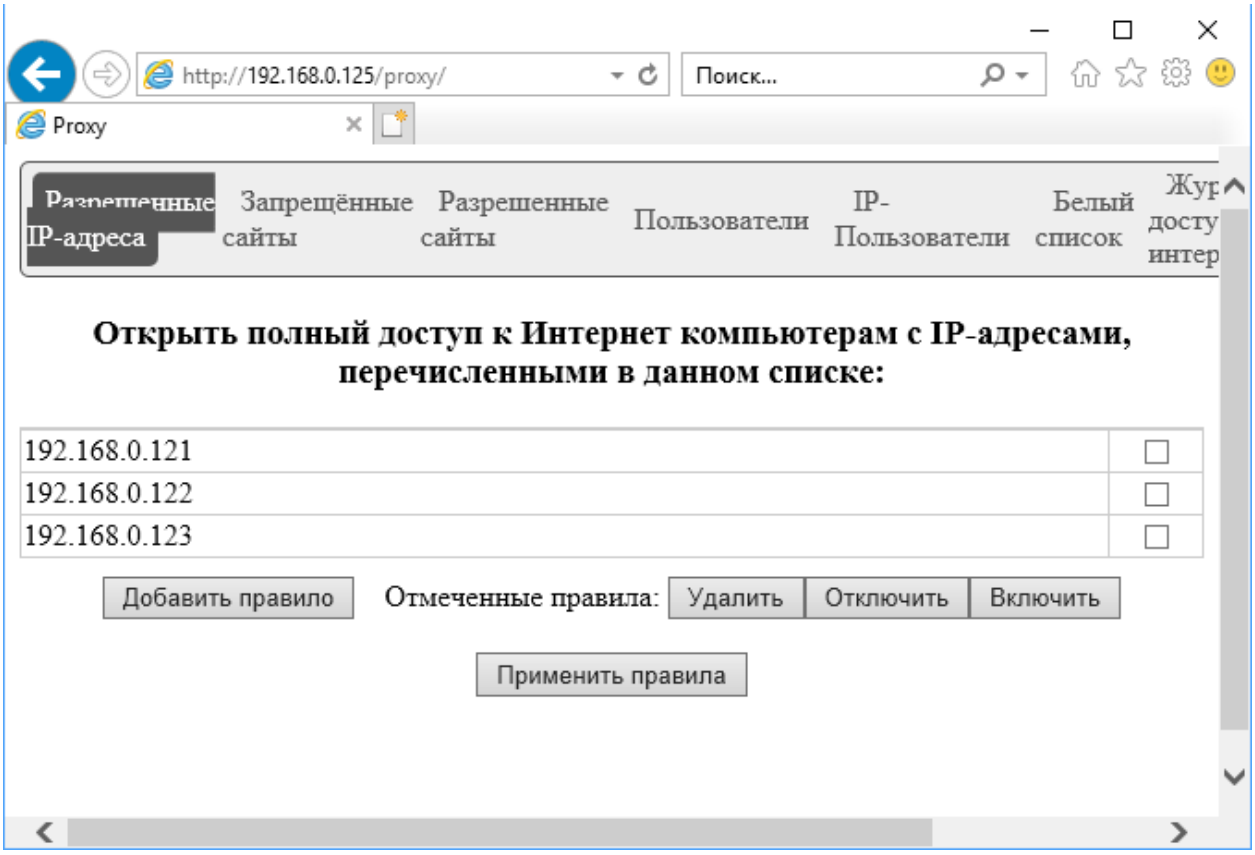


Рисунок 5. Управление IP-адресами

Следует помнить, если IP-адрес компьютера назначается автоматически (DHCP-сервером), то он может через какое-то время измениться. Адрес «Без фильтрации» может быть выдан компьютеру для учеников. Поэтому следует назначать такие адреса статически, либо вручную, либо через резервирование в DHCP-сервере.

Полный доступ в интернет

Для того, что бы открыть полный доступ в Интернет (в обход прокси-сервера) для определённых компьютеров, нужно на вкладке «Разрешённые IP-адреса» добавить адреса компьютеров в таблицу и нажать кнопку «Применить правила»



Настройка браузеров.

Настройка параметров прокси-сервера.

Если компьютерами вашей локальной сети используется DNS-сервер сервера контентной фильтрации, то параметры прокси-сервера будут настроены автоматически при помощи протокола WPAD (если стоит галочка «Автоматическое определение параметров»).

В случае, если используется другой DNS-сервер, то для автоматической настройки параметров прокси-сервера в вашей DNS-зоне необходимо создать запись wpad указывающую на IP-адрес прокси-сервера: например: `wpad A 192.168.0.254`. Так же всегда можно указать IP адрес или имя и порт прокси-сервера вручную:

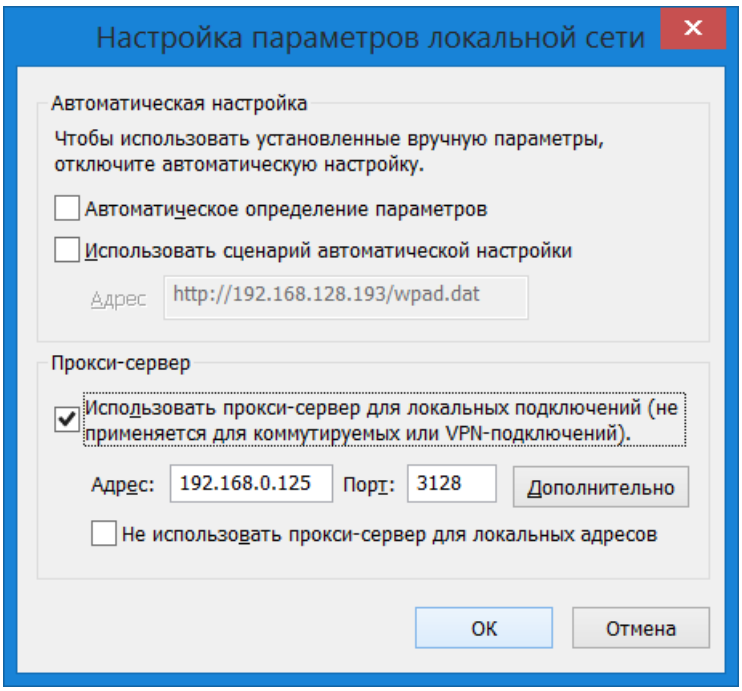


Рисунок 6. Параметры прокси сервера Internet Explorer.

IP-адрес прокси сервера зависит от настроек вашей локальной сети, и назначается специалистами ЦИТ по вашему запросу.

Установка корневого сертификата СКФ в хранилище сертификатов.

Для подавления сообщения об ошибочном сертификате при просмотре HTTPS-сайтов на ученических компьютерах необходимо установить корневой сертификат сервера контентной фильтрации.

Для этого необходимо:

1. Зайти на веб-интерфейс СКФ: http://proxy.school.lan (или http://xxx.xxx.xxx.xxx, где xxx.xxx.xxx.xxx адрес СКФ в локальной сети)
2. Скачать корневой сертификат для установки в браузер.
3. Открыть сертификат и установить его в «Доверенные корневые центры сертификации»

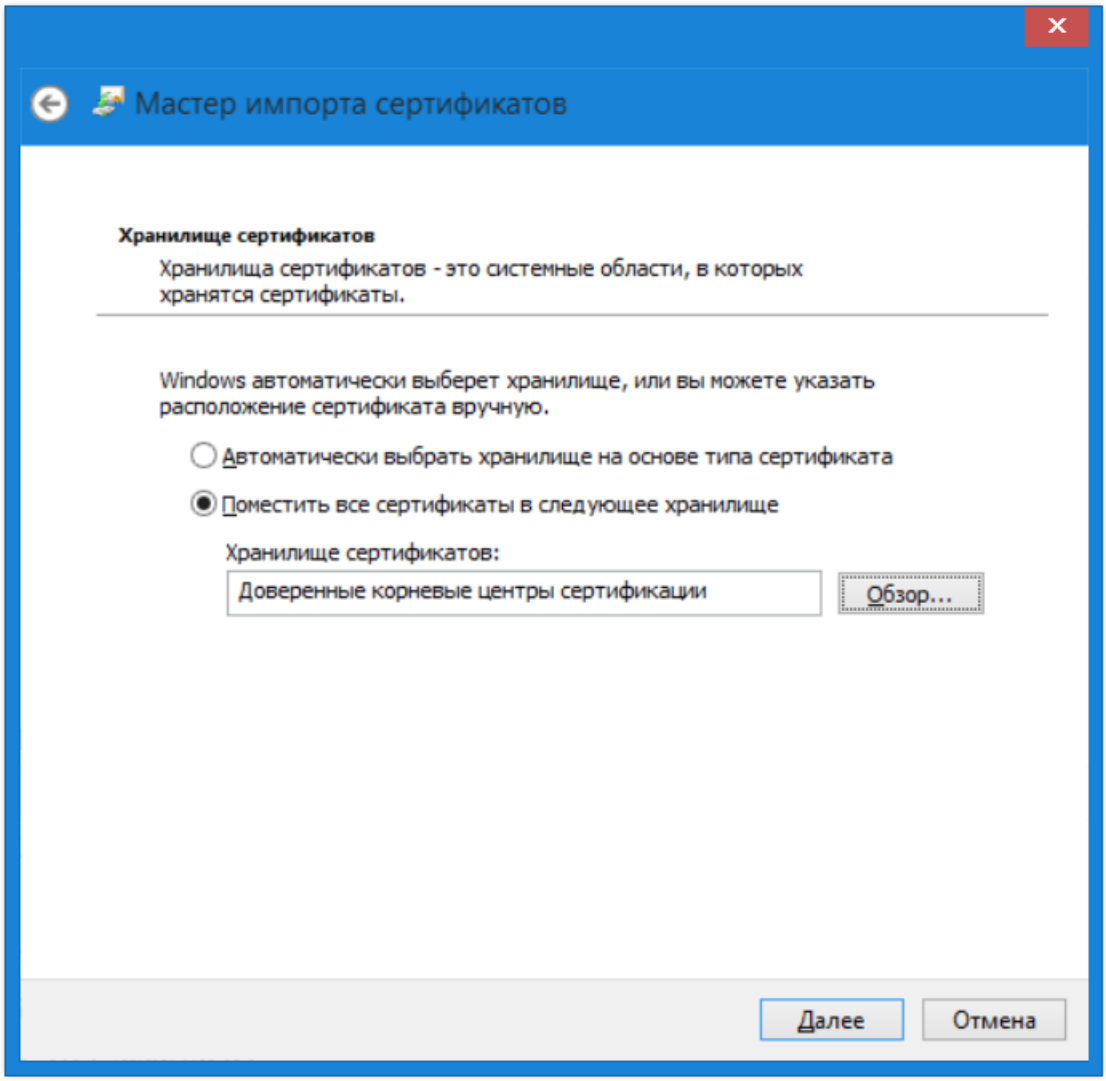


Рисунок 7. Установка SSL-сертификата в хранилище сертификатов ОС Windows.

Браузер Fire Fox использует собственное хранилище сертификатов, процедура установки сертификата в Fire Fox следующая:

1. Открыть Fire Fox;
2. Зайти на веб-интерфейс СКФ: http://proxy.school.lan (или http://xxx.xxx.xxx.xxx, где xxx.xxx.xxx.xxx адрес СКФ в локальной сети)
3. Перейти по ссылке «Скачать корневой сертификат…»;
4. В окне «Загрузка сертификата» поставить галочку напротив «Доверять при идентификации веб-сайтов» и нажать «ОК».

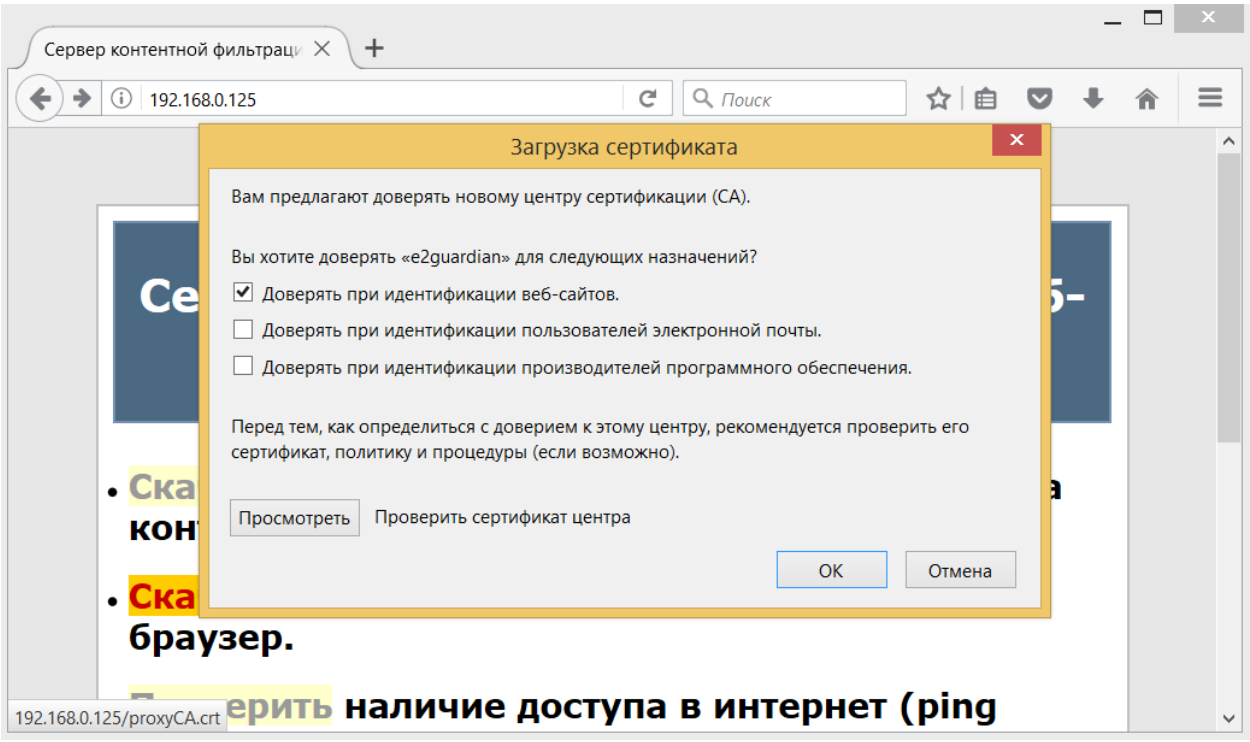


Рисунок 8. Установка SSL-сертификата в хранилище сертификатов браузера Fire Fox.

Классификатор информации

Приложение 1

УТВЕРЖДЕН
Решением регионального Совета
по вопросам регламентации доступа
учащихся образовательных
учреждений Самарской области
к информационным ресурсам сети
Интернет

от *« 5 »* *марта* 2007 г.

КЛАССИФИКАТОР ИНФОРМАЦИИ,
распространение которой запрещено в соответствии с законодательством Российской Федерации

Классификатор информации, запрещенной законодательством Российской Федерации к распространению, применяется в единообразном виде на всей территории Российской Федерации; разработан в соответствии с проведенным анализом законодательства Российской Федерации и международных договоров Российской Федерации.

№ п / п	Наименование тематической категории	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, пропаганду 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 контртеррористической операции
5	Злоупотребление сво-	Содержащая скрытые вставки и иные технические спо-

№ п / п	Наименование тематической категории	Содержание
	бодой СМИ / скрытое воздействие	собы воздействия на подсознание людей и (или) оказывающих вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская деятельность (экстремизм)	А) Экстремистские материалы, т.е. предназначенные для обнародования документы либо 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 в себя 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; - пропаганду 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, соединенное с насилием или угрозой его применения; - публичную клевету в отношении лица, замещающего

№ п / п	Наименование тематической категории	Содержание
		государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, соединенную с 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 на угрозу применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; - посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения 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 неприлично 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 пропаганду социального, расового, национального и религиозного неравенства; - публичные призывы к развязыванию агрессивной войны.
9	Ненадлежащая ре-	Информация, содержащая рекламу алкогольной про-

№ п / п	Наименование тематической категории	Содержание
	клама	дукции и табачных изделий
10	Информация с ограниченным доступом	Информация, составляющая государственную, коммерческую, служебную или иную специально охраняемую законом тайну