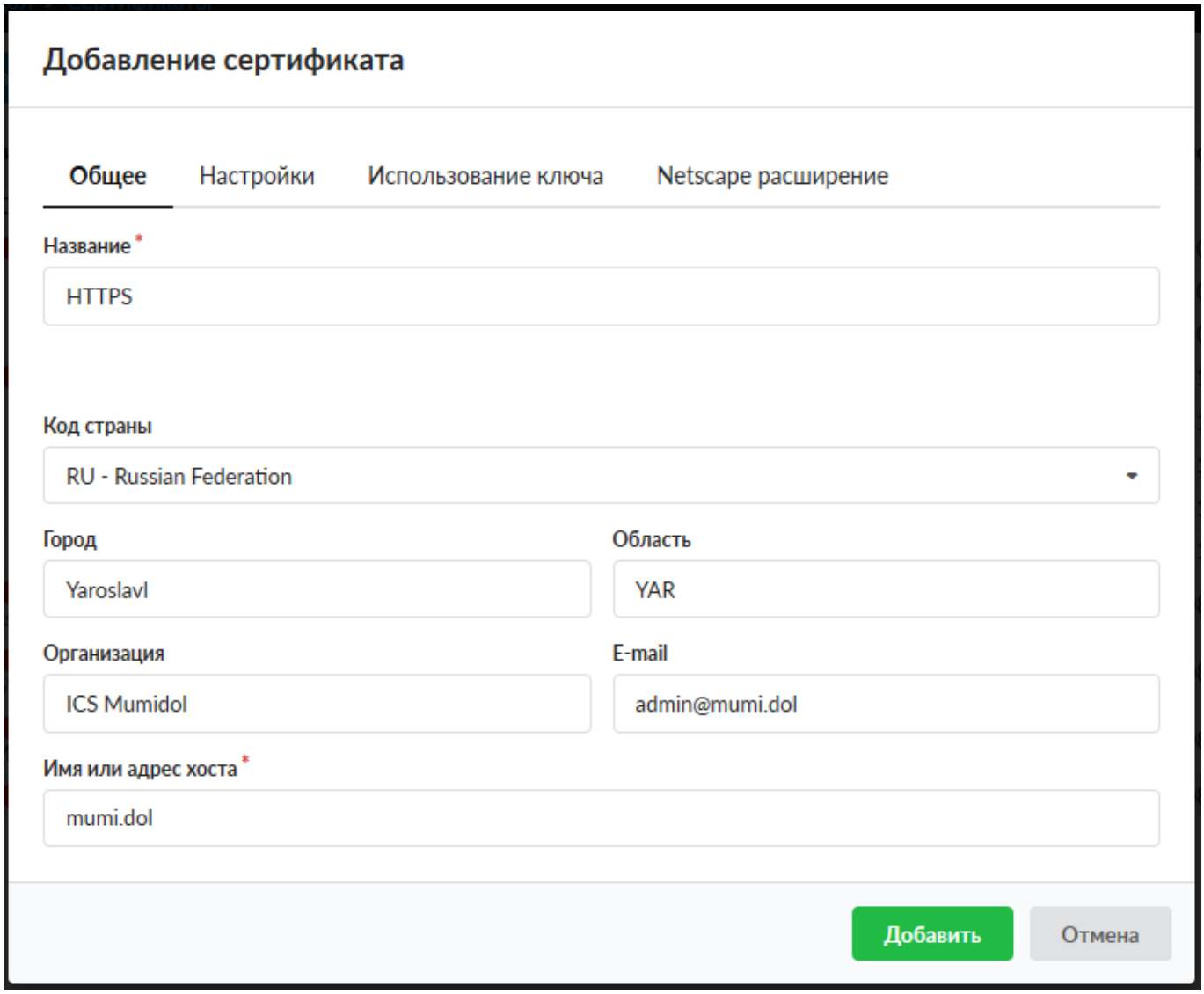
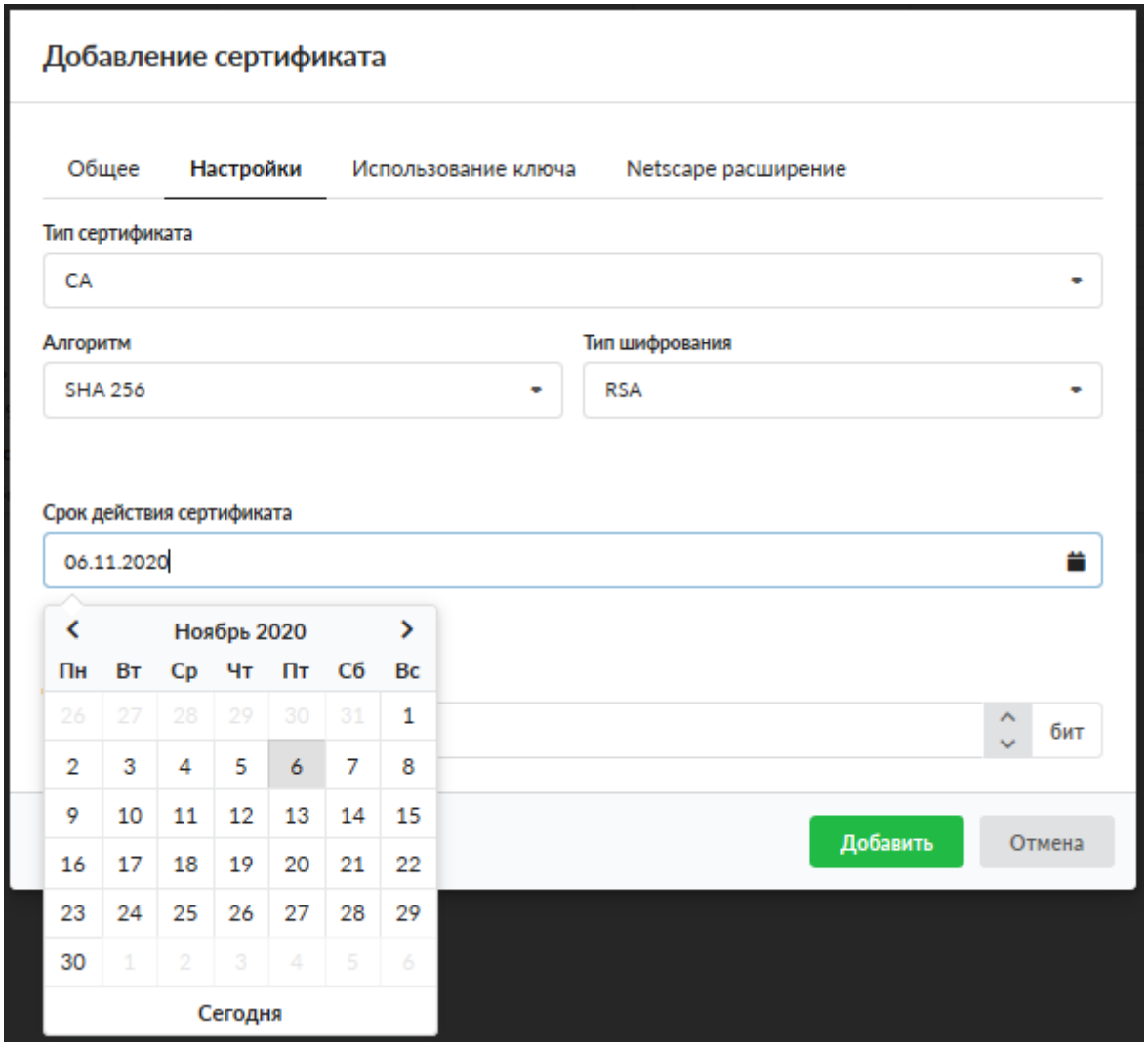
Настройка HTTPS-фильтрации

Для того, чтобы получить возможность фильтровать HTTPS-трафик пользователей, необходимо сделать следующее:

1. Добавить корневой сертификат (CA) со стандартными настройками в модуле сертификаты.

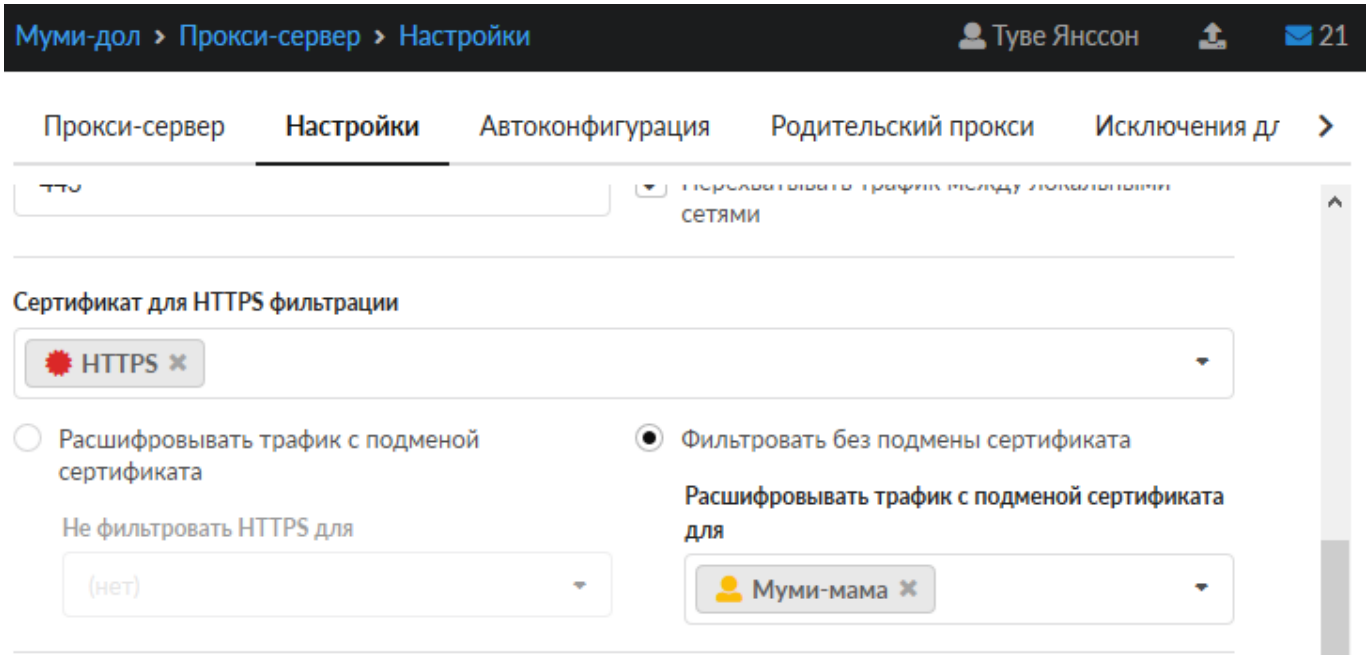


Для того, чтобы сертификат работал длительное время и не было необходимости менять его на конечных пользователях, установите дату окончания сертификата более чем 1 год (по умолчанию). Остальные параметры сертификата оставьте по умолчанию.



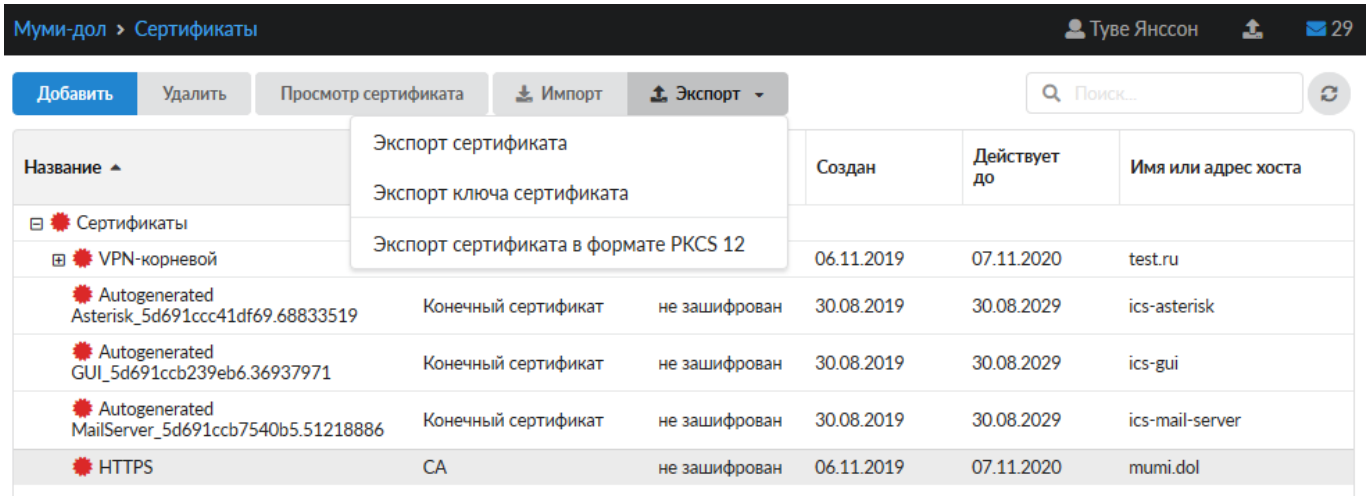
После нажатия кнопки «Добавить» система спросит, нужно ли шифрование ключа. Укажите «Не шифровать закрытый ключ».

2. Выбрать данный сертификат в поле «Сертификат для HTTPS-фильтрации» настроек модуля прокси.



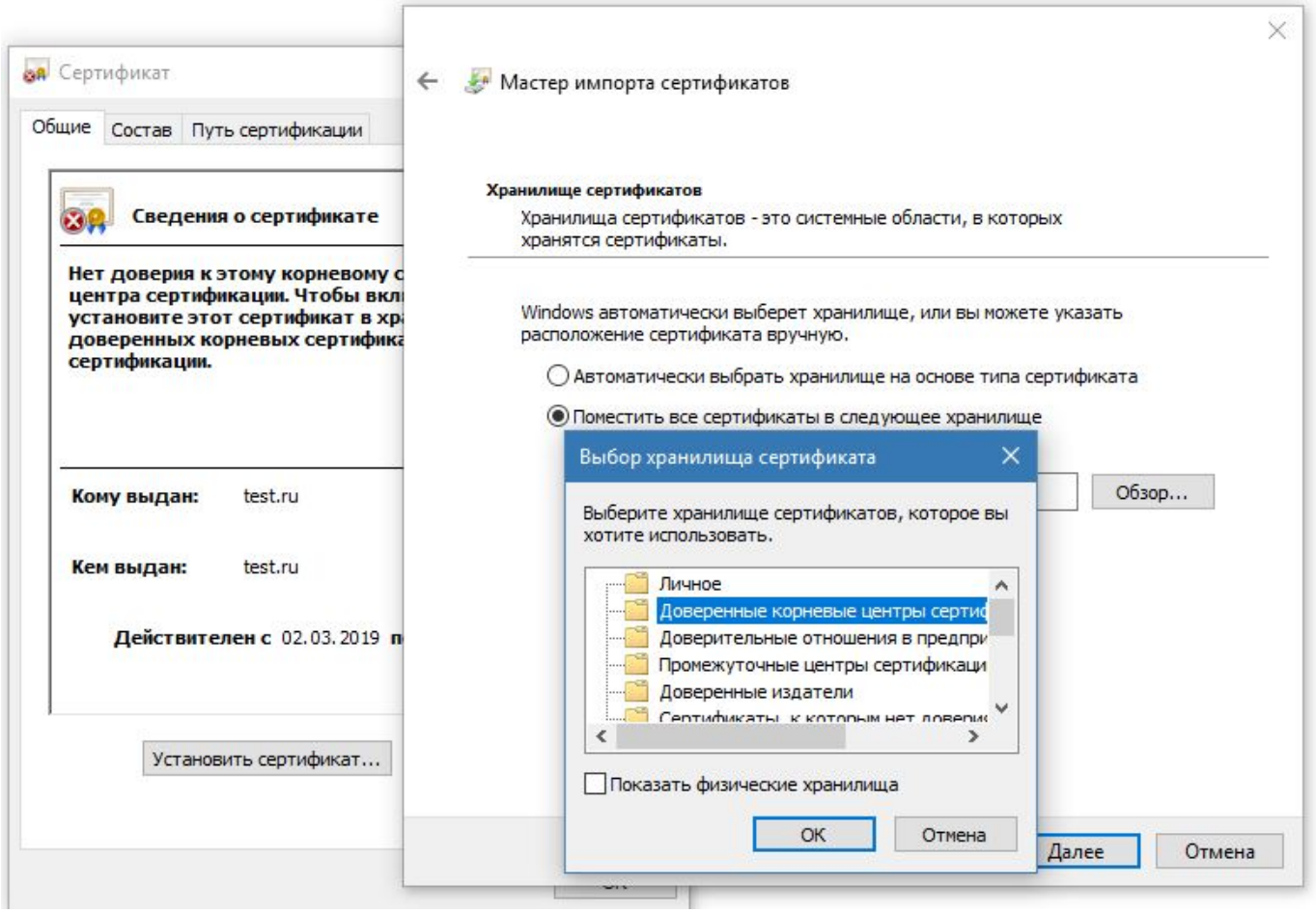
После этого необходимо выбрать один из двух режимов работы фильтрации:

Фильтровать весь HTTPS-трафик с расшифровкой. В этом режиме весь проходящий трафик будет расшифровываться посредством подмены сертификата. После этого правила фильтрации начнут работать, однако в связи с подменой сертификата при запросе браузер пользователя будет сообщать о некорректном сертификате. Чтобы исключить данную ошибку, необходимо сделать следующее:

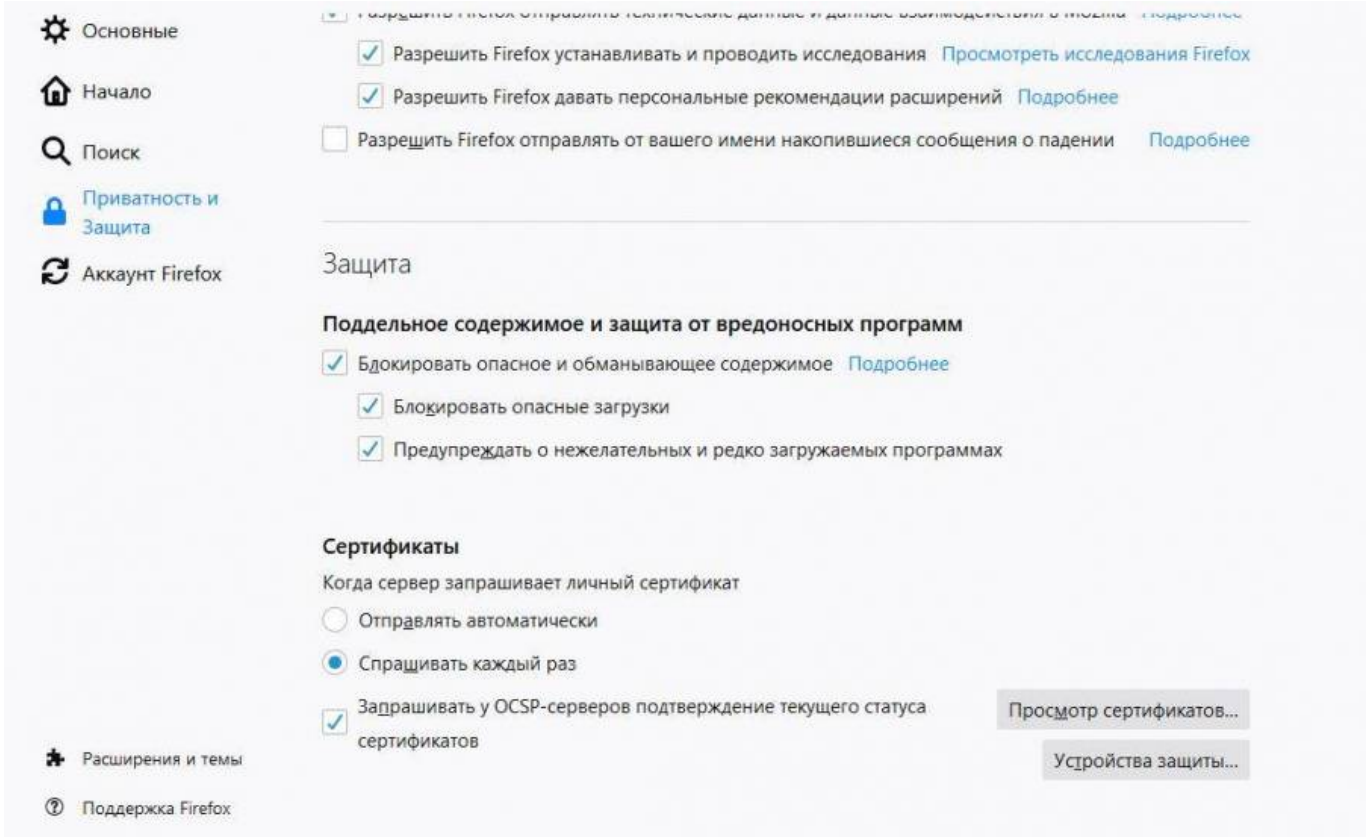


В модуле сертификаты экспортировать данный сертификат на машину конечного пользователя. Экспорт ключа сертификата не требуется.

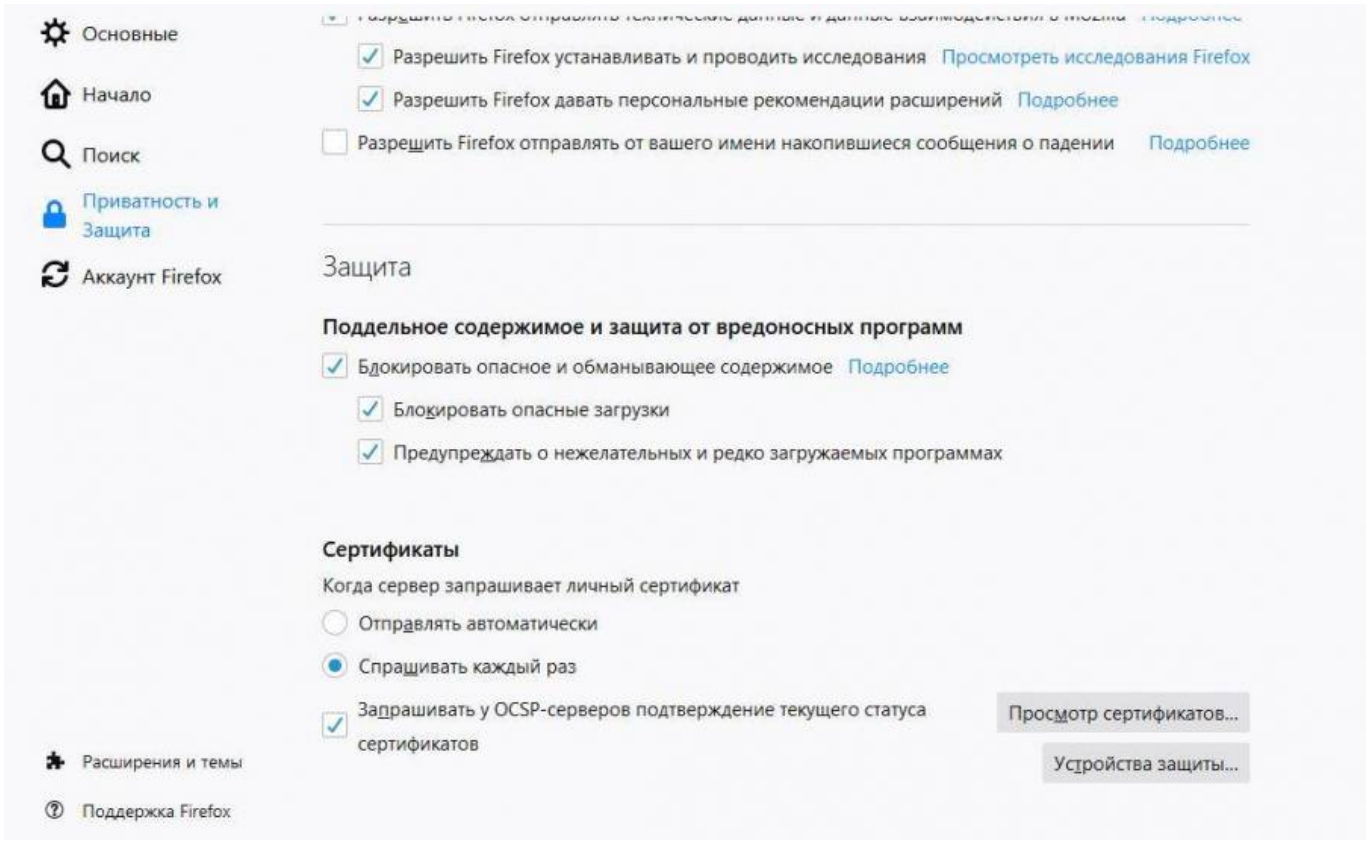
На каждом клиентском компьютере добавить сертификат в доверенные корневые центры сертификации. Это делается следующим образом (на примере Windows 7): дважды кликните на сертификат. Нажмите кнопку «Установить сертификат». Откроется мастер импорта сертификата. Когда мастер спросит выбор места хранения сертификата, выберите «поместить все сертификаты в следующее хранилище», нажмите кнопку «Обзор» и выберите «доверенные корневые центры сертификации».

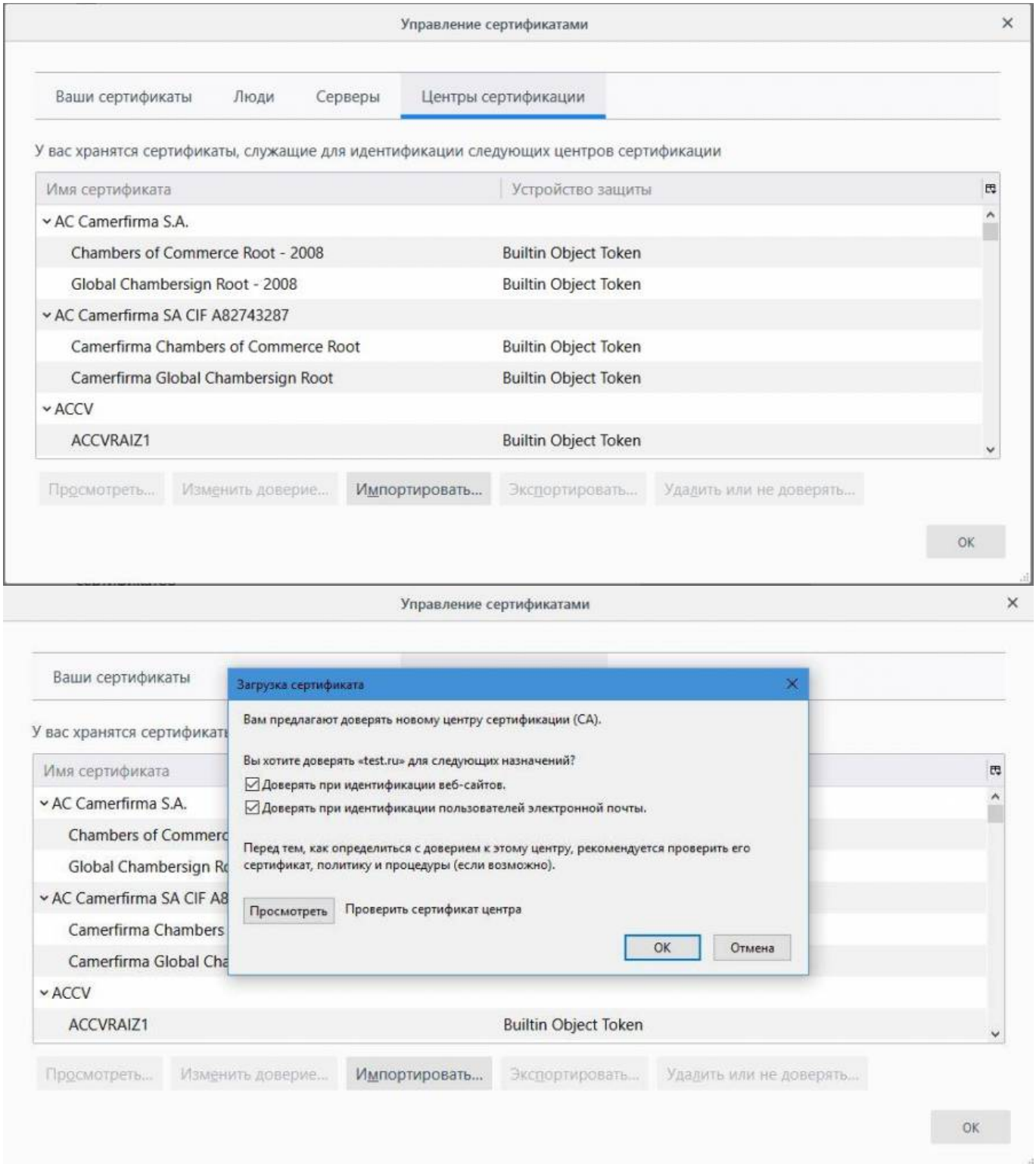


Таким образом, сертификат будет импортирован в глобальное хранилище системы. Он будет работать для тех браузеров, которые используют системные хранилища сертификатов, например, Internet Explorer, Chrome, Yandex. Если же браузер использует собственное хранилище, как, к примеру, Firefox, то импорт необходимо произвести непосредственно в настройках браузера. Это делается следующим образом (для Mozilla Firefox):



Зайдите в настройки браузера, перейдите в Дополнительные - Сертификаты - Просмотр сертификатов - WЦентры сертификации - Импортировать и укажите скачанный с ИКС сертификат.





Отметьте все флажки и импортируйте сертификат.

Для того, чтобы исключить выбранных пользователей или отдельные домены, применяется поле «Исключения». Соединения пользователей, указанных в этом поле не будут расшифровываться и, соответственно, импортировать сертификат для них нет необходимости. Аналогично, соединения на указанные домены также не будут расшифровываться. Добавлять домены может потребоваться для корректной работы безопасных сервисов в проверкой MitM-атак, таких как почтовые или банковские сервисы.

Фильтровать без подмены сертификата. В этом режиме установка сертификата в систему конечного пользователя не требуется. Однако, в данном режиме работы ИКС будет знать

только о домене назначения запроса, а не о полном URL.

Например, если вы хотите заблокировать весь домен yandex.ru, то для этого достаточно настроить фильтрацию в режиме работы без подмены сертификата. Если же вы хотите заблокировать домен yandex.ru, но при этом разрешить адрес yandex.ru/video, то вам потребуется настроить полную подмену сертификата для расшифровки URL назначения.

Также, в данном режиме работы есть возможность настроить отдельные домены либо же отдельных пользователей на полную расшифровку в поле «Фильтровать с расшифровкой». В этом случае импортировать сертификат нужно либо для тех пользователей, которые указаны в поле, либо для всех пользователей, которые будут обращаться к прописанному доменному имени (например vk.com).