Тамбовское областное государственное бюджетное учреждение
«Компьютерный центр»

Маковеев С.Н., Хорохорин О.А.

Обзор персональных контент-фильтров

Тамбов 2018

Оглавление

ВВЕДЕНИЕ

В настоящее время тема защиты детей от нежелательного воздействия Интернета весьма популярна. Однако чаще всего можно услышать только общие слова, а конкретные технические решения, как правило, не обсуждаются. Интернет содержит как негативную информацию, так и позитивную, важную для образования и развития. Попытки ограничить доступ ребенка только к специально отобранным сайтам (модель «белых списков») по сути убивает всю идею использования сети Интернет как неограниченного источника знаний и даже лишает возможности нормально использовать обычный поиск. С другой стороны, отсутствие фильтрации приводит к риску посещения разных нежелательных категорий сайтов. В этой связи важным становится выбор решения для интернет-фильтрации, которое, с одной стороны, обеспечит качественную защиту, с другой – не будет необоснованно ограничивать доступ на неопасные ресурсы. Важно также отметить, что любые решения, фильтрующие только по спискам и категориям, основанным на использовании баз URL, никак не могут обеспечить правильную фильтрацию создаваемого пользователями контента (Web 2.0). В социальных сетях, на блогах и на форумах есть и позитивная, и негативная информация, для анализа которой может применяться контент-фильтрация.

Актуальность темы защиты детей от вредоносных интернет-сайтов подчёркивается изменениями в законодательстве Российской Федерации. В частности, в июле 2012 года был принят Федеральный закон №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», в котором было введено понятие Единого реестра доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. Тем не менее, процедура ограничения доступа к вредоносным сайтам показывает свою неэффективность, попутно возникают побочные эффекты, нарушающие связность Интернета — например, ввиду того, что блокировка сайтов ведётся по IP-адресам, а на одном IP-адресе может находиться множество сайтов, страдают многие пользователи виртуальных хостингов.

Ситуация усугубляется тем, что несовершеннолетние подвергаются риску получить зависимость от сайтов сомнительного содержания. В соответствии со ст. 14 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» и ст. 10 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в каждом российском учебном заведении должно быть установлено специальное программное обеспечение, регулирующее доступ к интернет-сайтам. При этом может использоваться и фильтрация на уровне оператора связи, и шлюзовое решение, и интернет-фильтр для персональных компьютеров (далее – ПК).

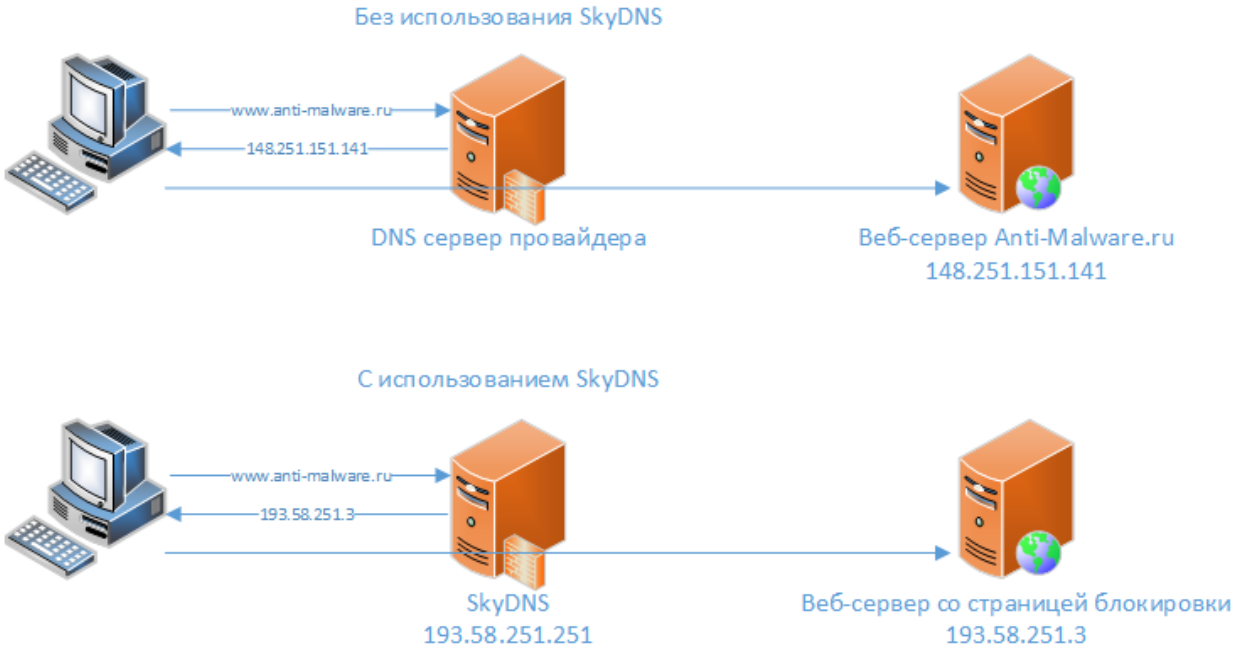
Итак, рассмотрим основные программные продукты по ограничению в образовательных организациях или домашних компьютерах доступа детей к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

1. SKYDNS

Технология работы SkyDNS основана на применении облачного DNS-сервера, который настраивается у пользователей сервиса вместо DNS-сервера провайдера. Система доменных имен (DNS) используется для преобразования доменного имени, символьной последовательности из букв и цифр в IP-адрес, используемый для непосредственной связи с удаленным устройством. Например, когда пользователь набирает в браузере адрес сайта www.anti-malware.ru, DNS-клиент в операционной системе запрашивает DNS-сервер (адрес которого он узнает из сетевых настроек, обычно настроенный на сервер провайдера)

реальный адрес веб-сервера и получает ответ — 148.251.151.141, уже по этому IP-адресу с помощью протоколов сетевой маршрутизации осуществляется доступ к веб-сайту. Если нужно запретить доступ к www.anti-malware.ru, достаточно изменить ответ от DNS-сервера и передать пользователю информацию о другом IP-адресе, где вместо ожидаемого сайта будет отображена страница с информацией о блокировке. SkyDNS предоставляет адрес собственного DNS-сервера, который устанавливается в настройках операционной системы или сетевого оборудования и производит фильтрацию по заданным параметрам.

Рисунок 1. Схема доступа к сайту без использования SkyDNS и после перехода на SkyDNS



SkyDNS использует один IP-адрес DNS-сервера для всех клиентских подключений, но позволяет выполнить гранулярные настройки правил фильтрации для разных заказчиков и профилей. Для того чтобы определить аккаунт клиента и необходимый профиль фильтрации, используется один из двух вариантов — привязка профиля к внешнему IP-адресу компьютера (если доступ в интернет осуществляется напрямую, без NAT-трансляции), либо с помощью установки на компьютер программы SkyDNS Agent для Windows или использования роутеров ZyXEL Keenetic со встроенным модулем SkyDNS. Техническим недостатком схемы работы SkyDNS можно считать относительную легкость обхода блокировок. Без дополнительных настроек пользователь может изменить DNS-сервер на своем устройстве для полного обхода блокировки или прописать в служебный файл hosts IP-адреса отдельных веб-сайтов, на которые ему необходимо попасть. Чтобы снизить вероятность обхода, нужно запретить доступ к другим DNS-серверам на уровне сетевого шлюза или установить ограничения в операционной системе, если доступ осуществляется только с администрируемых компьютеров, что в случае решения SkyDNS легко сделать даже не самому квалифицированному администратору. Функциональные возможности

Функциональные возможности SkyDNS:

Фильтрация по категориям — гранулярная настройка доступа к сайтам по категориям из встроенной базы данных SkyDNS.

Белые и черные списки — поддержка ведения собственных списков разрешенных и запрещенных сайтов, возможность запретить доступ к любому сайту по его адресу, возможность разрешить доступ только к сайтам из белого списка и возможность настройки исключений.

Поддержка профилей — для обеспечения определенного поведения контентного фильтра для разных пользователей (родители и дети, преподаватели и ученики, сотрудники

различных отделов) сервис SkyDNS поддерживает возможность создания разных профилей, разделение на которые осуществляется с помощью приложения SkyDNS (в том числе для разных учетных записей одного компьютера), модуля в роутерах ZyXEL Keenetic или путем привязки профиля к конкретному внешнему IP-адресу.

Статистика — отображение графиков активности по доступу в интернет, графики посещения веб-сайтов, перечень заблокированных ресурсов и статистика по категориям.

Безопасный поиск — специальный сервис, позволяющий выполнить принудительное перенаправление со всех поисковых систем на встроенный безопасный поиск SkyDNS.

Фильтрация рекламы — внутренняя база SkyDNS насчитывает большое число серверов, используемых для отображения и распространения рекламы. С помощью блокировки рекламных сайтов SkyDNS обеспечивает защиту от рекламных баннеров, объявлений, всплывающих окон и других типов рекламы.

Мобильная защита — дополнительный DNS-сервер, который обеспечивает защиту по преднастроенному профилю, предназначенный для установки на мобильных устройствах и обеспечения безопасного веб-серфинга для детей. В этом режиме принудительно включаются безопасные режимы в поисках «Яндекса» и Google. Дополнительные параметры и настройки блокировок не поддерживаются в мобильной защите. Настраиваемые страницы блокировок — опция для организаций и учебных заведений, позволяющая заменить стандартное сообщение о блокировке своей информационной страницей, отображающей произвольную информацию.

Расписание работы — поддержка настройки различных правил фильтрации по времени суток, актуально для бизнес-пользователей, желающих разрешить доступ сотрудников к запрещенным сайтам в нерабочее время, а также для родителей, которые ограничивают доступ детей к развлекательным ресурсам по времени суток.

Связывание доступа к DNS-серверу с конкретным пользователем и профилем настроек осуществляется с помощью указания внешнего IP-адреса или имени в сервисе работы с динамическими IP-адресами DynDNS (поддерживаются любые сервисы и API-обновления), а также с помощью специального приложения под ОС Windows «SkyDNS Агент» в случае, если доступ к сети осуществляется через NAT и прямой адрес отсутствует. Агент SkyDNS позволяет управлять основными настройками фильтрации (категории сайтов, белые и черные списки и т. д.), а также связывать профили настроек SkyDNS с пользователями локального компьютера. Приложение защищено от удаления и изменения настроек с помощью пароля от учетной записи, но не следит за неизменностью настроек DNS-сервера и не проверяет файл hosts, поэтому мы не рекомендуем использовать приложение, если у пользователя есть права локального администратора. Встроенная база сайтов насчитывает 58 категорий и постоянно пополняется URL-адресами. Все категории разделены на группы, что позволяет быстрее выполнять поиск. Перечень доступных групп и категорий:

Черные сайты — вредоносные страницы, ресурсы, не рекомендованные для доступа детей, сайты для обхода блокировок. Для ряда категорий, связанных с безопасностью, возможна отправка уведомлений администратору при попытке доступа к ним.

Сайты для взрослых — интернет-площадки с рекламой и пропагандой алкоголя и табака, сайты знакомств, онлайн-казино, лотереи, тотализаторы, сайты с информацией порнографического содержания.

Пожиратели трафика — сервисы онлайн-стриминга, радиостанции, музыкальные сайты, торренты, файлохранилища, фотогалереи и онлайн-кинотеатры.

Пожиратели времени — развлекательные сайты, социальные сети, форумы, чаты и мессенджеры.

Прочие сайты — большой набор интернет-ресурсов различных категорий — авто, бизнес, блоги, здоровье, хобби и другие.

Запрещенные законодательно сайты — данная группа доступна для учебных заведений и провайдеров, блокирует сайты из реестра Роскомнадзора и экстремистские сайты из реестра Министерства юстиции.

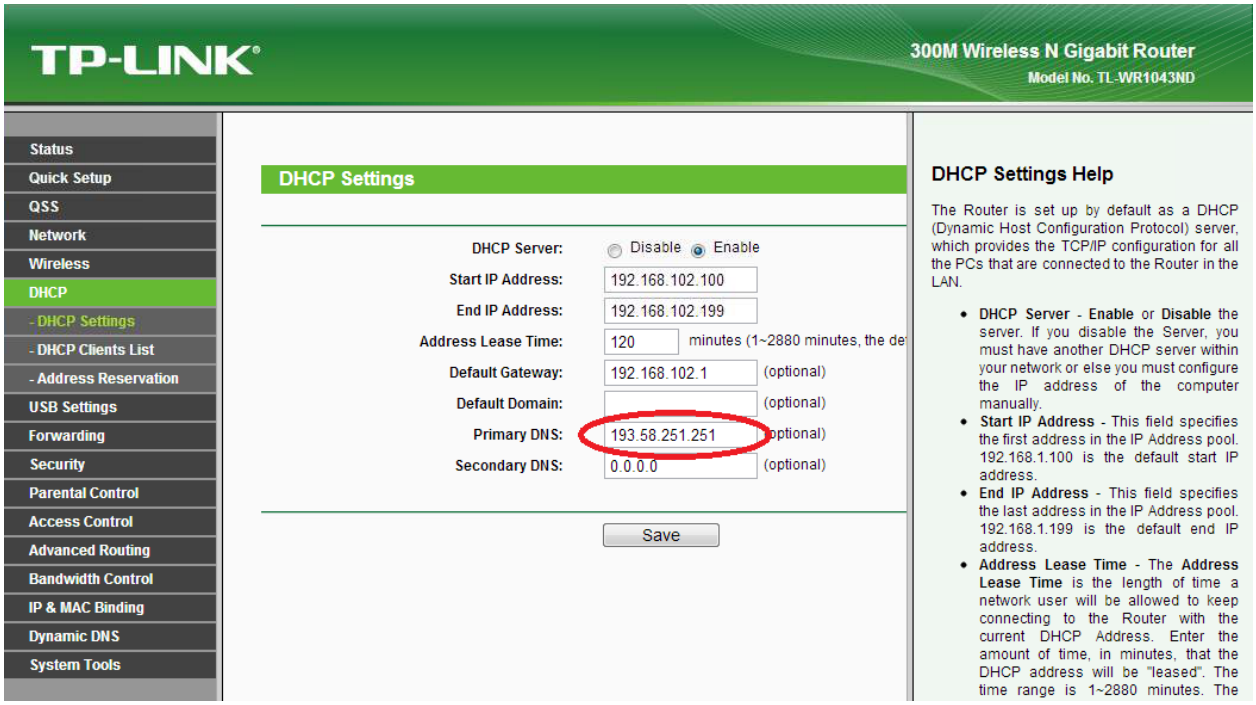
Лицензирование и тарифы

Сервис SkyDNS предоставляется по подписке, при этом пользователям предлагается три коммерческих вида тарифов и бесплатная версия с рядом ограничений. Базовая бесплатная версия предназначена для персонального некоммерческого использования, позволяет фильтровать сайты по категориям, задавать список исключений не более чем из 20 доменов и собирать статистику только за один месяц работы. Кроме того, в бесплатной версии не блокируются рекламные баннеры, отсутствуют профили настроек, «детский режим» и работа с сервисами DynDNS. Платные тарифы разделяются по целям использования. Тариф «Премиум» предназначен для домашних пользователей, предоставляет доступ ко всем функциям продукта, поддерживает до 3 профилей настроек, до 50 записей в списке исключений и хранение статистики за 6 месяцев работы; стоимость — 395 рублей в год без ограничения на число используемых компьютеров. Тариф «Школа» предназначен для учебных заведений, включает в себя все функции, кроме мобильной защиты, поддерживает до 10 профилей, 400 записей в списке исключений и хранение данных за 1 год. Тариф «Бизнес» для коммерческих организаций аналогичен тарифу «Школа», за исключением количества профилей (их 5) и размера списка — до 1000 записей. Стоимость тарифов «Школа» и «Бизнес» рассчитывается индивидуально и начинается от 300 и 360 рублей за один компьютер в год соответственно. SkyDNS также предлагает готовые решения в виде программно-аппаратных комплексов с использованием сетевых Wi-Fi-маршрутизаторов ZyXEL Keenetic с модулем SkyDNS для учебных заведений, библиотек и организаций, а также платформы контент-фильтрации операторского класса SkyDNS ISP Go и системы Zapret ISP для организации у провайдеров фильтрации трафика по реестру запрещенных сайтов Роскомнадзора.

Установка и начало работы

Работа со SkyDNS начинается с регистрации личного кабинета на официальном сайте сервиса. При регистрации выбирается будущий тариф — «Премиум» (для домашних пользователей), «Бизнес» или «Школа». Первые 15 дней любой из тарифов действует бесплатно, по окончанию этого срока тариф «Премиум» переключается на тариф FREE, а коммерческие тарифы отключаются. Для регистрации по домашнему тарифу достаточно указать e-mail и придумать пароль для доступа, на тарифах для бизнеса и учебных заведений дополнительно требуется ввести контактные данные и название учреждения. После регистрации в личном кабинете доступна информация об адресе DNS-сервера, инструкции по настройке и ссылки для скачивания агента SkyDNS для Windows. Установка SkyDNS, как уже упоминалось выше, производится с помощью смены DNS-сервера на маршрутизаторе или локальном компьютере, либо с помощью установки программы «SkyDNS Агент». Смена DNS-сервера осуществляется по-разному для разных устройств и операционных систем, и этот процесс подробно описан в документации к устройствам и на сайте SkyDNS.

Рисунок 2. Изменение DNS-сервера на примере домашнего маршрутизатора TP-LINK

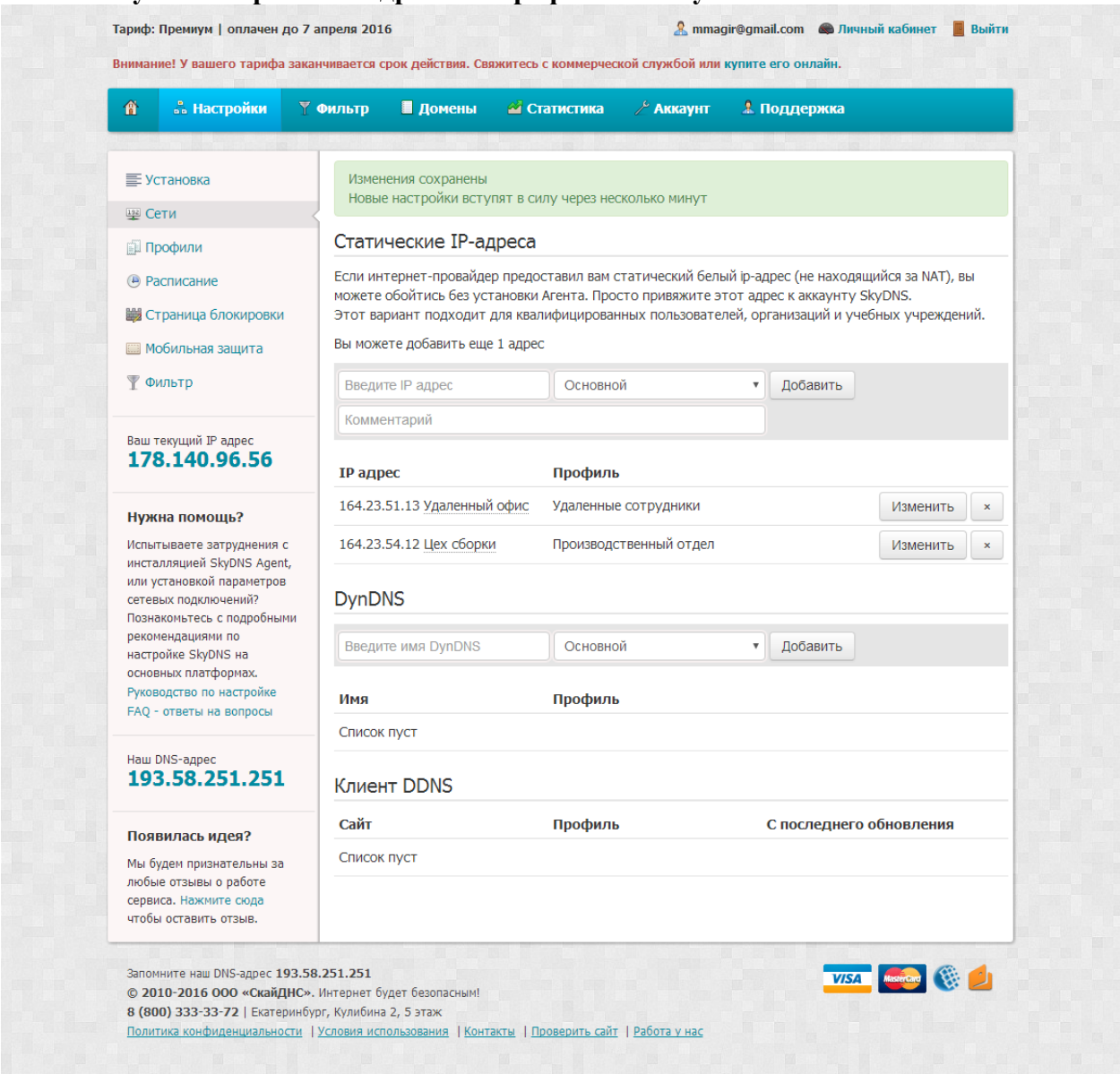


Установка агента SkyDNS осуществляется с помощью стандартного мастера, запрашивающего путь для установки приложения и предлагающего запустить программу после развертывания.

Настройка и управление

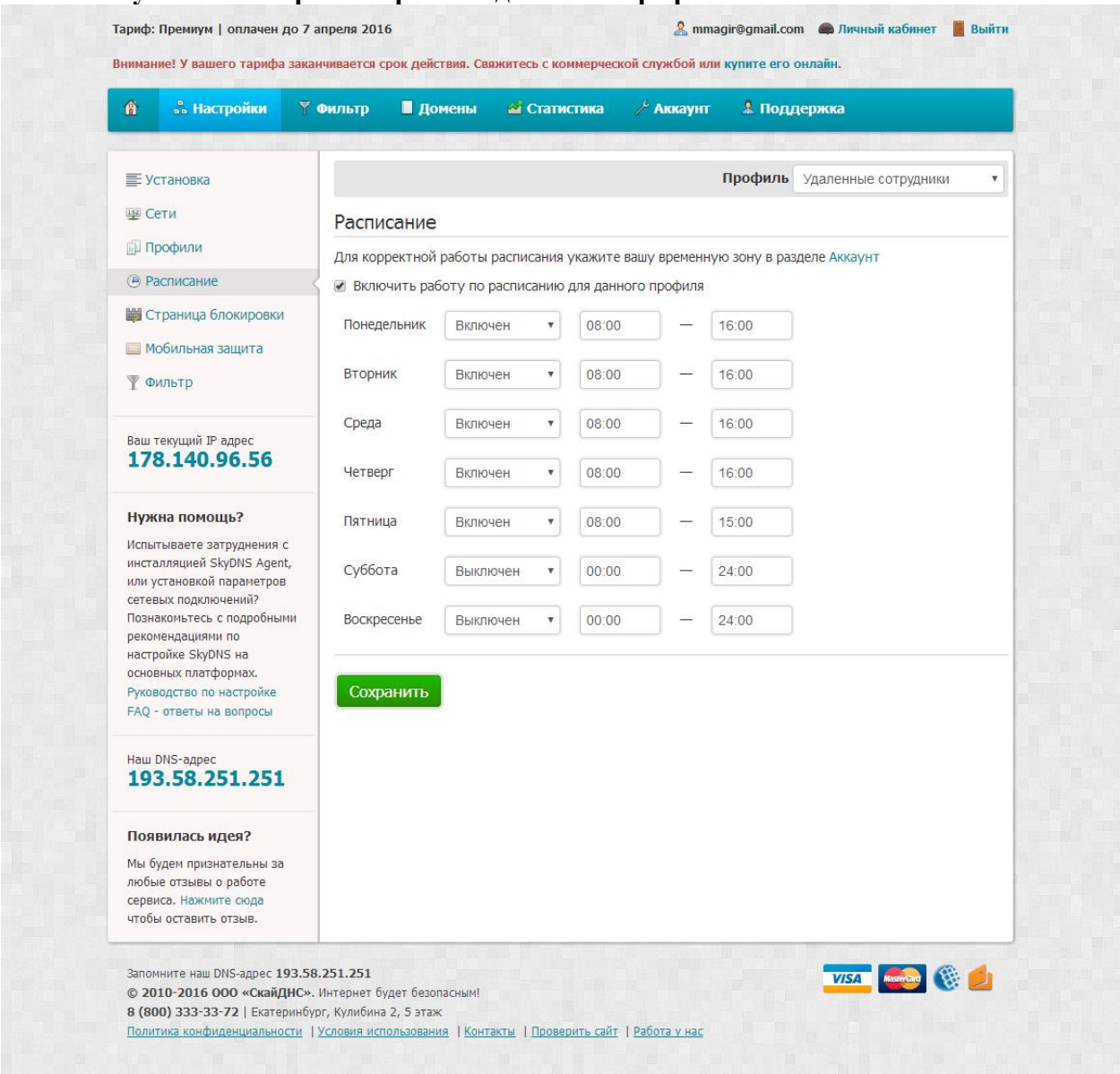
Настройки выполняются из веб-интерфейса в личном кабинете на сайте SkyDNS. Весь интерфейс состоит из пяти основных разделов — «Настройки», «Фильтр», «Домены», «Статистика» и «Аккаунт». Также из личного кабинета доступен раздел «Поддержка», откуда можно отправить обращение в техническую поддержку SkyDNS и получить оперативный ответ. В разделе «Настройки» находится семь подразделов, на первом экране описаны способы установки SkyDNS и ссылка на загрузку дистрибутива агента. В подразделе «Сети» настраивается привязка внешних IP-адресов или DynDNS-имен к профилям настроек.

Рисунок 3. Привязка адресов к профилям в SkyDNS



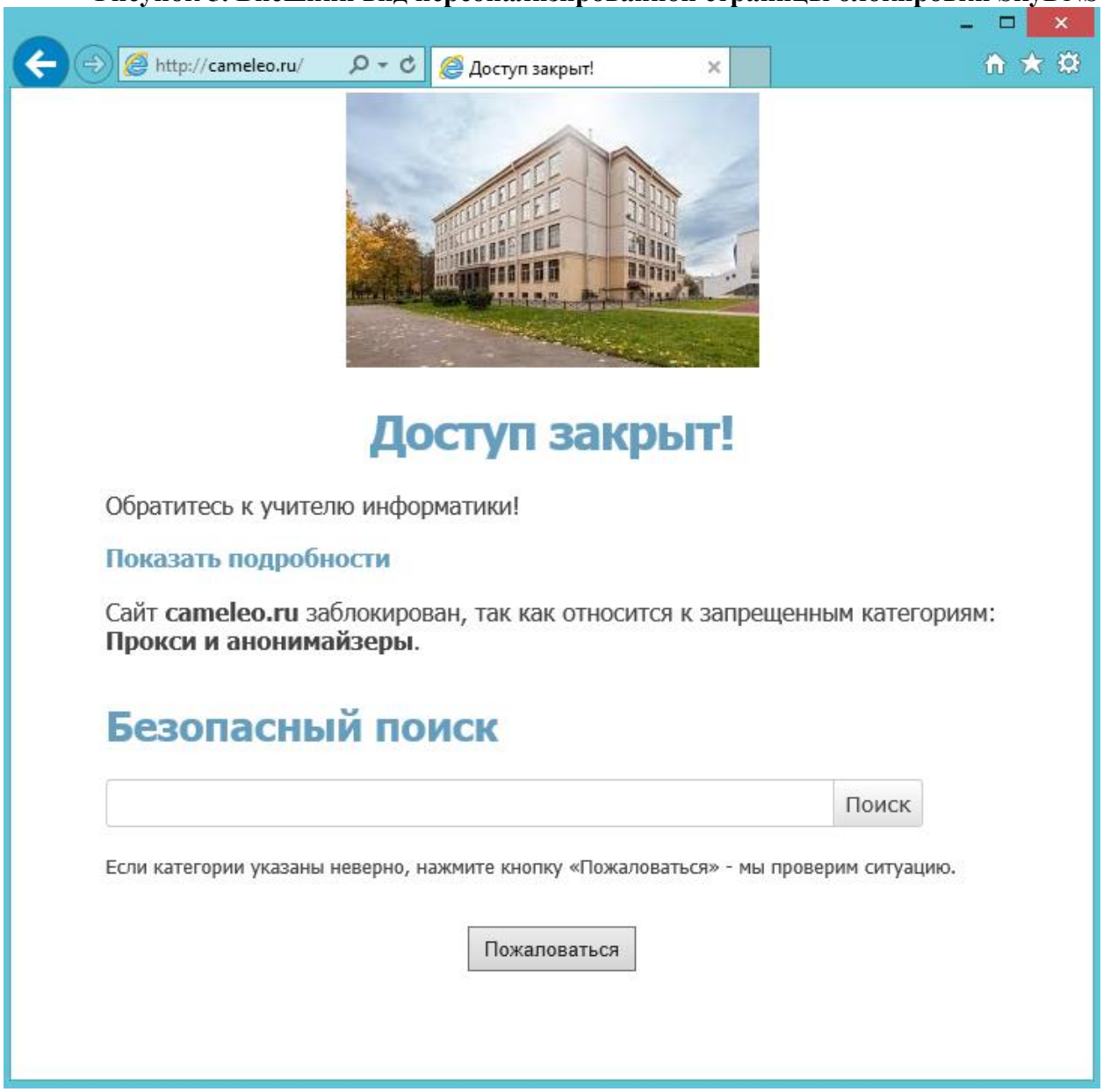
В разделе «Профили» — управление профилями, их создание, смена названия и удаление. Расписание работы профилей по времени суток и дням недели настраивается из подраздела «Расписание». Расписание устанавливается для каждого профиля в отдельности, переключение профилей выполняется с помощью выпадающего меню в правой верхней части экрана. На тарифах для организаций предлагается расширенный вариант расписания с возможностью нескольких несвязанных диапазонов расписания в течение суток.

Рисунок 4. Настройка времени действия профиля



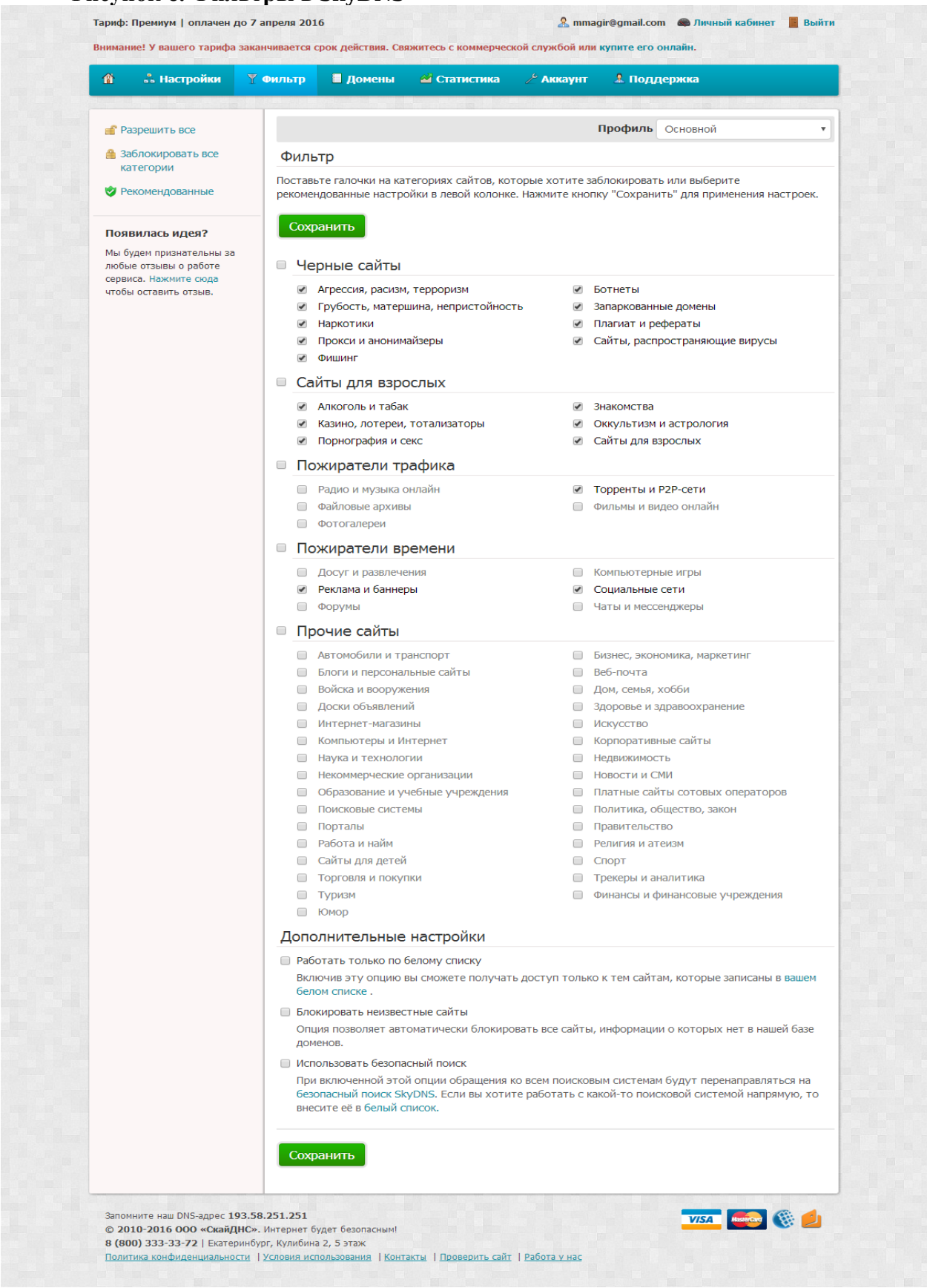
В подразделе «Страница блокировки» настраивается персональный внешний вид сайта, отображаемого вместо заблокированных. Данная настройка применяется на весь аккаунт и не привязывается к профилю. В качестве страницы блокировки можно выбрать стандартный вариант, персонализированный с указанием текста и изображения, и отключить экран блокировки (в этом случае либо эмулируется ошибка веб-сервера, либо отправляются пустые DNS-ответы). На тарифах для организаций дополнительно предлагается HTML-режим, позволяющий полностью переделать внешний вид страницы блокировки.

Рисунок 5. Внешний вид персонализированной страницы блокировки SkyDNS



Подраздел «Мобильная защита» содержит информацию о работе DNS-сервера для мобильных устройств и инструкцию по изменению DNS-сервера в iOS и Android. В подразделе «Фильтрация» находится кнопка для включения или отключения всей фильтрации на аккаунте. В разделе «Фильтры» находится выбор категорий сайтов для блокировки. Так же, как и расписание, фильтры применяются к отдельным профилям. Доступны кнопки быстрого выбора всех фильтров и переключения выбора на рекомендованные настройки.

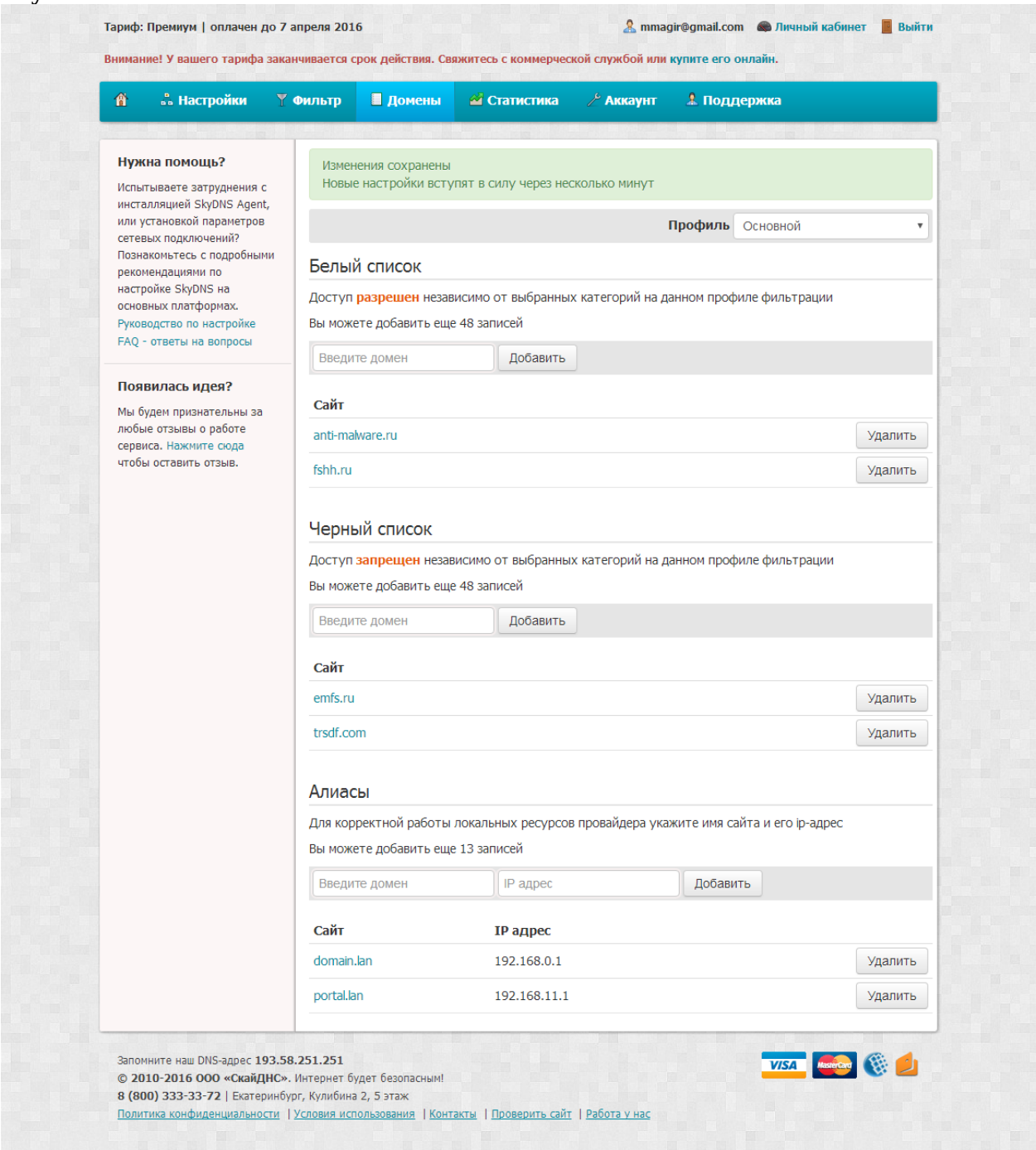
Рисунок 6. Фильтры в SkyDNS



Произвольные домены могут быть внесены в черный или белый список в разделе «Домены». Домены, занесенные в белый список, будут доступны вне зависимости от правил фильтрации. Домены в черном списке, соответственно, блокируются в любом случае. Списки доменов могут быть настроены независимо для разных профилей.

Дополнительно в данном разделе могут задаваться алиасы, фактически являющиеся произвольными DNS-записями. В случае, если используются локальные доменные имена или внутренние ресурсы в компании, их можно прописать в SkyDNS.

Рисунок 7. Управление белым и черным списком доменов и алиасами в SkyDNS



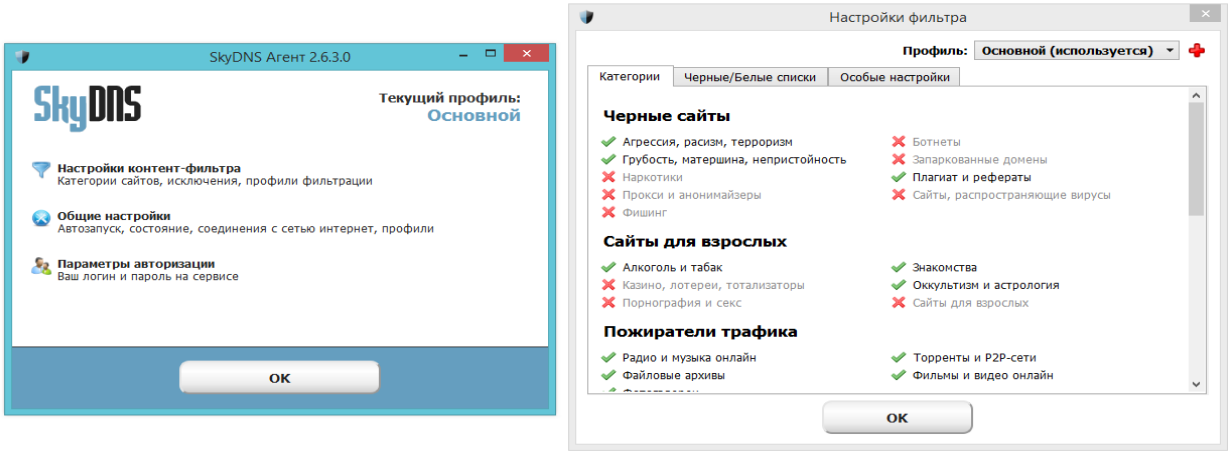
В разделе «Статистика» представлены графики и списки посещения веб-сайтов. На странице выложены повременные графики (за час, сутки, неделю) использования интернета, списки веб-сайтов по количеству посещений, перечень заблокированных адресов и диаграмма популярных категорий сайтов. Поддерживается фильтрация вывода данных по произвольному промежутку времени и просмотр статистики для отдельных профилей. Время хранения статистики зависит от тарифного плана и составляет от 1 месяца до 1 года. При этом на тарифах для школ и организаций предлагаются дополнительные

отчеты с детальной статистикой, возможностью выгрузки отчетов в формате CSV и автоматической отправкой ежемесячных отчетов на e-mail.

Рисунок 8. Статистика посещений сайтов по категориям в SkyDNS

В разделе «Аккаунт» собраны интерфейсы управления учетной записью, контактной информацией, паролями доступа и лицензирования. Здесь отображается текущий тарифный план и доступна возможность оплаты с помощью банковских карт, электронных платежей или со счета мобильного телефона.

Рисунок 9. Интерфейс агента SkyDNS



В интерфейсе агента SkyDNS можно управлять большинством настроек профилей, там также дополнительно представлен ряд опций — управление защитой программы с помощью пароля, опции запуска и автообновления, выбор сетевых интерфейсов для контроля и интерфейс связывания пользователей с профилями фильтрации. Настройки, сделанные в агенте SkyDNS, сразу же отображаются в личном кабинете на веб-сайте, и наоборот, поэтому управлять параметрами работы можно любым из способов без каких-либо ограничений.

Использование в корпоративной среде

Кроме вышеперечисленного, сервис контент-фильтрации SkyDNS содержит множество дополнительных функций, облегчающих его использование в корпоративных сетях, таких как: Возможность создания нескольких администраторов для управления учетной записью в сервисе с ведением полного журнала их действий в кабинете сервиса. Облачная поддержка сервисов и ресурсов Active Directory. Возможность централизованной установки агента SkyDNS в скрытом режиме с заданными настройками. Централизованная настройка сервиса в распределенных сетях и на отдельных компьютерах и мобильных устройствах. Оповещение администратора о наличии зараженных компьютеров в сети, пытающихся обратиться к управляющим серверам ботнетов. Детальная статистика с поддержкой экспорта в формате CSV и автоматическая передача отчета по итогам месяца на e-mail.

Выводы

Облачный сервис контент-фильтрации SkyDNS — бюджетное решение для домашних пользователей, малого и среднего бизнеса, учебных заведений, библиотек и операторов доступа к интернету, которое позволяет разграничить доступ к веб-сайтам и интернет-сервисам без больших финансовых и технических затрат. SkyDNS не требует сложных настроек, подключение доступно для пользователя с любым уровнем компьютерной грамотности — внедрить его можно без привлечения квалифицированных специалистов. SkyDNS позволяет выполнить требования законодательства в части ограничения доступа в интернет для учебных заведений и ответственности оператора по защите детей от нежелательной информации. Для организаций SkyDNS помогает повысить эффективность сотрудников путем запрета доступа к развлекательным ресурсам в рабочее время. Решение обладает гибкими настройками и поддержкой профилей, что позволяет обеспечить гранулярное применение правил фильтрации и не препятствовать полноценной работе в интернете пользователям, которым это разрешено. Например, для учителей в школе можно разрешить доступ без ограничений, применяя при этом все фильтры для доступа учеников. У SkyDNS есть ряд недостатков, связанных с используемыми технологиями. Блокировку, построенную на управлении DNS-запросами, можно обойти с помощью смены DNS-сервера, доступа к сайтам по IP-адресу или записью соответствия домена и адреса в файл hosts. Вместе с тем при правильной настройке сервиса практически

все эти бреши возможно закрыть. Для снижения риска обхода блокировки требуется ряд дополнительных технических мер, не требующих высокой квалификации от специалиста — ограничение прав доступа в операционной системе на рабочих компьютерах, фильтрация DNS-запросов на другие сервера на сетевом оборудовании и т. д.

2. UserGate Proxy & Firewall

Основой решения UserGate Proxy & Firewall является сервер UserGate. Он инсталлируется непосредственно на корпоративный интернет-шлюз и реализует совместное использование глобальной сети, ведение статистики, подсчет трафика и т.п.

Администрирование системы доступа осуществляется с помощью консоли управления. Это отдельное приложение, которое соединяется с сервером по специальному протоколу поверх TCP/IP (используется протокол собственной разработки, передача защищена по технологии Open SSL с длиной ключа 1024 бита), что позволяет использовать его не только локально, но и удаленно. Таким образом, системный администратор имеет возможность управлять UserGate Proxy & Firewall непосредственно со своего рабочего места, не нуждаясь в физическом доступе к интернет-шлюзу.

Помимо этого в UserGate Proxy & Firewall реализован целый ряд дополнительных модулей для решения различных специфических задач.

- **Статистика UserGate**. Отдельное приложение, которое инсталлируется на компьютер ответственных сотрудников, и позволяет им просматривать статистику использования Интернета.
- **Веб-статистика**. Модуль для просмотра статистики удалено через веб-браузер. При необходимости доступ к нему может осуществляться не только из локальной сети, но и из сети Интернет.
- **Обозреватель кэша**. Отдельное приложение для просмотра содержимого кэша, сохраненного UserGate Proxy & Firewall.
- **Клиент авторизации UserGate**. Отдельное приложение, которое устанавливается на компьютерах конечных пользователей, и обеспечивает возможность применения "расширенных" методов авторизации – с использованием Active Directory, Windows-логина и пр.
- **Контроль приложений.** Отдельное приложение, устанавливающееся на рабочие станции. Оно позволяет ограничить перечень программ, которым разрешен доступ в сеть Интернет.

2.1.Системные требования

Системные требования, предъявляемые прокси-сервером к компьютеру, описаны в таблице.

Параметры	Минимальные требования	Рекомендуемая конфигурация
Процессор	1 ГГц	1-2 ГГц в зависимости от числа пользователей
Оперативная память	512 Мбайт	512 Мбайт – 1 Гбайт в зависимости от числа пользователей
Операционная система	Windows 2000/XP/2003/2008/7/2008 R2 (поддерживаются 32- и 64-битные ОС)	
Подключение к Интернету	Тип и пропускная способность определяются в каждом конкретном случае, исходя из потребностей	

2.2.Возможности UserGate Proxy & Firewall

Продукт UserGate Proxy & Firewall обладает широким спектром возможностей по обеспечению совместной работы в сети Интернет, защите корпоративной информационной системы от внешних угроз, контроля использования глобальной сети пользователями.

Организация совместной работы в Интернете

UserGate Proxy & Firewall позволяет организовать совместную работу в Интернете большого количества пользователей. Для этого в нем реализован ряд прокси-серверов (для протоколов HTTP, FTP, POP3, SMTP, SOCKS4, SOCKS5, SIP и H323), собственный NAT-драйвер, система DNS-форвардинга.

Прозрачный режим прокси-серверов

Прокси-сервера в UserGate Proxy & Firewall могут работать в прозрачном режиме. В этом случае не требуется дополнительная настройка программного обеспечения на стороне клиента. Для его реализации используется технология NAT.

Поддержка нескольких провайдеров

Рассматриваемая программа может работать с несколькими сетевыми интерфейсами, подключенными к разным провайдерам. Это позволяет реализовать такие возможности, как перенаправление трафика от разных групп пользователей на различные интернет-каналы, а также резервирование доступа к сети Интернет.

Traffic Manager

В UserGate Proxy & Firewall реализован модуль Traffic Manager, предназначенный для гибкого управления шириной интернет-канала. С его помощью можно указать приоритет различных видов трафика, ограничить скорость передачи данных по определенным протоколам и т.д.

Кэширование

В рассматриваемой программе реализована система кэширования. Она сохраняет загружаемые пользователями файлы на жестком диске интернет-шлюза и, при последующих обращениях к ним, не скачивает их повторно с удаленного сервера. Это позволяет уменьшить загрузку интернет-канала и потребление трафика в целом.

Поддержка IP-телефонии

Интересной особенностью UserGate Proxy & Firewall является поддержка IP-телефонии. Помимо прокси-серверов протоколов SIP и H323, в ней реализованы такие функции, как SIP Registrar (фактически, сервера IP-телефонии) и H323 GateKeeper.

Широкий набор методов авторизации

В UserGate Proxy & Firewall реализовано восемь способов авторизации пользователей. Например, по IP-адресу, по MAC сетевой карты, а также и посредством Active Directory, задаваемых администратором логинов и паролей, учетных записей Windows.

Ограничение трафика и скорости доступа

Рассматриваемый прокси-сервер позволяет устанавливать правила, ограничивающие использование сети Интернет. В частности, можно определить суточный, недельный или месячный лимит потребленного трафика, максимальную скорость передачи данных, разрешенные к использованию протоколы и пр. Правила могут привязываться как к отдельным пользователям, так и к целым их группам.

Биллинговая система

В UserGate Proxy & Firewall реализована собственная биллинговая система, которая может использоваться для подсчета затрат на использование Интернета. Тарифы могут задаваться как временные, так и по потребленному трафику. При этом доступна возможность гибкой их настройки и автоматического переключения с одного на другой в зависимости от времени суток или категории просматриваемого сайта.

Контроль приложений

UserGate Proxy & Firewall позволяет ограничить перечень приложений, которым разрешен доступ в сеть Интернет. Это позволяет решить задачу единообразия использования программного обеспечения в локальной сети. Кроме того, данный модуль может служить средством дополнительной защиты от вредоносных программ. Даже если они будут на компьютере в активном состоянии, интернет-канал для них будет недоступен.

Фильтрация по категориям

Рассматриваемый прокси-сервер позволяет ограничить доступ к нежелательным сайтам по категориям. Для этого используется "облачная" технология Entensys URL Filtering. В ее основе лежит специальная база данных сайтов, разделенная на 82 категории. Именно по ним и можно ограничивать доступ. База данных содержит более 500 миллионов веб-проектов, постоянно дополняется и редактируется разработчиками. Стоит отметить, что использование фильтрации по категориям требует приобретения дополнительной лицензии.

Контроль приложений

В UserGate Proxy & Firewall реализована система фильтрации трафика на основе приложений, которые его генерируют. Это позволяет разрешить выход в Интернет одного ПО и блокировать сетевую активность другого. Стоит отметить высокую гибкость правил фильтрации. С их помощью можно разрешить приложениям работу лишь по определенному протоколу, передачу сетевых пакетов только на указанный IP-адрес или диапазон IP-адресов и пр. Для реализации такого вида фильтрации требуется установка на рабочие станции специальной программы «Контроль приложений», входящей в комплект поставки продукта.

Статистика и отчеты

Рассматриваемый прокси-сервер ведет подробнейшую статистику использования сети Интернет всеми пользователями. Работа с ней осуществляется с помощью специального приложения или через веб-интерфейс. При этом реализована система разделения прав доступа, которая позволяет ответственным сотрудниками просматривать полную информацию, а остальным пользователям – только свою статистику. В процессе работы можно применять такие инструменты, как фильтрация по различным условиям, генерация табличных и графических отчетов, импорт данных в формат HTML и программы Microsoft Excel и OpenOffice.org Calc.

Встроенный DHCP-сервер

В UserGate Proxy & Firewall реализован собственный DHCP-сервер, который может раздавать клиентам IP-адреса из указанного администратором пула. Данный инструмент не нужен, если в информационной системе предприятия поднят домен. Однако он может упростить администрирование компьютеров в небольших одноранговых сетях.

Встроенный маршрутизатор

Другим инструментом для администратора является встроенный маршрутизатор. Он позволяет объединить две или несколько локальных сетей, обеспечив прозрачную двустороннюю связь между ними. При этом, можно указать протоколы и службы, которым будет разрешено использование сетевых соединений.

Антивирусная защита

С помощью UserGate Proxy & Firewall может быть организована проверка всего проходящего через прокси-сервер трафика на наличие вредоносных программ. Для этого используются интегрированные модули, разработанные компаниями "Лаборатория Касперского" и Panda Security. Причем проверка трафика может осуществляться либо одним из указанных антивирусных модулей, либо последовательно. Стоит отметить, что использование антивирусных требует приобретения дополнительных лицензий от соответствующих производителей.

Межсетевой экран

В рассматриваемом прокси-сервере реализован полноценный межсетевой экран, который позволяет блокировать нежелательный сетевой трафик и способствует защите от

внешних вторжений. При этом, он весьма прост в настройке. При включении или отключении сервисов и правил назначения портов соответствующие порты будут автоматически открываться или закрываться.

Поддержка VPN

UserGate Proxy & Firewall поддерживает работу с протоколами PPTP и L2TP, которые применяются для связи с VPN-серверами. Это позволяет легко обеспечить безопасные удаленные подключения к информационным ресурсам предприятия или его филиалов.

2.3.Развертывание UserGate Proxy & Firewall и работа с ним

Процедуру развертывания прокси-сервера UserGate Proxy & Firewall можно условно разделить на несколько этапов.

1. Установка программы.
2. Базовая настройка прокси-сервера.
3. Создание правил, реализующих корпоративную политику использования Интернета.
4. Внесение пользователей.

2.3.1. Установка программы

Процедура установки UserGate Proxy & Firewall очень проста и не требует от исполнителя каких-то особых знаний и навыков. В первую очередь загружаем дистрибутив с официального сайта разработчика, запускаем его и выбираем язык работы инсталлятора. В открывшемся приветственном окне нажимаем на кнопку «Далее» (рис.1).

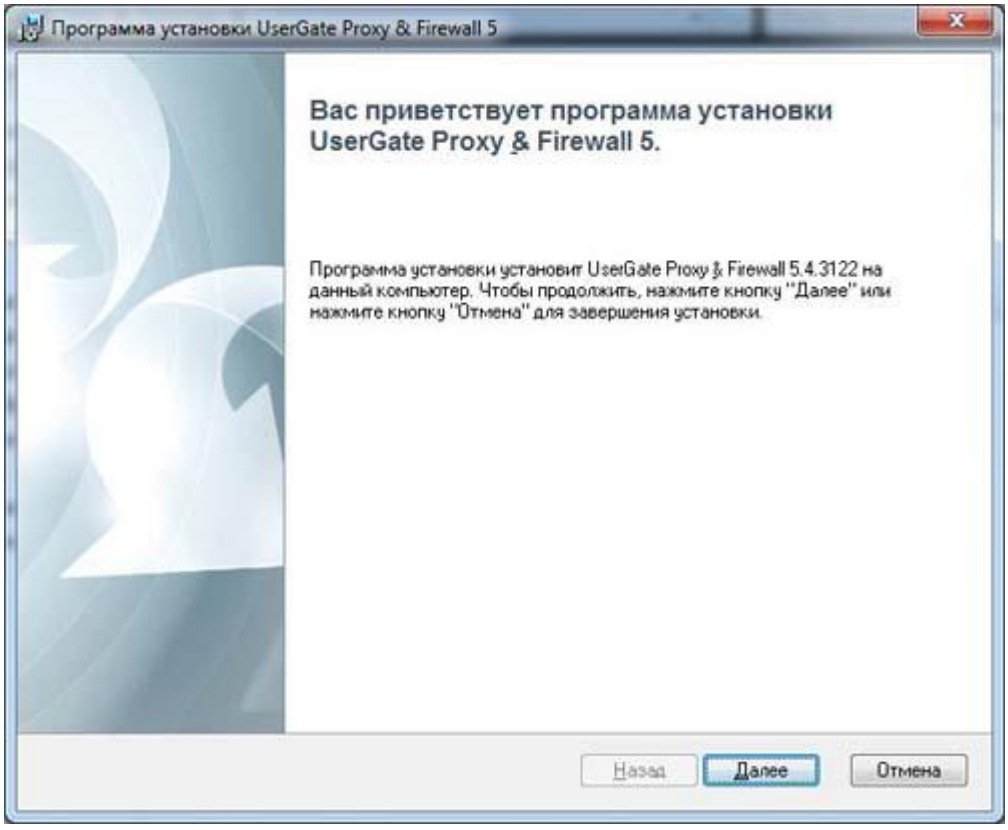


Рисунок 1. Приветственное окно инсталлятора UserGate Proxy & Firewall

На следующем шаге читаем лицензионное соглашение, принимаем его и снова нажимаем на «Далее» (рис. 2).

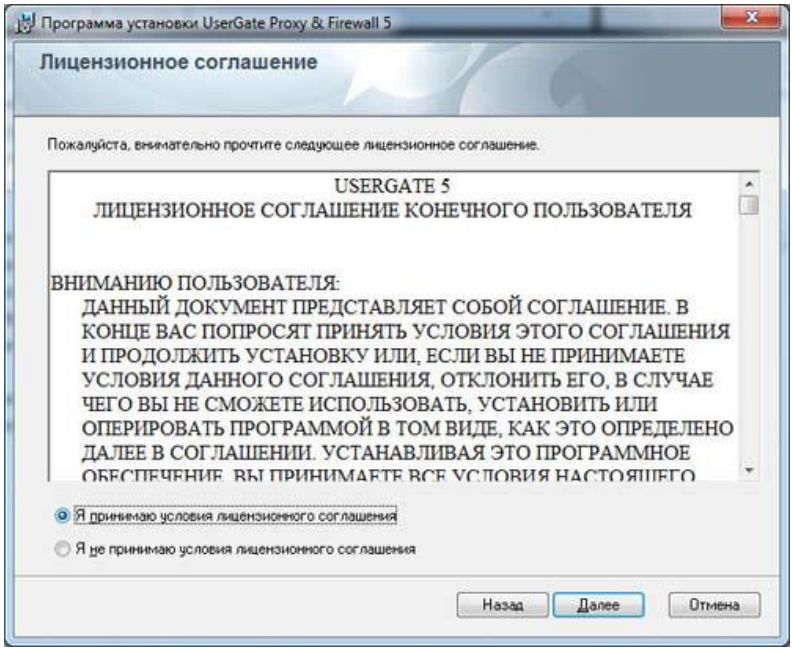


Рисунок 2. Лицензионное соглашение UserGate Proxy & Firewall

Третий этап заключается в выборе устанавливаемых компонентов. Если осуществляется установка программы на интернет-шлюз, то необходимо включить пункт «Базовые файлы UserGate Proxy & Firewall 5» и выбрать в нем необходимые подпункты. Так, например, если у Вас нет лицензии на модули антивирусной проверки или вы не собираетесь использовать веб-статистику, то и устанавливать соответствующие модули нет необходимости. Отдельно можно выбирать консоль управления и компонент «Статистика UserGate». Это может потребоваться при установке продукта на ПК администратора или ответственного сотрудника для удаленного управления прокси-сервером и просмотра отчетности.

Здесь же при необходимости можно изменить папку, в которую будет установлен продукт (по умолчанию используется папка C:\Program Files\Entensys\UserGate 5\).

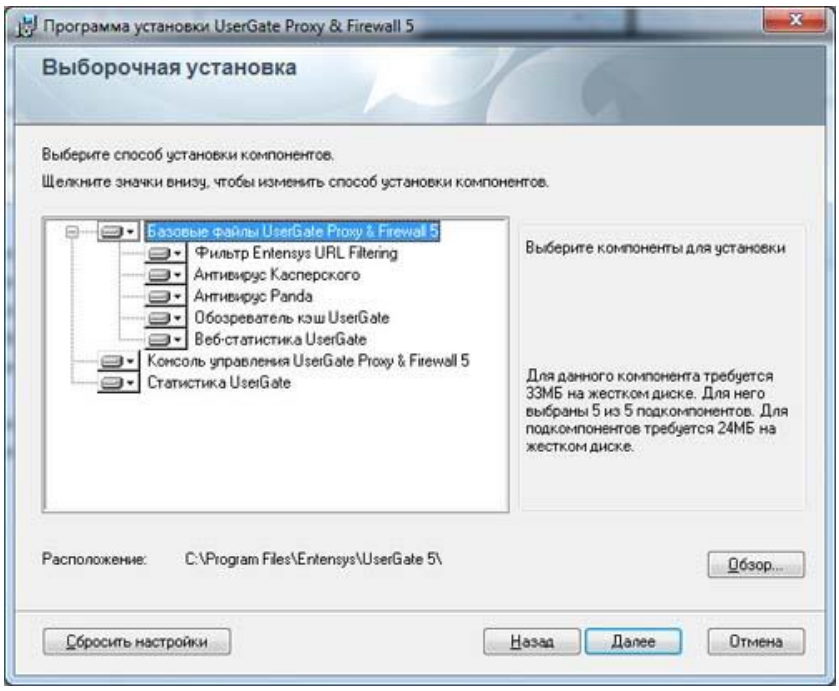


Рисунок 3. Выбор компонентов установки UserGate Proxy & Firewall

После этого отображается заключительное окно инсталлятора, в котором для запуска процесса необходимо нажать на кнопку «Установить» (рис. 4).

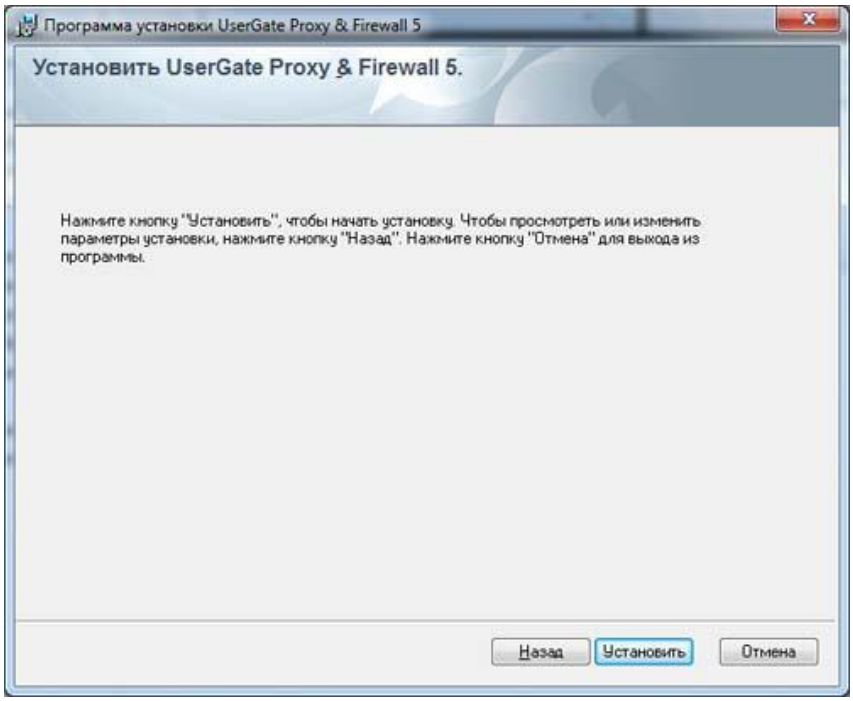


Рисунок 4. Заключительное окно инсталлятора UserGate Proxy & Firewall

Время выполнения процедуры установки зависит от доступных системных ресурсов.

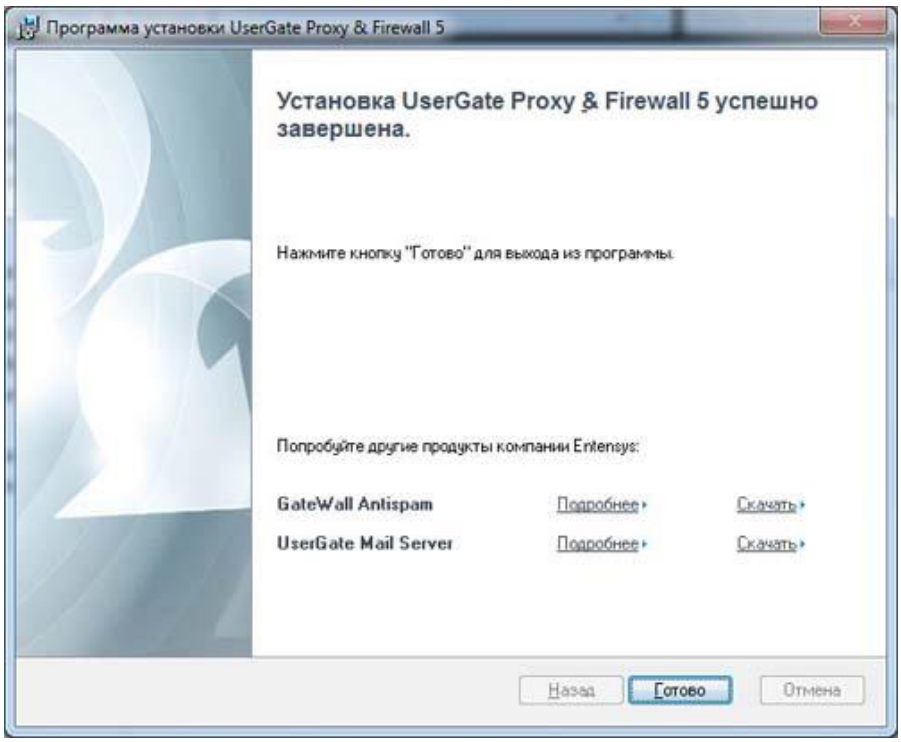


Рисунок 5. Установка UserGate Proxy & Firewall

Для завершения установки требуется перезагрузка компьютера.

3.3.2. Базовая настройка прокси-сервера

Вся работа по администрированию прокси-сервера осуществляется с помощью консоли управления. Ее можно осуществлять как непосредственно с интернет-шлюза, так и удаленно с рабочего места администратора. Если консоль установлена вместе с сервером на одном компьютере, то соединение создается автоматически. В противном случае необходимо настроить подключение вручную – указать доменное имя или IP-адрес сервера, порт (по умолчанию 2345), логин и пароль (рис. 6).

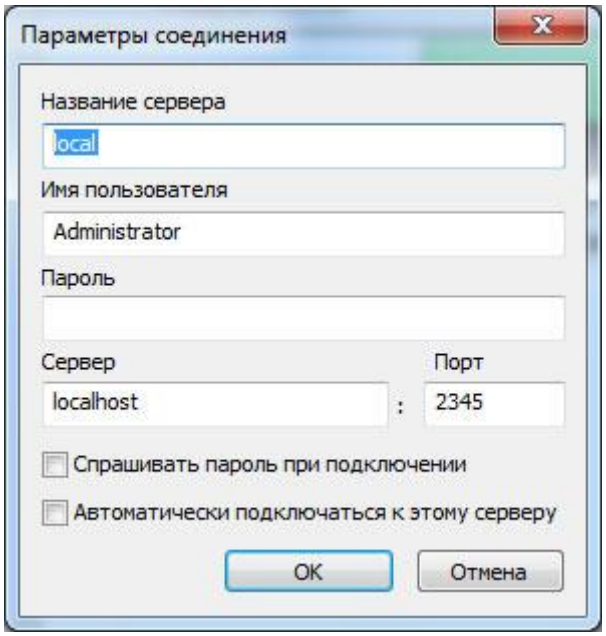


Рисунок 3.6. Настройка подключения к серверу UserGate Proxy & Firewall

После первого подключения к серверу необходимо настроить интерфейсы. Сделать это можно на одноименной вкладке консоли управления. UserGate Proxy & Firewall автоматически определяет все доступные сетевые интерфейсы и отображает их в списке. Выберите среди них те, которые «смотрят» в локальную сеть и измените их тип на LAN. Все внешние интерфейсы должны иметь тип WAN. Помимо сетевых интерфейсов в списке перечислены такие подключения, как PPoE, VPN и пр. Они сразу имеют тип PPP, изменить который нельзя (рис. 7).

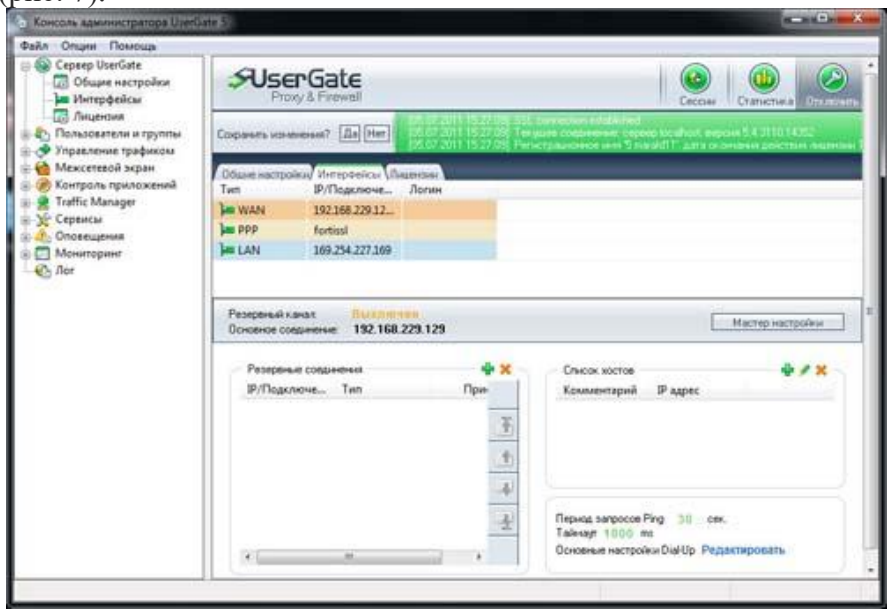


Рисунок 7. Настройка сетевых интерфейсов UserGate Proxy & Firewall

При необходимости можно организовать систему резервирования интернет-канала. Она позволяет автоматически переключаться на другой интерфейса при недоступности основного. Для ее использования необходимо наличие двух или более подключений к сети Интернет. Для настройки резервирования удобнее всего использовать специальный мастер. На первом его этапе укажите основное и резервные соединения (рис. 8).

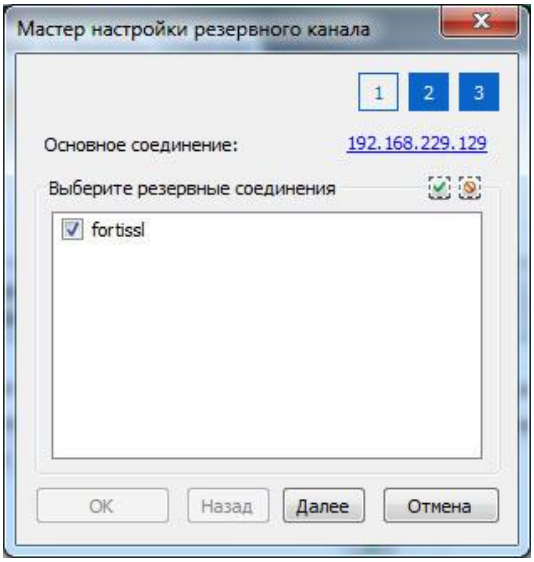


Рисунок 8. Указание основного и резервных соединений в UserGate Proxy & Firewall

На втором этапе введите адреса серверов, недоступность которых будет означать «падение» канала. Обратите внимание, что лучше всего использовать популярные сервисы, причем не один, а несколько. Это позволяет избежать переключение на резервный канал из-за внутренних проблем сервера, магистральной аварии и других подобных причин. Дополнительно можно ввести интервал проверки и таймаут команды Ping (рис. 9).

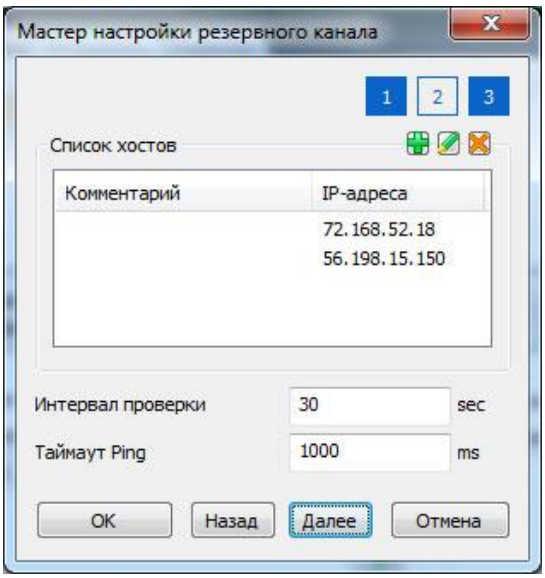


Рисунок 9. Список серверов для проверки работоспособности подключения в UserGate Proxy & Firewall

Все настройки резервирования интернет-канала отображаются на странице «Интерфейсы» консоли управления. Здесь же можно изменять их вручную, не обращаясь к мастеру настройки.

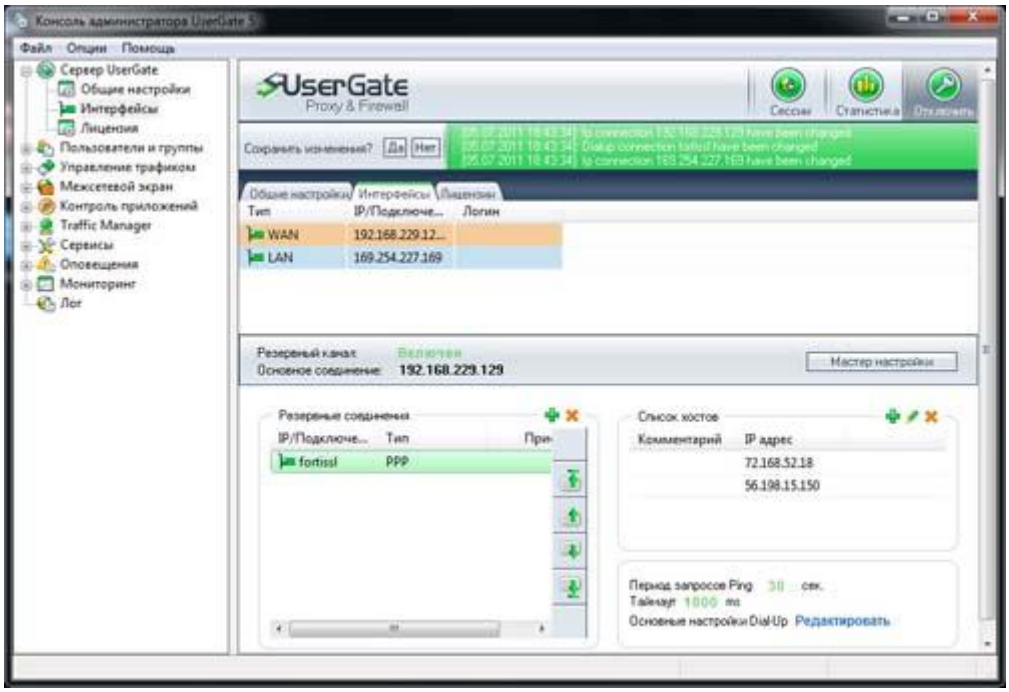


Рисунок 10. Свойства резервирования интернет-канала в UserGate Proxy & Firewall

Далее необходимо настроить прокси-сервера. Для этого откройте в консоли управления раздел «Сервисы» и выберите в нем вкладку «Настройка прокси». При этом в правой части окна будет отображен список всех доступных прокси-серверов. Включите нужные сервисы и выключите все остальные (рис. 11).

Рисунок 11. Список прокси-серверов в UserGate Proxy & Firewall

В случае необходимости можно изменить параметры работы любого прокси-сервера. Осуществляется это в специальном окне, вызываемым двойным нажатием на нужном пункте. В нем нужно указать сетевые интерфейсы, которые будет прослушивать прокси-сервер. В большинстве случаев необходимо выбрать все подключения к локальной сети. В свойствах можно не указывать интерфейсы, но в этом случае UserGate Proxy & Firewall будет прослушивать их все, в том числе и внешние. Здесь же можно изменить и порт, на котором работает прокси-сервер.

Дополнительно в данном окне можно перевести прокси-сервер в так называемый прозрачный режим работы. Суть его заключается в следующем. При включении «прозрачности» драйвер NAT прослушивает соответствующие порты (80 TCP для HTTP, 110 TCP для POP3 и т.д.) интернет-шлюза, обнаруживает поступающие по ним запросы и пересылает их прокси-серверу. В результате этого работа, по сути, ведется через «прокси», однако администраторам уже не нужно настраивать приложения на рабочих станциях. Все они будут работать как при прямом подключении к Интернету. Правда, при использовании прозрачного режима работы необходимо перенастроить свойства сетевого подключения рабочих станций (указать IP-адрес интернет-шлюза в качестве шлюза и ввести DNS-сервер) (рис. 12).

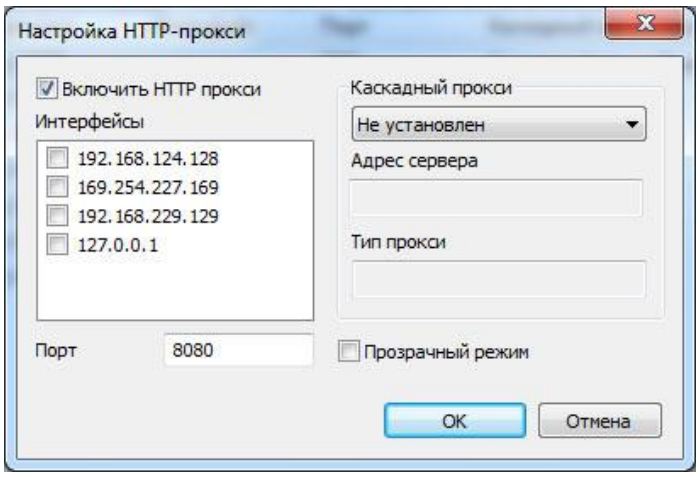


Рисунок 12. Свойства прокси-сервера в UserGate Proxy & Firewall

Далее необходимо обеспечить прохождение через прокси-сервер DNS-запросов. Проще всего это можно сделать с помощью DNS-форвардинга. При использовании данной технологии запросы, поступающие на 53 порт интернет-шлюза (прослушиваются только LAN-интерфейсы) перенаправляются на DNS-сервер провайдера. Для ее включения перейдите на вкладку «Настройка DNS» в разделе «Сервисы». В открывшемся окне включите DNS-форвардинг и укажите адрес DNS-сервера. По умолчанию он будет браться автоматически из настройки сетевой карты WAN-интерфейса. Однако, при необходимости, можно задать собственный список DNS-серверов (рис. 13).

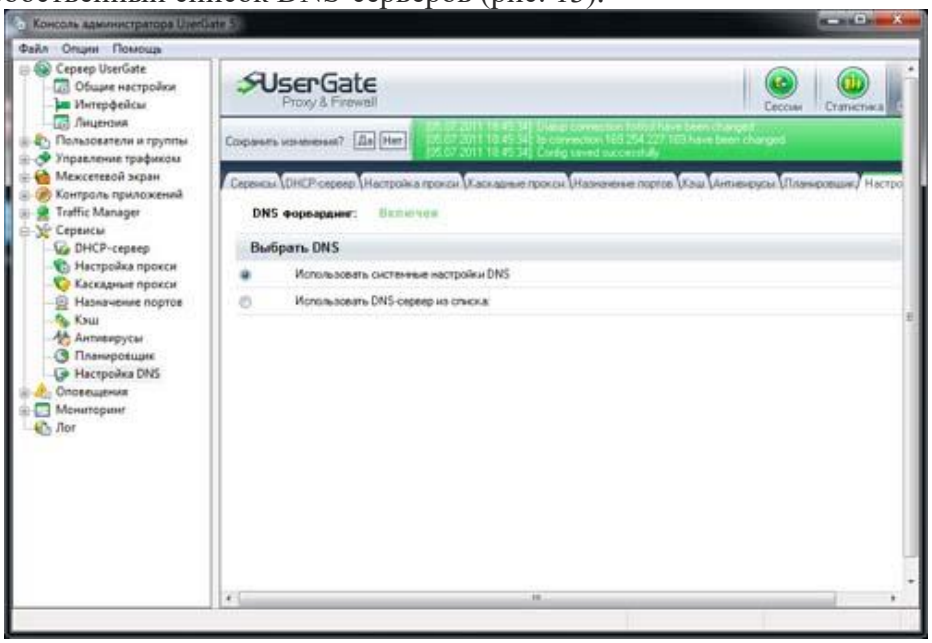


Рисунок 13. Настройка DNS в UserGate Proxy & Firewall

Дополнительно можно настроить такие возможности программы, как общее управление полосой пропускания, перенаправление портов, контроль приложений и пр. Однако подробно разбирать их мы уже не будем: UserGate Proxy & Firewall слишком функционален для описания его полной настройки в рамках одного обзора. Кроме того, данный продукт сопровождается достаточно подробной справочной системой.

3.3.3. Создание правил, реализующих корпоративную политику использования Интернета

Важной особенностью UserGate Proxy & Firewall является система управления трафиком, которая позволяет предотвращать нецелевое использование корпоративных ресурсов сети Интернет сотрудниками организации, усилить защищенность информационной системы и решить ряд других подобных задач. Она основана на правилах, в которых описывается поведение системы в тех или иных случаях. Основная работа с ними осуществляется на одноименной вкладке раздела «Управление трафиком». Здесь их можно создавать, удалять и редактировать. Правил может быть произвольное количество. При этом не обязательно все они должны быть задействованы. Правила присваиваются группам или пользователям и работают только для них.

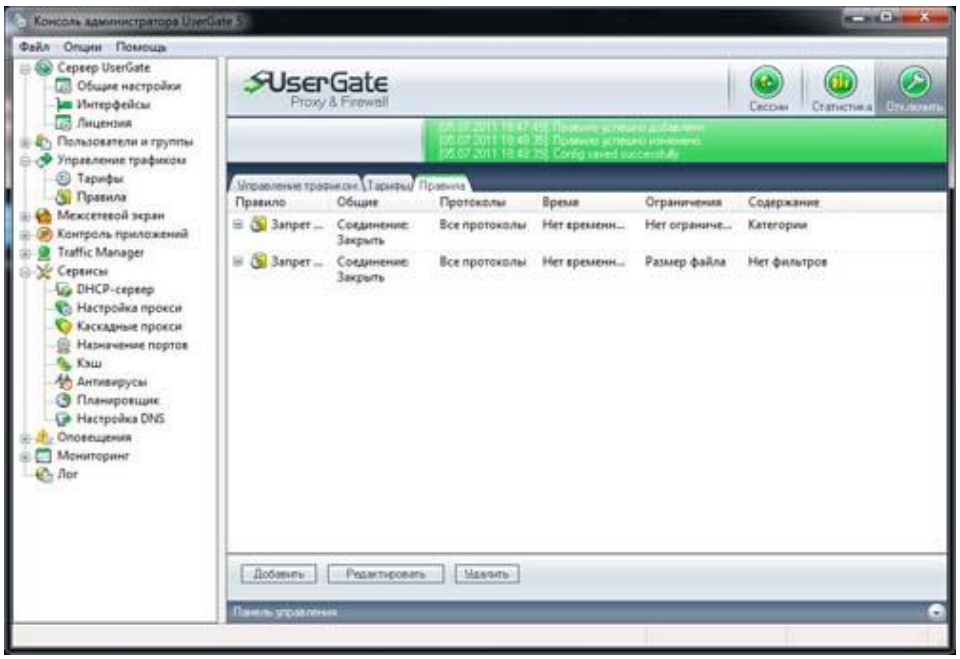


Рисунок 14. Список правил управления трафиком в UserGate Proxy & Firewall

Каждое правило представляет собой одно или несколько условий, объединенных логическими операциями И или ИЛИ. При их выполнении срабатывает заданное действие. Окно свойств правила состоит из пяти вкладок. На первой задаются основные параметры: имя, тип логики, а также объект и выполняемое с ним действие. Здесь доступны такие варианты, как закрыть соединение, отключить подсчет трафика, включить ограничение на скорость и прочее (рис.15).

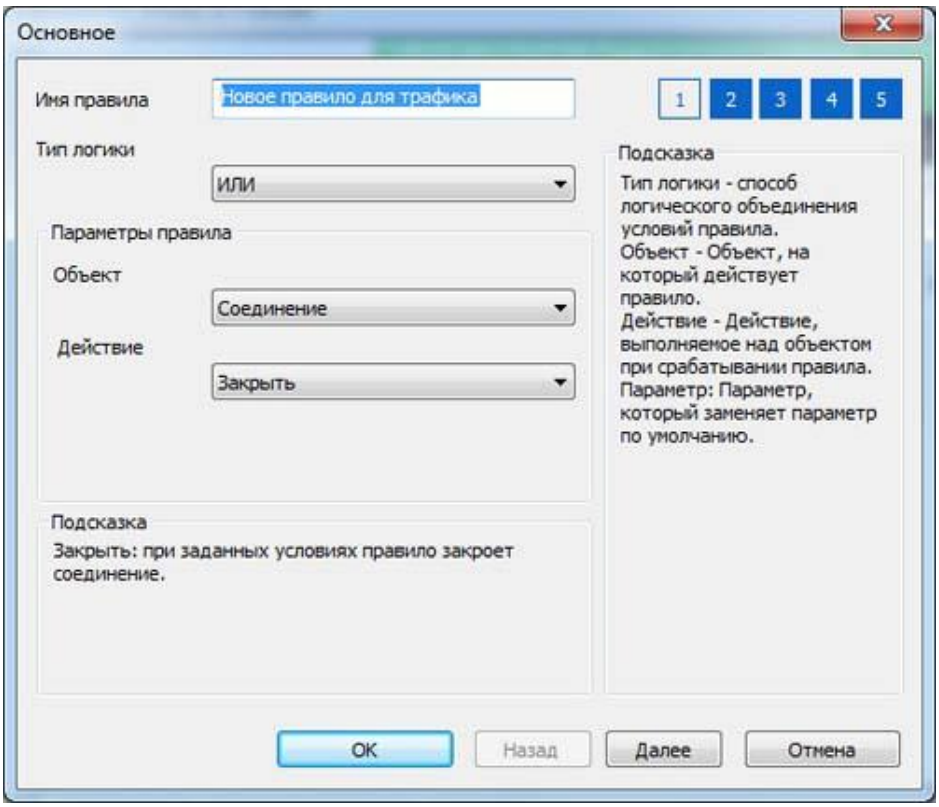


Рисунок 15. Основные параметры правила управления трафиком в UserGate Proxy & Firewall

На второй вкладке указываются протоколы, для которых будет работать правило. По умолчанию они активированы все. Однако администратор может часть из них отключить.

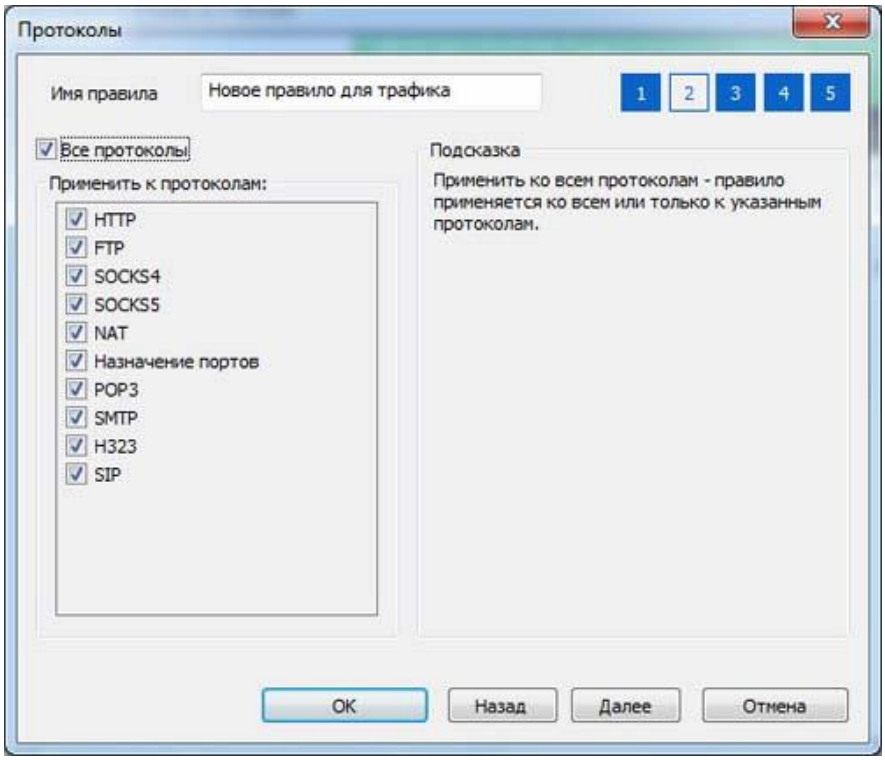


Рисунок 16. Настройка протоколов в правиле управления трафиком в UserGate Proxy & Firewall

Следующая вкладка позволяет задать расписание, т.е. указать время действия правила (рис. 17).

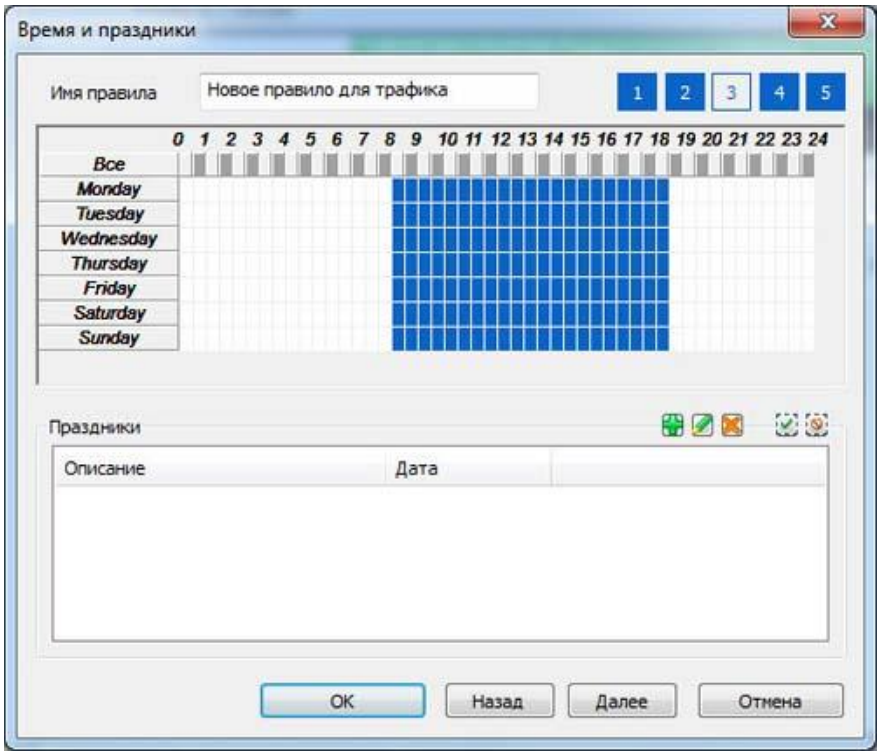


Рисунок 17. Настройка расписания действия правила управления трафиком в UserGate Proxy & Firewall

Четвертая вкладка предназначена для ввода ограничений на суточное, недельное или месячное потребление трафика. Правило будет срабатывать при достижении пользователем определенного лимита. Помимо этого, на данной вкладке можно устанавливать ограничения на размер загружаемых файлов (рис. 18).

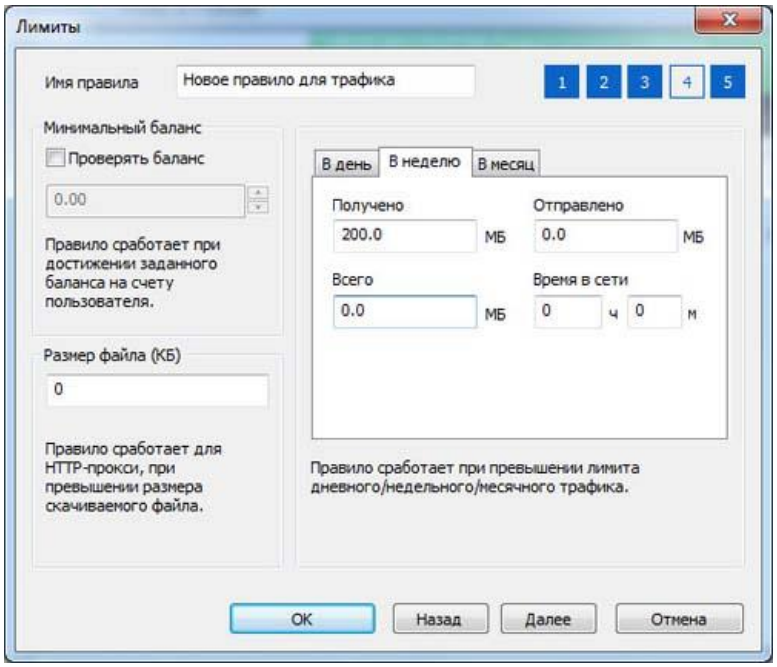


Рисунок 18. Настройка ограничений на потребление в правиле управления трафиком в UserGate Proxy & Firewall

Последняя, пятая вкладка позволяет осуществлять настройку фильтрации веб-контента. На ней можно задать условия четырех разных типов: по IP-адресу (или диапазону IP-адресов), по адресу сайта (в том числе и по фрагменту адреса), по типу контента (по целым категориям – аудио, видео, картинки, текстовые документы и пр. или по отдельным расширениям – *.avi, *.mp3, *.flv и т.д.), а также по категории. Стоит отметить, что тип фильтруемого контента можно задавать.

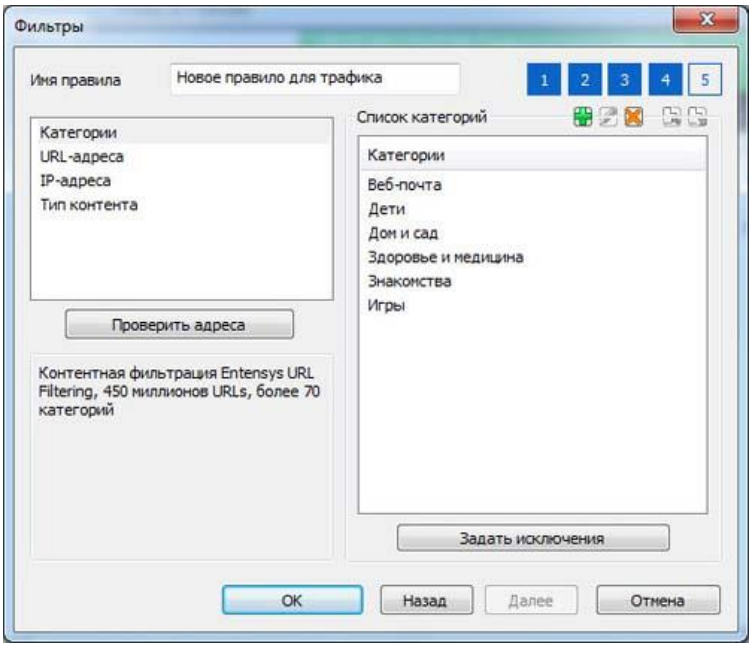


Рисунок 19. Настройка условий фильтрации веб-контента в правиле управления трафиком в UserGate Proxy & Firewall

Описанные выше условия могут комбинироваться в любых сочетаниях, что позволяет создавать очень гибкие правила, описывающие практически любую корпоративную политику использования Интернета.

3.3.4. Внесение пользователей

В UserGate Proxy & Firewall реализовано два способа внесения пользователей: вручную и путем интеграции с Active Directory. Понятно, что первый из них предназначен только для малых организаций, в которых используется простая одноранговая сеть. Если же в организации развернут домен, то гораздо проще и эффективнее использовать интеграцию с Active Directory.

Если выбран второй вариант внесения пользователей, то сначала необходимо настроить параметры синхронизации. Сделать это можно на вкладке «Группы» раздела «Пользователи и группы». Для ввода параметров нажмите на кнопку «Настройка синхронизации с AD» и введите в открывшемся окне наименование домена, адрес контроллера, логин и пароль администратора, а также частоту обновления данных (рис. 20).

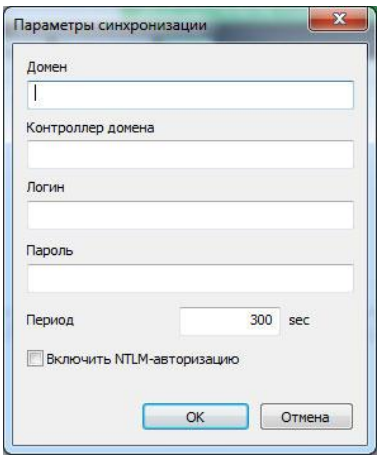


Рисунок 20. Настройка синхронизации UserGate Proxy & Firewall с Active Directory

Работа с учетными записями начинается с ввода групп пользователей, для каждой из которых можно указывать введенные ранее правила. При этом они будут распространяться сразу же на все учетные записи, что упрощает управление.

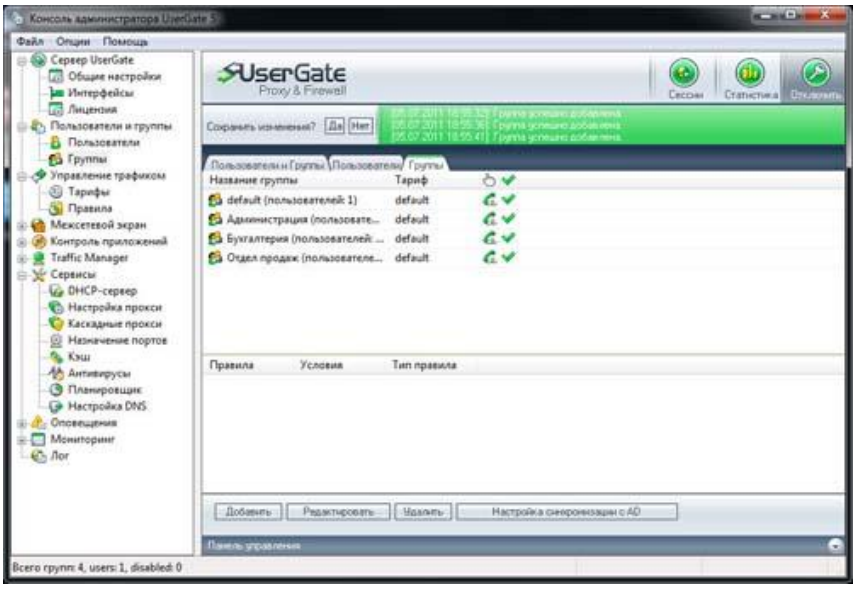


Рисунок 21. Список групп в UserGate Proxy & Firewall

После завершения работы с группами можно приступить к настройке списка пользователей. При ручном способе каждую учетную запись придется вводить самостоятельно, задавая все ее свойства, включая метод авторизации. При синхронизации список учетных записей заполняется и поддерживается в актуальном состоянии автоматически. При необходимости в аккаунты пользователей можно внести изменения, например, установить другой метод авторизации (по умолчанию используется NTLM-авторизация) (рис. 22).

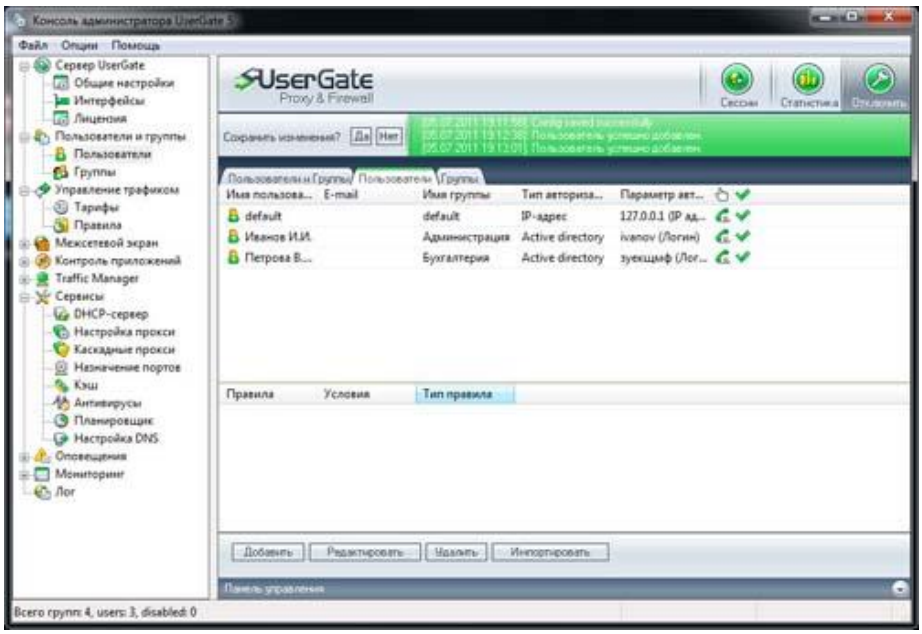


Рисунок 22. Список учетных записей в UserGate Proxy & Firewall

Здесь необходимо сделать небольшое отступление. Для использования некоторых методов авторизации (логин и пароль, введенные в UserGate Proxy & Firewall, Windows-логин, авторизация через Active Directory.) на рабочие станции необходимо установить специальную программу – клиент авторизации UserGate. Его инсталляционный пакет (AuthClientInstall.msi) находится в подпапке Tools каталога установки продукта. Он может быть установлен как вручную, так и с помощью групповых политик Active Directory (рис. 23).

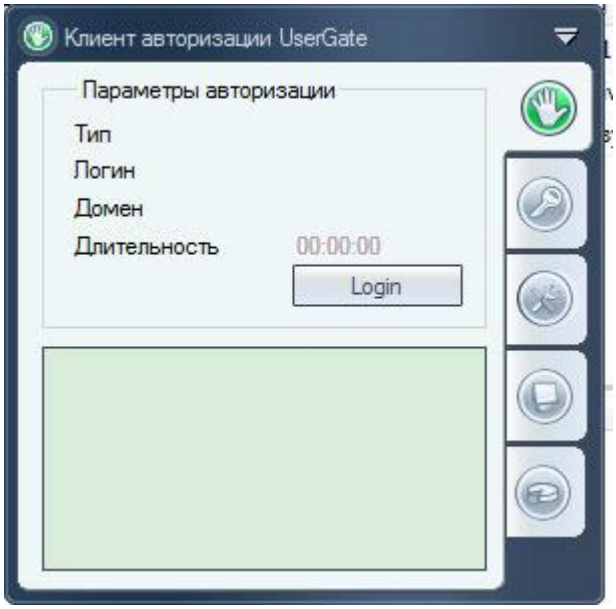


Рисунок 23. Клиент авторизации UserGate

На этом процедуру первоначальной настройки UserGate Proxy & Firewall можно считать законченной. Наш прокси-сервер полностью готов к работе. В будущем администратор может в любой момент подключиться к нему удаленно и изменить заданные ранее параметры.

UserGate Proxy & Firewall относится к приложениям, которые не нуждаются в постоянном внимании со стороны администратора. Подключение к сети Интернет, переключение на резервный канал и обратно, контроль использования глобальной сети сотрудниками компании и другие действия выполняются автоматически. Так что,

фактически, вся дальнейшая работа сводится к изучению статистики и, иногда, изменению некоторых параметров работы.

Для работы с собираемой системой информацией может использоваться специальное приложение – «Статистика UserGate». С его помощью администратор или ответственный сотрудник может просматривать полные данные, фильтруя их по дате, адресу назначения, пользователю, протоколу, категории веб-сайтов и другим параметрам, а также экспортировать их в разных форматах (рис. 24).

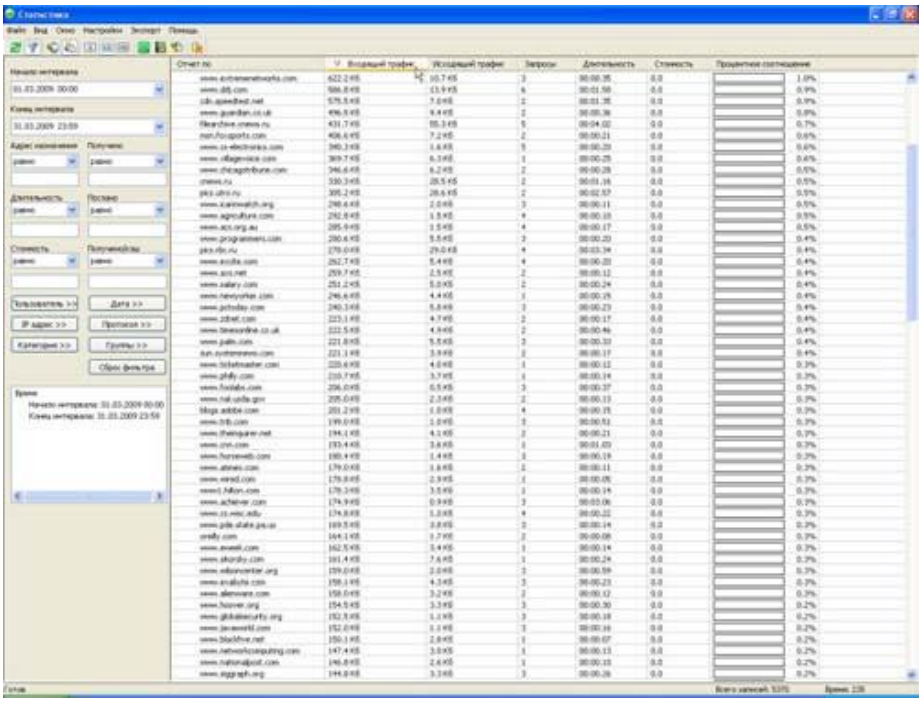


Рисунок 24. Просмотр статистики с помощью специального приложения

Есть и другой вариант просмотра собираемой информации – веб-статистика. С ее помощью можно изучать данные с помощью браузера. Интересно, что делать это могут не только администраторы, но и простые пользователи. При этом, им будет доступна только их личная статистика (рис. 25).

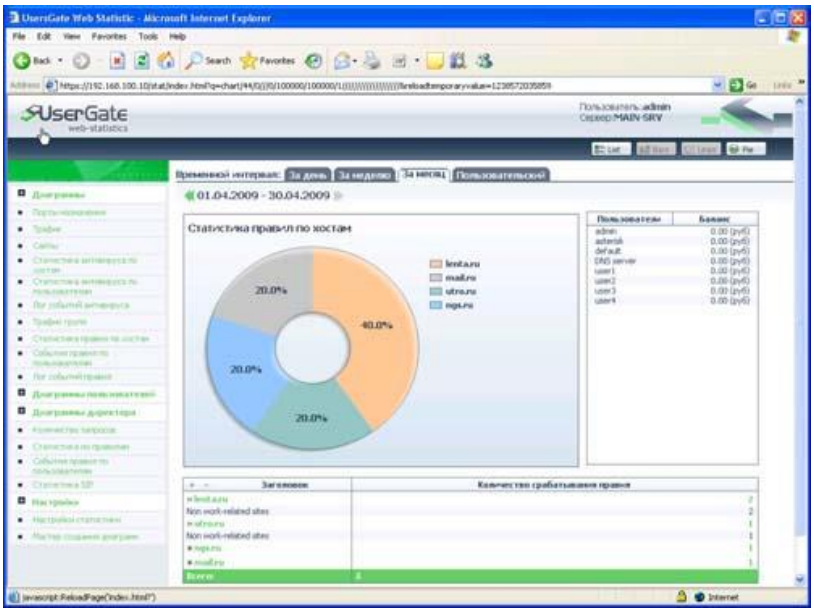


Рисунок 25. Просмотр статистики с помощью браузера

3.4. Выводы

В завершение, подведём небольшой итог. Подробное рассмотрение возможностей UserGate Proxy & Firewall показало, что на сегодняшний день данный продукт является одним из наиболее функциональных прокси-серверов, присутствующих на российском рынке. С его помощью можно решить практически любую задачу, связанную с организацией совместного доступа к сети Интернет.

Важной особенностью рассмотренного продукта является возможность реализации корпоративной политики использования глобальной сети. Запрет доступа к потенциально опасным сайтам, блокировка загрузки контента определенного типа и некоторые другие возможности увеличивают степень защищенности информационной системы.

Немаловажным фактором является наличие в UserGate Proxy & Firewall инструментов безопасности, которые позволяют быстро и просто организовать защиту периметра локальной сети от внешних угроз: антивируса и брандмауэра. Конечно же, их использование не отменяет необходимость защиты рабочих станций. Тем не менее, двухступенчатая «оборона», в ходе которой сетевой трафик проверяется последовательно (сначала на уровне интернет-шлюза, а потом на уровне компьютеров пользователей) обычно оказывается заметно эффективнее.

Основные недостатки UserGate Proxy & Firewall носят не технический, а скорее «экономический» характер. Речь идет о необходимости ежегодного продления лицензий на использование антивирусных модулей, а также системы фильтрации сайтов на основе категорий. В принципе, прокси-сервер может работать и без них, тем более, лицензия на сам UserGate Proxy & Firewall бессрочная. Однако, данные функции позволяют заметно увеличить безопасность информационной системы, и, поэтому, их использование все-таки желательно.

Более того, за лицензию на контент-фильтр Entensys URL Filtering надо будет приобретать отдельно, и причем каждый год.

3. KinderGate

Среди основных возможностей программы можно отметить следующие:

- **Запрет посещений нежелательных категорий сайтов.** С помощью технологии Entensys URL Filtering 2.0, использующей базу из 500 миллионов веб-сайтов, фильтр имеет возможность блокировать не только сайты с содержанием для взрослых, но и вредоносные сайты, игровые и другие категории нежелательных сайтов;
- **Контентная фильтрация.** В Entensys KinderGate Parental Control 3.0 встроен модуль морфологического анализа загружаемого контента, что является необходимым дополнением к блокировке доступа по URL;
- **Блокировка опасных сайтов.** Представляет собой функцию запрета доступа к сайтам, содержащим вредоносные программы, а также созданные для реализации механизмов социальной инженерии (фишинговые сайты);
- **Блокировка контекстной рекламы и баннеров**;
- **Безопасный поиск**. Представляет собой блокировку запросов сомнительного содержания;
- **Установка режима доступа в Интернет.** В Entensys KinderGate Parental Control 3.0 можно ограничивать для ребёнка время доступа в Интернет.

3.1.Системные требования KinderGate 3.2

Entensys KinderGate Parental Control можно установить на ПК, работающие под управлением следующих операционных систем:

- Windows XP,Vista, 7, 8;
- Linux;
- Mac OS X 10.7.5 и выше.

Для комфортной работы требуется не менее 512 МБ оперативной памяти и не менее 200 МБ свободного пространства на жёстком диске.

Примечание. Для данного обзора производилась установка и настройка Entensys KinderGate Parental Control 3.0 на MacOS X 10.9.

3.2. Установка KinderGate 3.2, первоначальная настройка и регистрация лицензии

После запуска дистрибутива установка идёт по единственному стандартному сценарию (рис. 26).

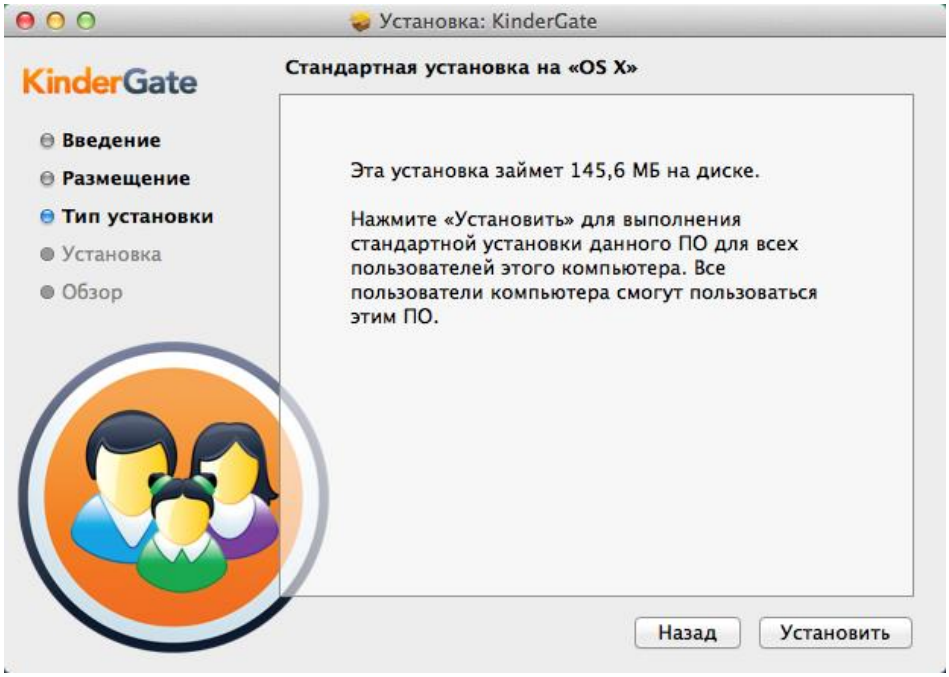


Рисунок 26. Программа установки KinderGate 3.2

Во время установки необходимо ввести имя и пароль администратора компьютера (рис. 27).

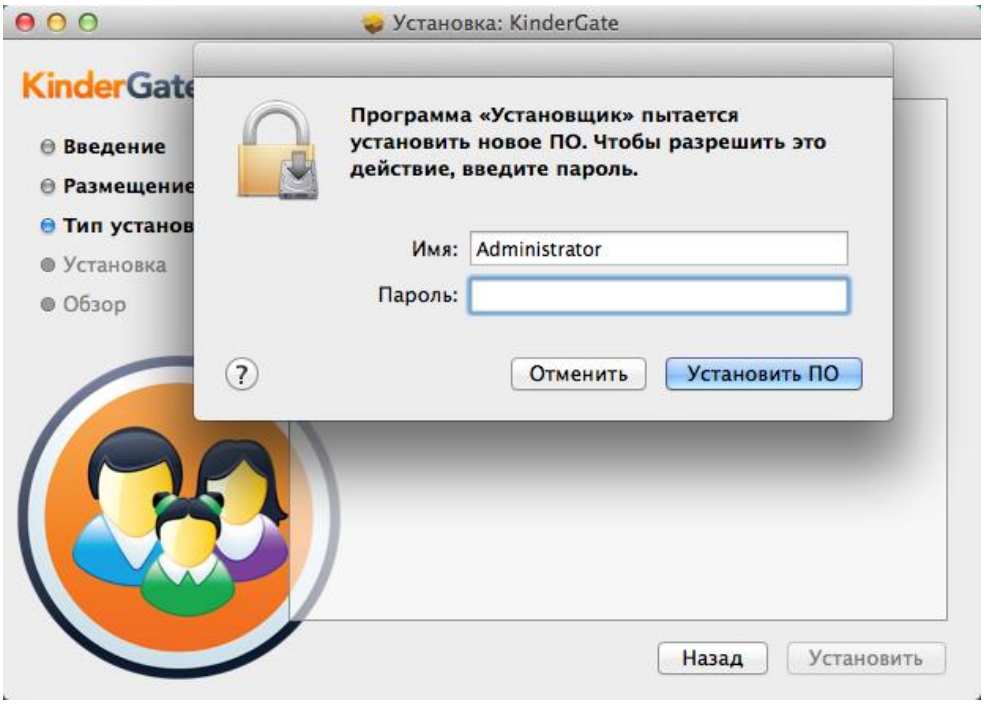


Рисунок 27. Ввод пароля администратора во время установки KinderGate 3.2

Установка также включает в себя необходимость перезагрузки компьютера.
При первом запуске KinderGate 3.2 необходимо выбрать язык интерфейса (рис. 28).

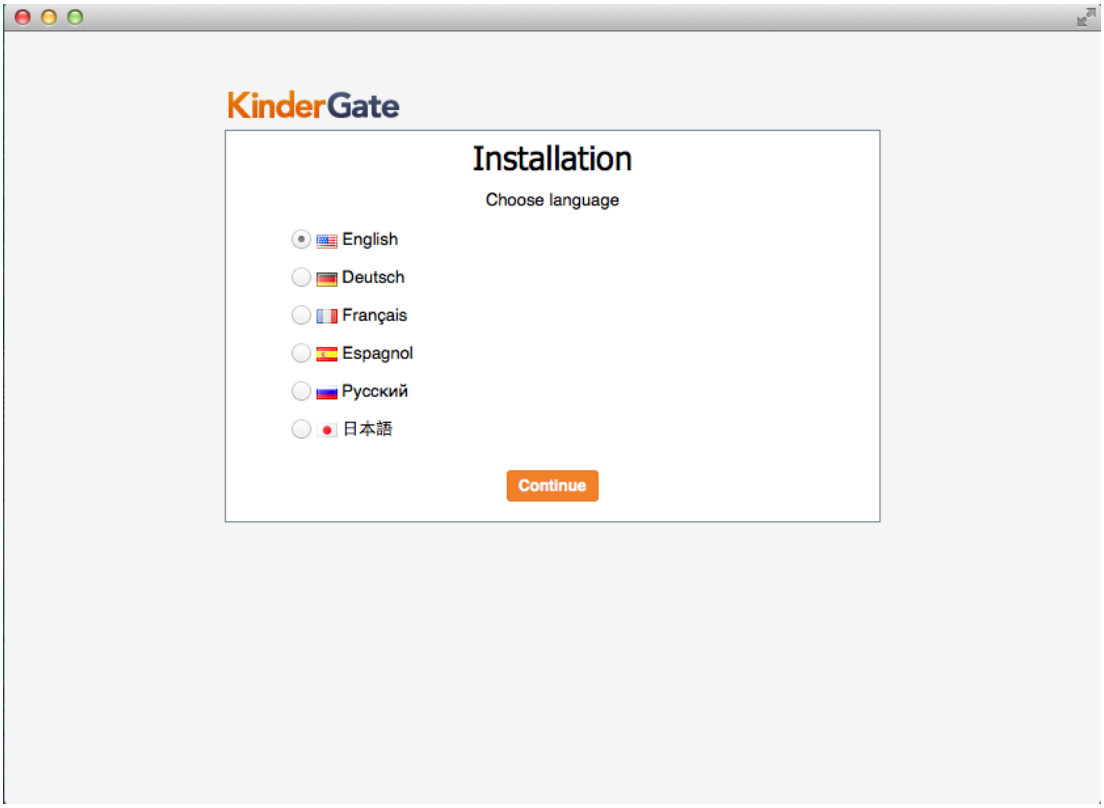


Рисунок 28. Выбор языка интерфейса KinderGate 3.2

После этого требуется принять лицензионное соглашение и ввести пароль для доступа к настройкам работы KinderGate 3.2 (рис. 29).

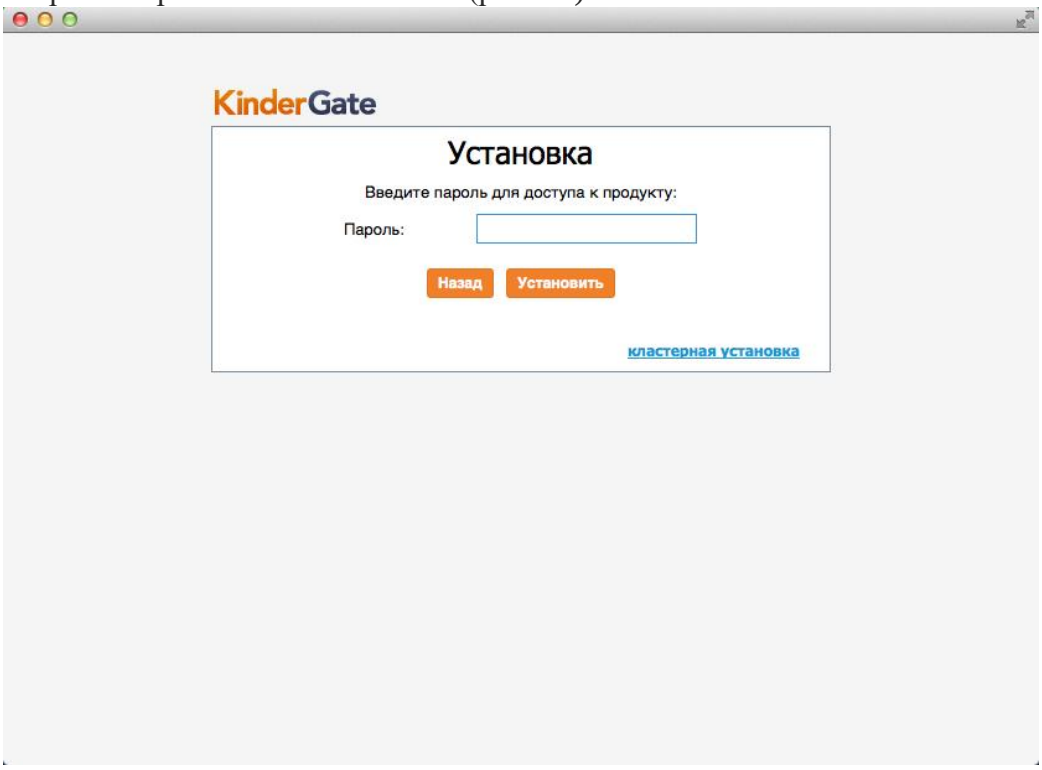


Рисунок 29. Указание пароля доступа к настройкам KinderGate 3.2

Далее необходимо зарегистрировать демонстрационную лицензию или ввести пин-код от приобретённой лицензии (рис. 30).

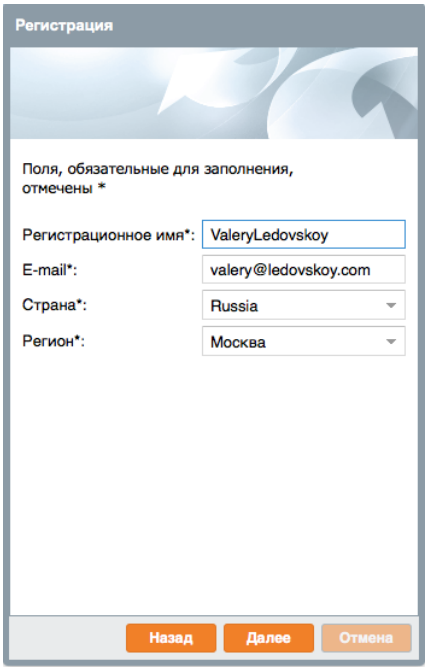


Рисунок 30. Регистрация лицензии на KinderGate 3.2

На этом установка KinderGate 3.2 для Mac OS X завершена.

3.3.Управление фильтрацией трафика

При первом запуске KinderGate 3.2 отображается упрощённый вариант консоли, в котором собрана общая информация о статусе фильтрации трафика, действующей лицензии. Здесь же можно выбрать уровень фильтрации, проверить сайт на принадлежность к какой-либо категории, а также посмотреть общую статистику (рис. 31). Из упрощённой консоли можно перейти в расширенную.

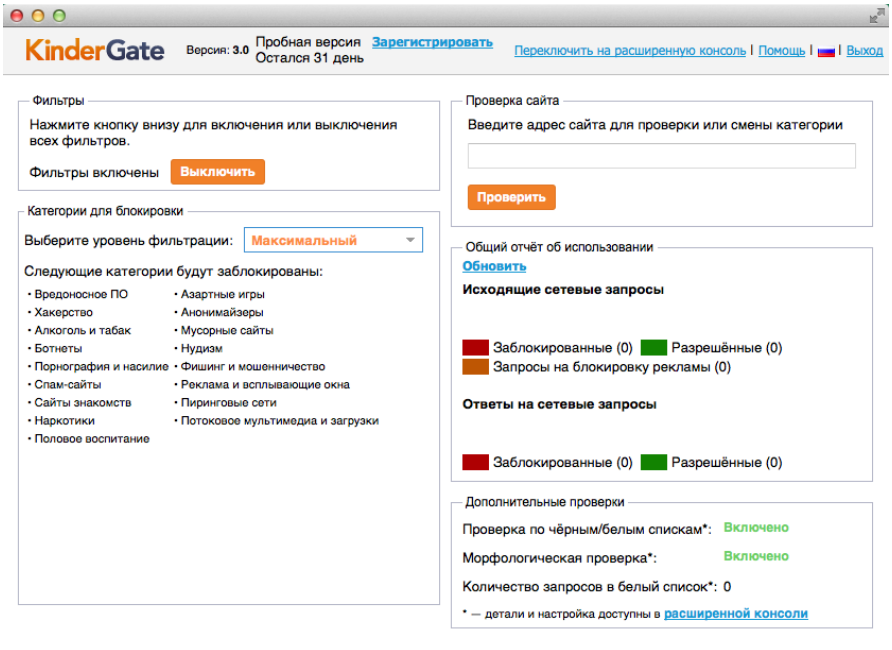


Рисунок 31. Упрощённая консоль KinderGate 3.2

Интерфейс расширенной консоли состоит из нескольких окон. В окне «Лицензия» содержится подробная информация о текущей лицензии на KinderGate 3.2 (рис. 32).

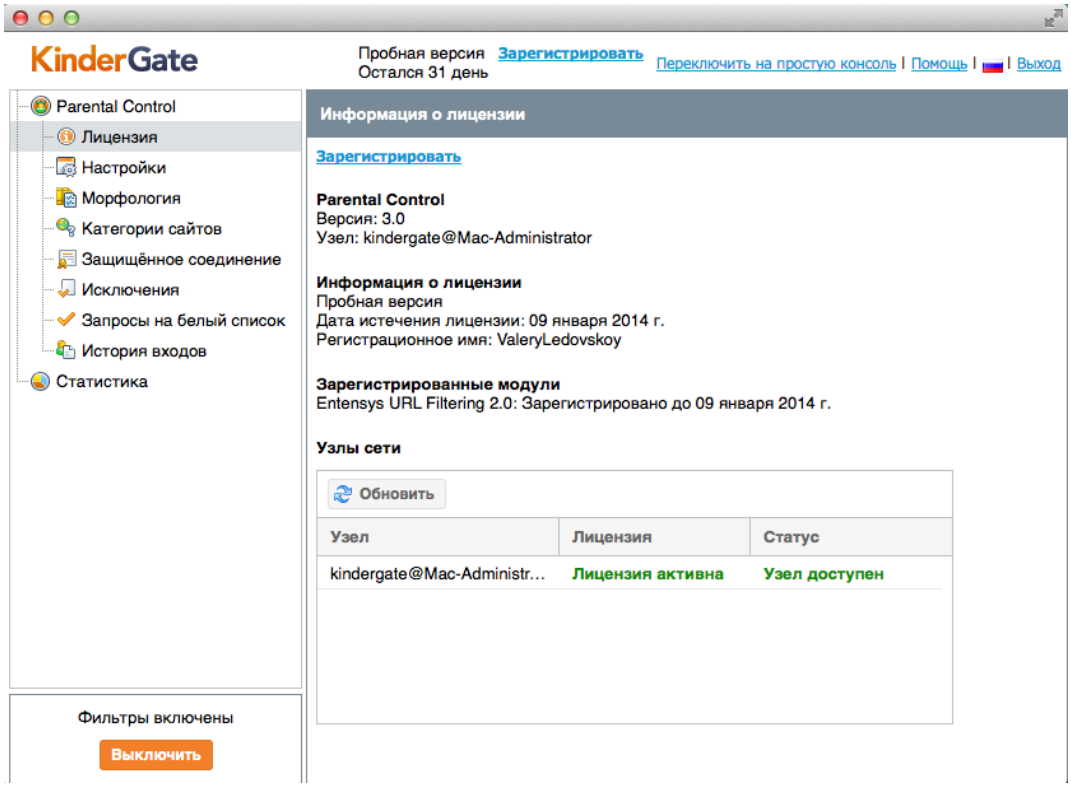


Рисунок 32. Информация о лицензии на KinderGate 3.2

В окне «Настройки» (рис. 33) можно изменить параметры отображения интерфейса KinderGate 3.2, включить или отключить функцию безопасного поиска и блокировщика рекламных баннеров. Также в этом окне содержатся настройки, связанные с блокировкой загрузки на компьютер файлов определённых типов. И, наконец, здесь же можно сменить пароль администратора для доступа к настройкам KinderGate 3.2.

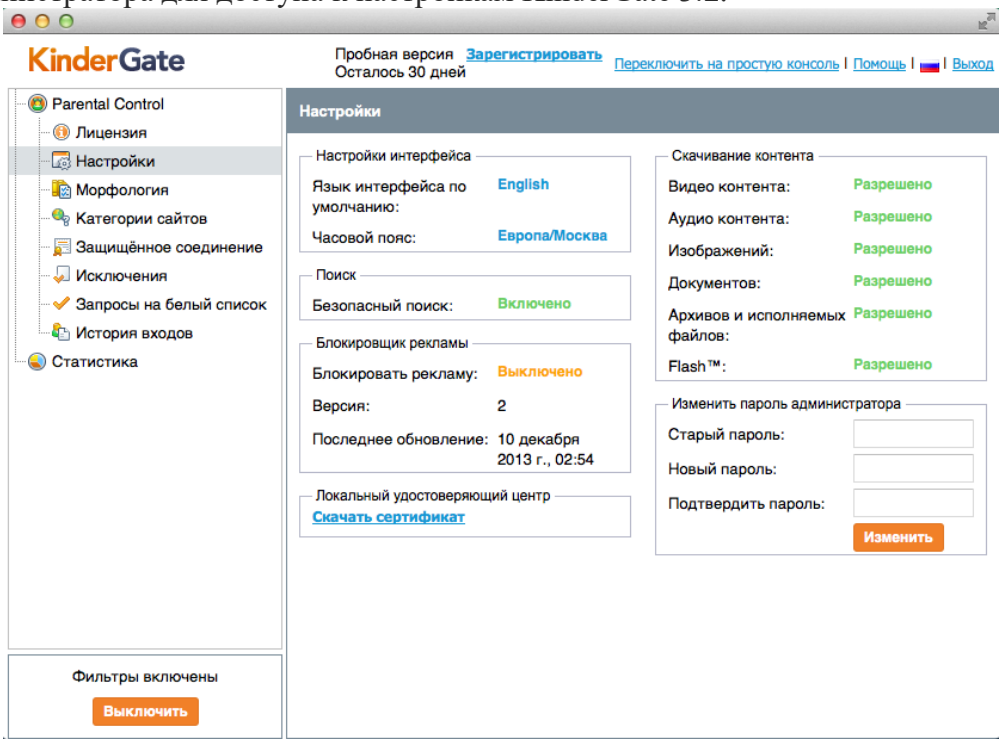


Рисунок 33. Основные настройки KinderGate 3.2

В окне «Морфология» содержатся настройки тематик, на наличие которых будет проверяться входящий интернет-трафик (рис. 34). В продукт встроено использование ряда морфологических словарей, которые поддерживаются и обновляются компанией Entensys. Словари содержат большое количество слов, терминов, жаргонных выражений, относящимся к темам, определенным законом о защите детей – наркотики, суицид, порнография, экстремизм, а также категории нецензурных слов и азартных игр.

Словарь, относящийся к терроризму, содержит все экстремистские материалы, запрещенные на территории России, из списка Министерства юстиции РФ. Это позволяет блокировать любые страницы, где размещены какие-либо произведения, книги, видеоролики, звуковые файлы из данного списка.

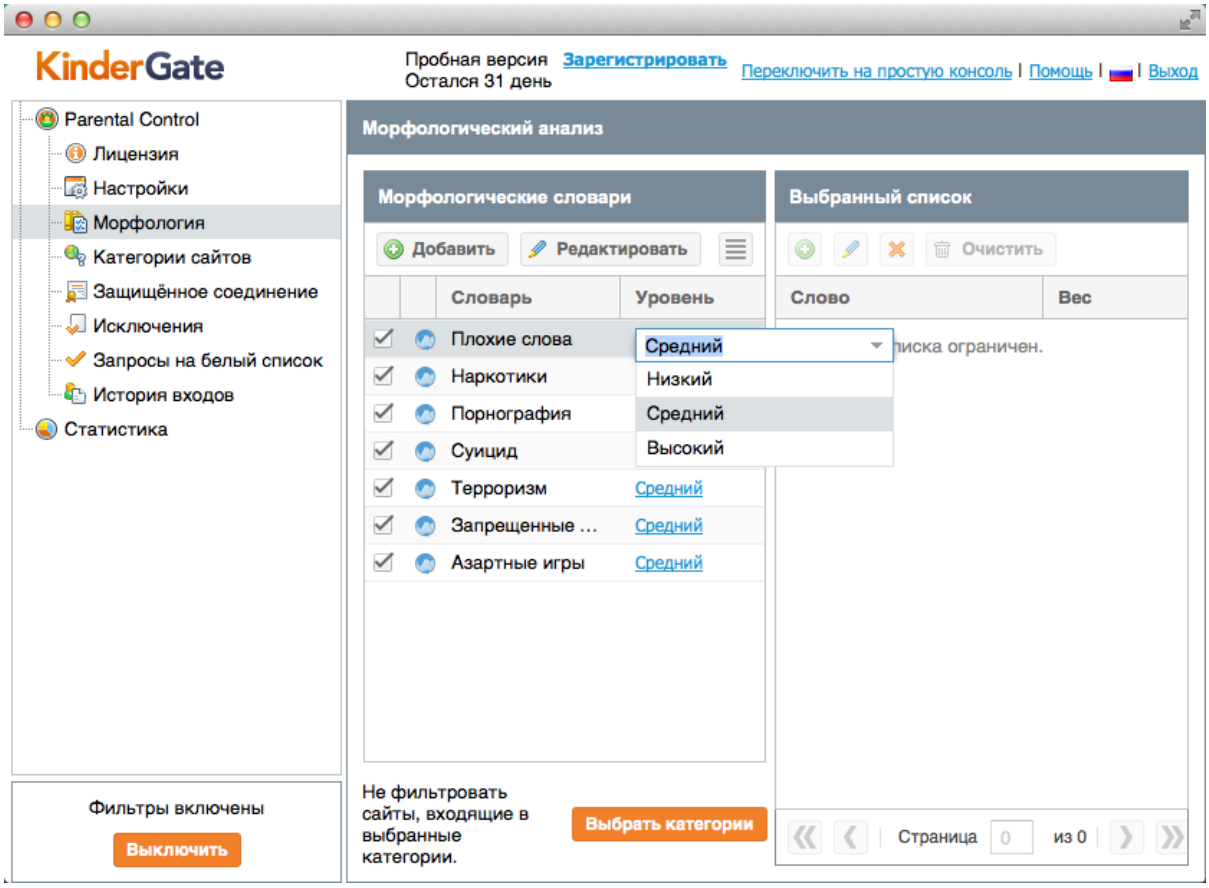


Рисунок 34. Настройки морфологического анализа KinderGate 3.2

В окне «Категории сайтов» (рис. 35) можно выбрать уровень фильтрации, от которого зависит перечень блокируемых тематик сайтов. Также можно проверить сайты на вхождение в какую-либо категорию и отправить запрос на смену категории для определённых сайтов, введя соответствующие запросы прямо в консоли администратора.

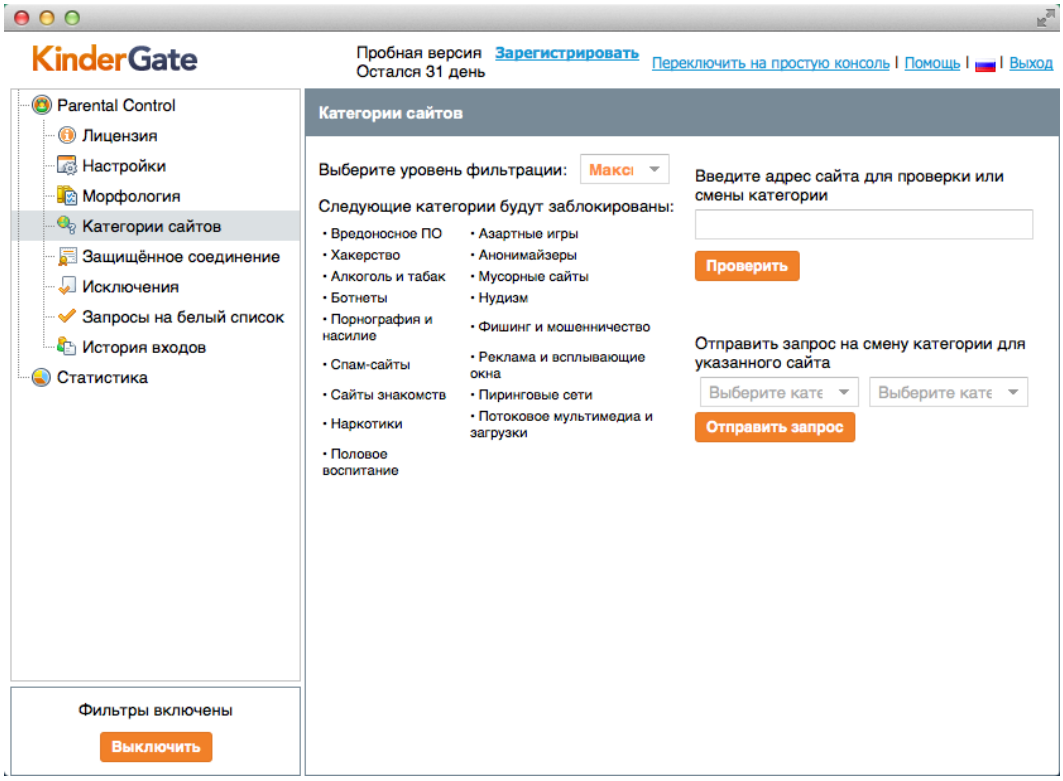


Рисунок 35. Работа с категориями сайтов в KinderGate 3.2

Окно «Защищённое соединение» (рис. 36) предназначено для настройки проверки трафика по протоколу HTTPS. При этом используется технология Man-in-the-Middle, подразумевающая следующий алгоритм работы: программа перехватывает запросы на соединение с HTTPS-сайтом, а затем создаёт собственный сертификат для сайта, к которому подключается пользователь и подписывает им зашифрованный трафик, являясь, по сути, своеобразным прокси между интернет-браузером и HTTPS-сайтом. В данном окне можно выбрать категории сайтов, для которых будет проверяться трафик, идущий по HTTPS-протоколу, а также добавить домены, для которых будет контролироваться HTTPS-трафик.

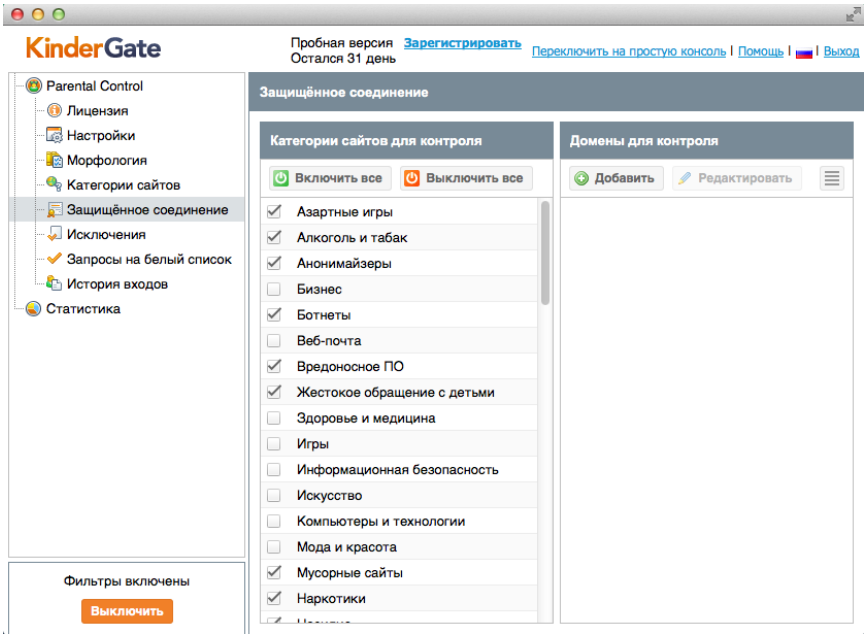


Рис. 36. Настройки контроля HTTPS-трафика в KinderGate 3.2

В окне «Исключения» можно настроить списки исключений из проверки трафика посредством KinderGate 3.2. С помощью окна «Запросы на белый список» можно обрабатывать запросы пользователей на добавление сайтов в белый список. Окно «История входов» содержит информацию о подключениях администратора к консоли управления KinderGate 3.2 для контроля попыток несанкционированного доступа к настройкам программы.

Окно «Статистика» содержит гистограммы, визуализирующие статистику пользовательских запросов к интернет-ресурсам (рис. 37).

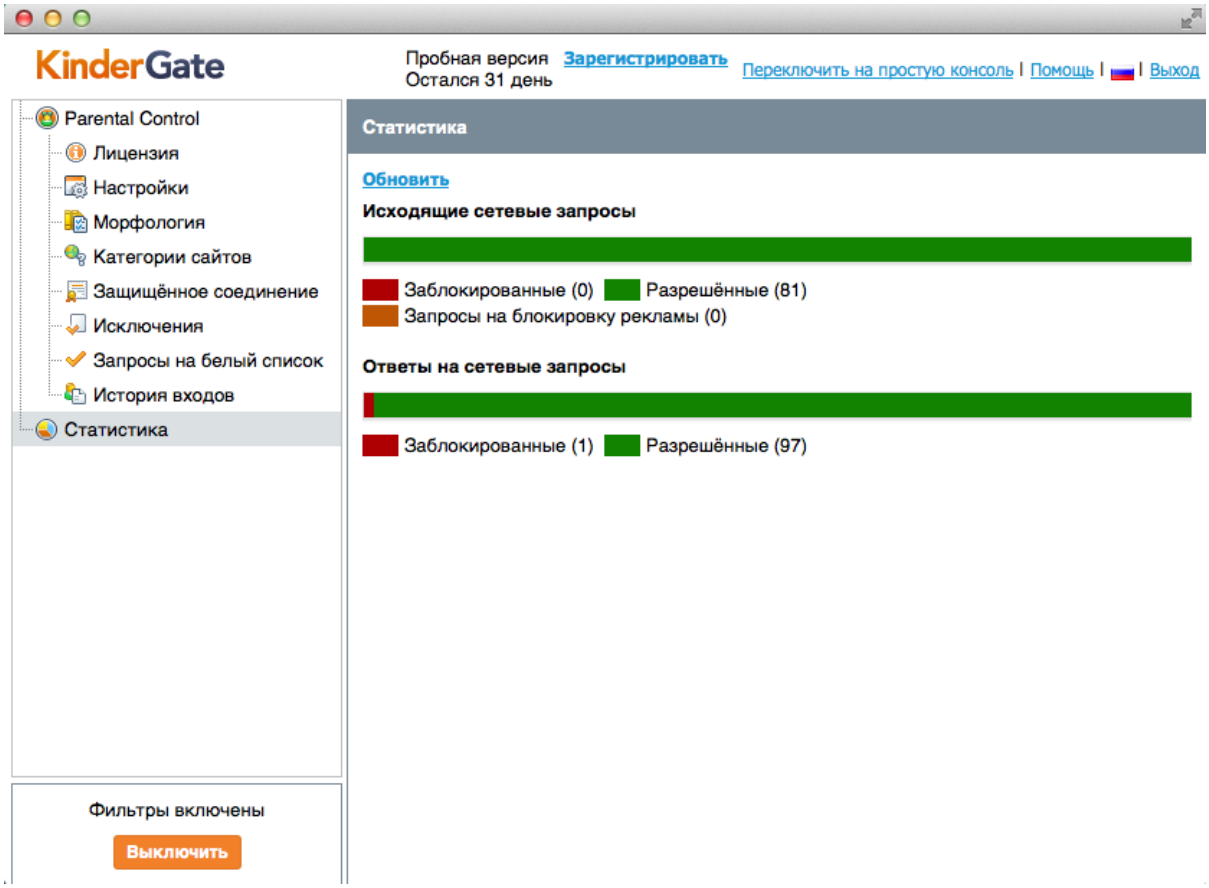


Рисунок 37. Статистика работы KinderGate 3.2

3.4.Практический пример работы KinderGate 3.2

Проверить правильную работу фильтров KinderGate 3.2, достаточно попытаться открыть страницу веб-энциклопедии Wikipedia, посвящённую суициду. В интернет-браузере появится сообщение о блокировке, при этом можно будет обратить внимание на то, что в данном случае работает блокировка не по URL, а согласно модулю морфологии (рис. 38).

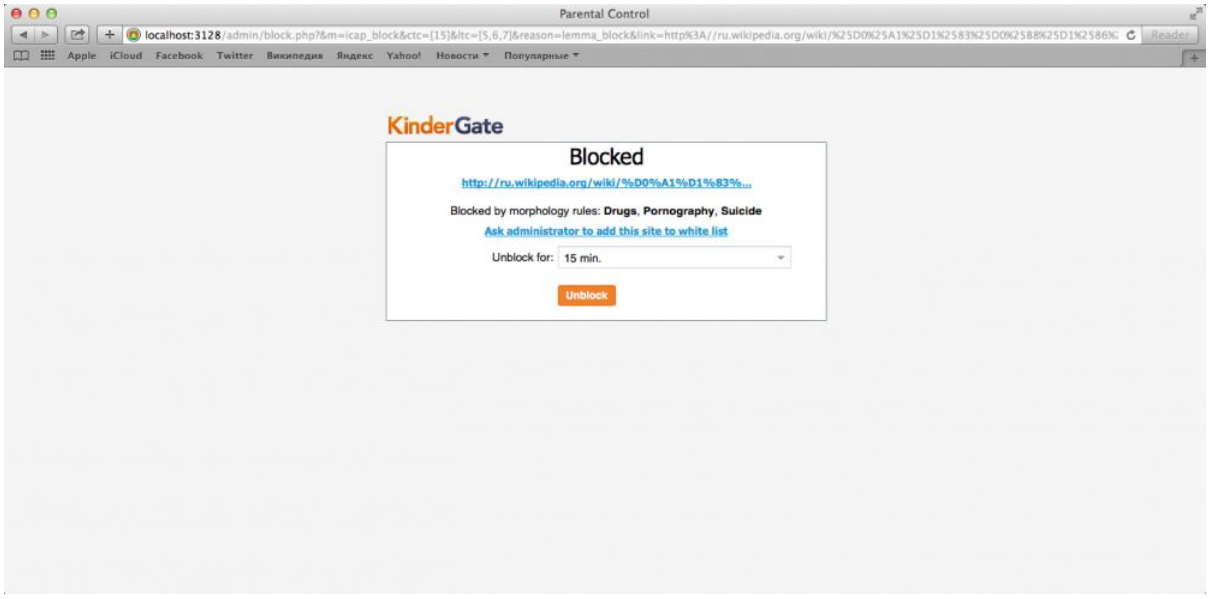


Рис. 38. Блокировка доступа к сайту в KinderGate 3.2

Также можно проверить работу фильтрации поисковых запросов, набрав, например, в Поиске Google запрос «Суицид» (рисунок 39).

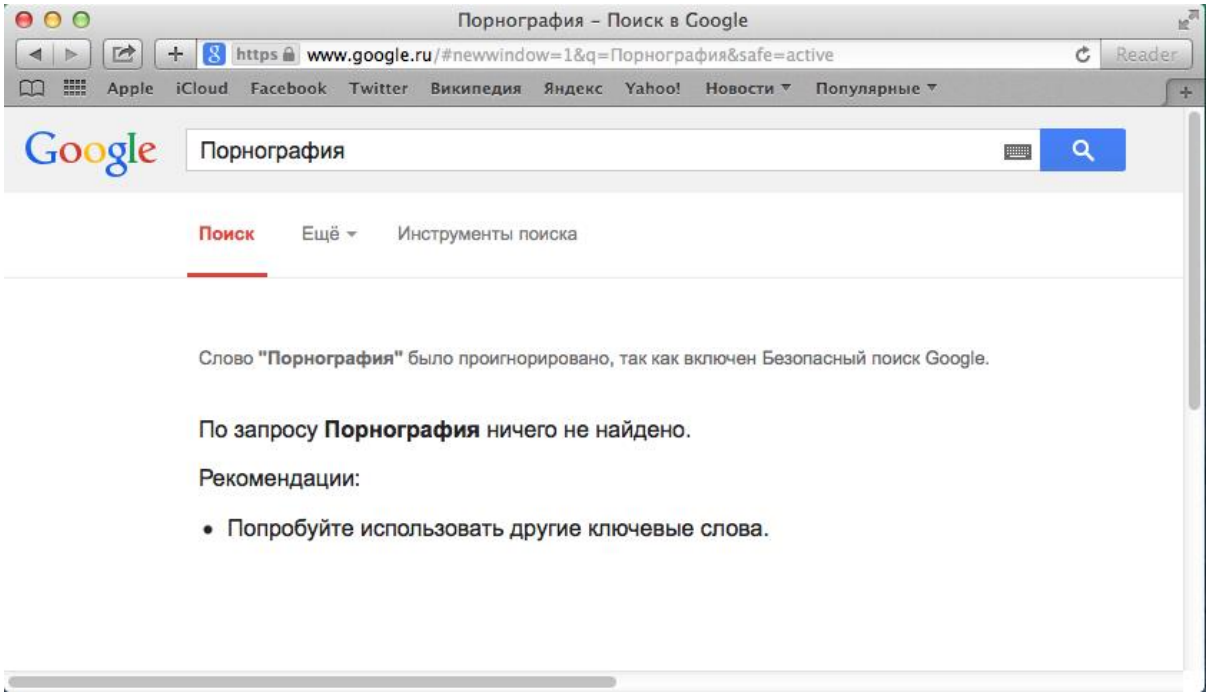


Рисунок 39. Блокировка поискового запроса в KinderGate 3.2

Кроме того, можно проверить блокировку рекламы, предварительно включив её в настройках KinderGate 3.2. Если после этого зайти на страницу веб-сайта компании Entensys, посвящённую KinderGate, то мы увидим практически пустой экран – реклама не отображается, но меню сайта доступно (рис. 40).

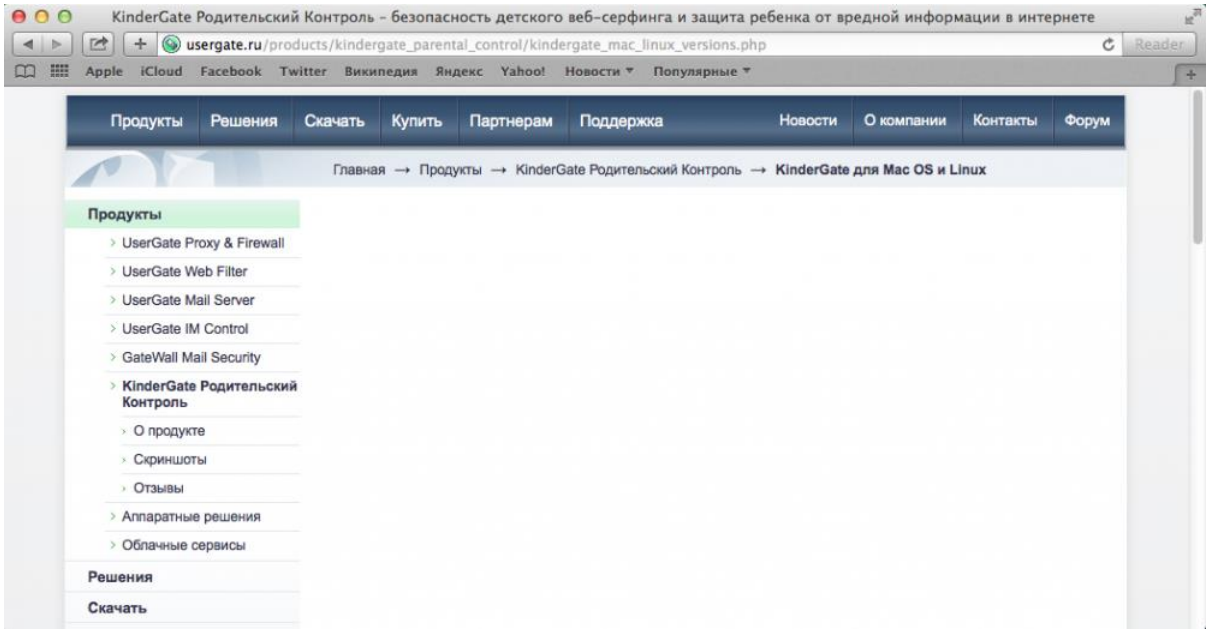


Рисунок 40. Блокировка рекламы в KinderGate 3.2

В целом при использовании продукта сложилось ощущение высокой защищенности пользователя. Все опасные ресурсы, на которые автор статьи пытался зайти, блокировались фильтрацией либо по категориям, либо по контенту. Принудительно включенный безопасный поиск также резко ограничивает возможность сознательного поиска таких ресурсов.

Также необходимо отметить высокую адаптацию продукта к специфике русского языка не просто в плане интерфейса, а в плане знания русскоязычных сайтов, качественного контент-анализа на русском языке и поддержки специальных морфологических словарей.

3.5.Выводы

KinderGate может быть эффективным интернет-фильтром как для домашних пользователей, так и для образовательных учреждений. Основным достоинством продукта является сочетание нескольких методов фильтрации, понимание русского языка, наличие специальных словарей, обеспечивающих соответствие российскому законодательству. Эффективность фильтра также подтверждена тестированием, проведённым исследовательской лабораторией портала Anti-Malware.ru.

Преимущества:

- доступность установки и настройки для домашних пользователей;
- комплексная фильтрация, сочетающая использование категоризированных баз и контент-анализа;
- поддержка морфологии русского языка, качественное покрытие Рунета;
- наличие словарей, позволяющих отфильтровывать сайты, страницы, сообщения, содержащие опасную информацию или просто нецензурный текст;
- соответствие требованиям российского законодательства;
- поддержка фильтрации HTTPS;
- поддержка платформ Windows, Linux и Mac OS X.

Недостатки:

- отсутствие возможности настройки нескольких профилей фильтрации трафика для возможности быстрого переключения между ними;
- требуется вручную установить сертификат локального удостоверяющего центра (если этого не сделано, то при включённой функции безопасного поиска при открытии Поиска Google выводится сообщение о том, что Safari не может проверить подлинность сертификата сайта www.google.ru);

- до полного удаления продукта (через встроенную в дистрибутив программу удаления KinderGate) наблюдались проблемы с доступом к сервису App Store и получением обновлений системы. При попытке получить обновление выводилось системное сообщение о невозможности доступа к сервису обновлений Mac OS X.

Стоимость составляет 490 рублей на компьютер в год. В итоге на 100 компьютеров конечная стоимость составит 49 000 рублей в год. При тестировании данного продукта стал ощутимо медленнее работать Интернет.

4. Интернет Контроль Сервер

ИКС 2.3.4 (Интернет Контроль Сервер) от российской компании «А-Реал Консалтинг» – это многофункциональный межсетевой экран и прокси-сервер. Представляет собой программный комплекс, в основе которого лежит операционная система FreeBSD 8.1. Использование операционной системы FreeBSD означает минимальное потребление системных ресурсов, высокую надёжность, безопасность и скорость работы. Продукт имеет сертификат ФСТЭК №2623 от 19 апреля 2012 г.

К ключевым особенностям интернет-шлюза – межсетевого экрана ИКС стоит отнести:

- Большое количество сетевых сервисов, в том числе FTP, Web, DNS, DHCP, VPN, прокси, почтовый и jabber сервера, LDAP, и другие. Это позволяет строить конфигурации системы практически произвольного уровня сложности, в зависимости от сценария использования.
- Для доступа к сети Интернет могут быть использованы различные варианты подключения к провайдерам. Поддерживаются:
  - DHCP;
  - PPPOE;
  - PPTP over IP;
  - PPTP over DHCP;
  - Провайдер VLAN.
- Система обнаружения вторжений (IPS) Snort.
- Возможность проверки трафика антивирусами ClamAV (бесплатный продукт) и Dr.Web (для работы требуется приобретение отдельной лицензии).
- Проксирование, в том числе и прозрачное.
- Модуль контентной фильтрации.
- Гибкая система работы с правилами для пользователей, групп пользователей.
- Удобная настройка ширины полосы пропускания.
- Интеграция с сетями Microsoft Windows.
- Поддержка установки и работы на виртуальных машинах Virtualbox, VmWare Workstation и VmWare ESXi;
- Межсетевой экран ИКС сертифицирован ФСТЭК.

Подробнее остановимся на сертификации ФСТЭК. Согласно Федеральному закону РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных», существенно возросли требования ко всем частным и государственным компаниям и организациям, а также физическим лицам, которые хранят, собирают, передают или обрабатывают персональные данные (в том числе фамилия, имя, отчество). Это означает, что для обеспечения безопасности персональных данных, при работе с ними, должны использоваться средства, которые прошли сертификацию ФСТЭК. К тому же, в случае наличия доступа к сети Интернет локальной вычислительной сети (или её сегмента), в которой идёт работа с персональными данными, то для защиты персональных данных, такая локальная вычислительная сеть (или сегмент) должна быть защищена сертифицированным ФСТЭК межсетевым экраном.

Полученный сертификат Государственной технической комиссии при Президенте РФ (ФСТЭК) удостоверяет, что программный межсетевой экран Интернет Контроль Сервер соответствует требованиям руководящего документа Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по 4-му классу защищённости.

Изменения в межсетевом экране ИКС версии 2.3.4

Версия 2.3.4.10458. Четвертое обновление ИКС 2.3 "Drumba the Dramatic Droid"

- Добавлена команда для получения списка провайдеров и сетей с использованием Jabber/ICQ-бота.
- Добавлены графики загруженности VLAN интерфейсов.
- Добавлена возможность работы веб-почты по https.
- Теперь пользователи могут менять свой пароль в веб-интерфейсе.
- Для сетевого интерфейса теперь можно задать скорость и режим работы.
- Добавлена возможность перенаправлять GRE трафик.
- Добавлена возможность удаления отчётов старше 2 месяцев.
- Различные компоненты системы обновлены до последних версий.

Стоит отметить, что на данный момент сертификацию ФСТЭК проходит новая версия межсетевого экрана – ИКС 4.4, которая содержит ряд важных улучшений и нововведений. Укажем наиболее важные изменения версии 4.4:

- Ядро системы обновлено до FreeBSD 8.3;
- Поддержка работы с WiFi и 3G.
- IP-телефония поддержкой протоколов SIP и IAX.
- Layer-7 фильтрация.
- Добавлена функция NAT для перенаправления портов и VPN-сети.
- Добавлена возможность работы с почтовым сервером по протоколам SMTPs, IMAPs и POP3s.
- Категории трафика SkyDNS.
- Поддержка протокола L2TP для VPN-подключений.
- Поддержка VMware Tools.
- Другие функциональные возможности.

5.1. Системные требования

Количество пользователей	Архитектура	Процессор	Жесткий диск	Оперативная память
10—50 пользователей	i386	Intel Atom D410 1,6GHz	80 Gb SATA	1024 Mb
50—150 пользователей	i386	Intel Core2DUO T7100 1,8 GHz	160 Gb SATA	2 Gb
>150 пользователей	i386	Intel CoreI7 3.06Ghz	500 Gb SATA	4 Gb

5.2. Установка межсетевого экрана ИКС версии 2.3.4

Установку межсетевого экрана ИКС можно проводить с компакт-диска или USB-накопителя, предварительно записав туда скачанный с сайта производителя iso-образ, который содержит программу установки межсетевого экрана ИКС. На данный момент отсутствуют iso-образы для виртуальных машин, которые содержат уже установленный межсетевой экран ИКС.

Сама установка предельно проста и проходит в несколько этапов. Программа-установщик имеет внешний вид сходный с sysinstall FreeBSD.

На первом этапе установки будет предложено выбрать язык интерфейса.

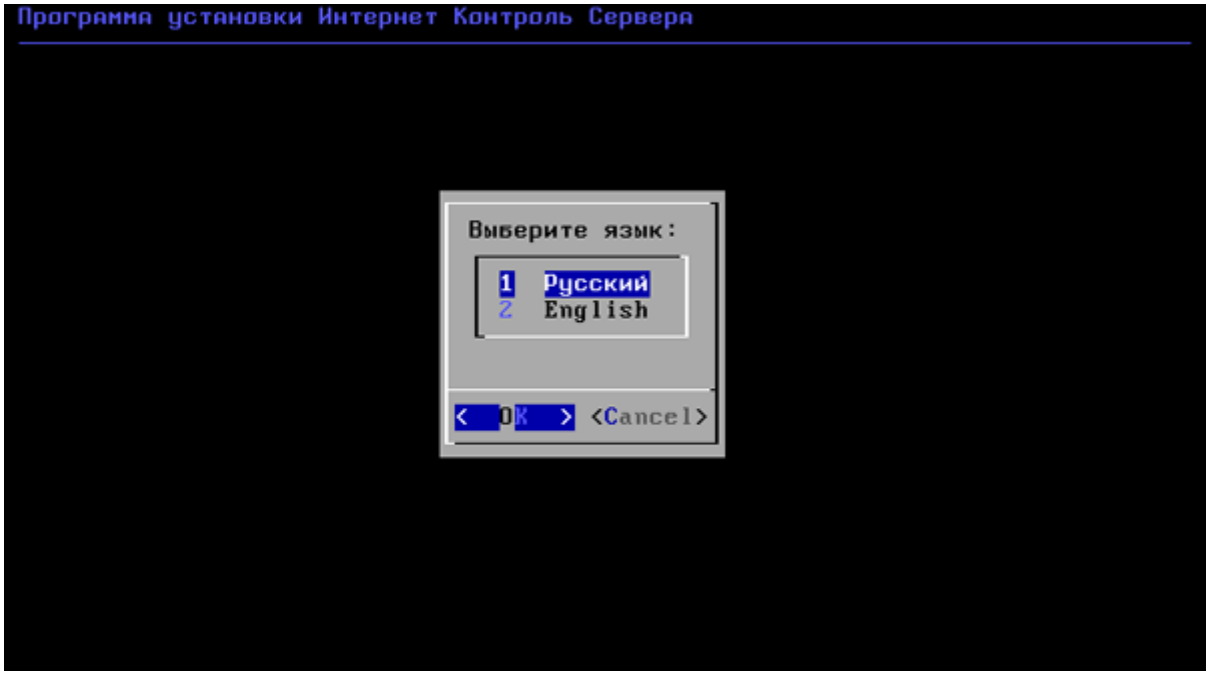


Рисунок 41. Выбор языка установки межсетевого экрана ИКС

После чего запустится сама программа установки. Далее необходимо будет принять лицензионное соглашение, выбрать сетевой интерфейс, который подключен к локальной сети, провести его настройку и выбрать жёсткий диск для установки.

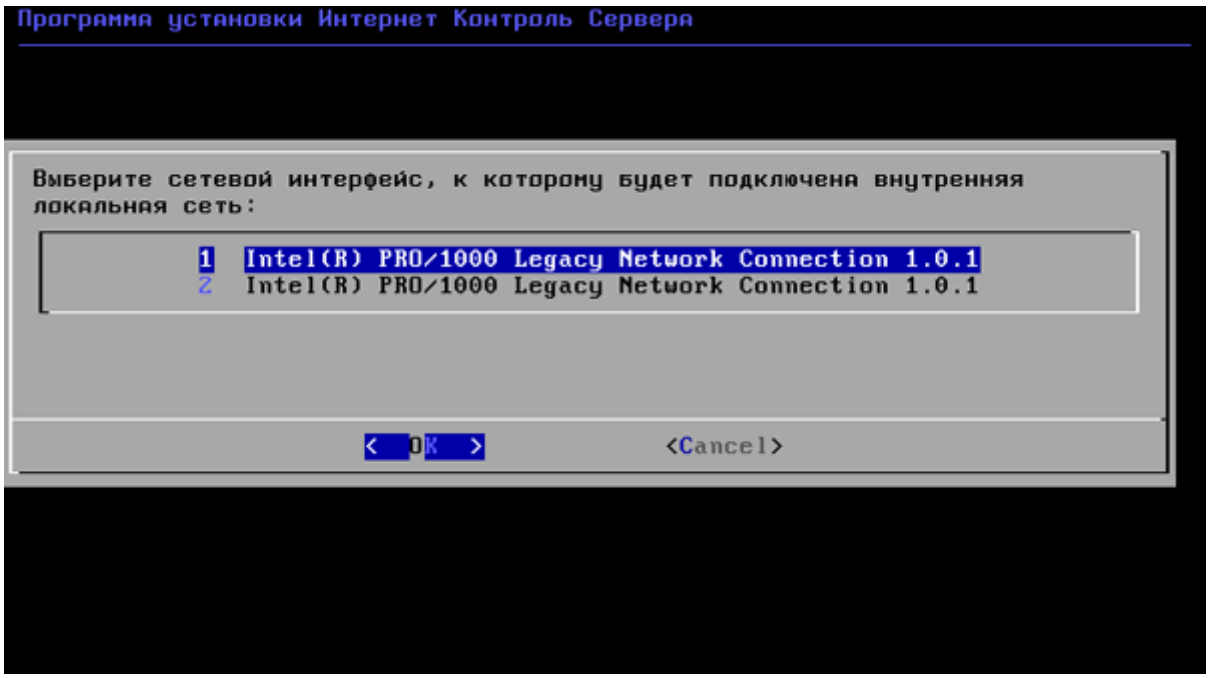


Рисунок 42. Выбор сетевого интерфейса для настройки

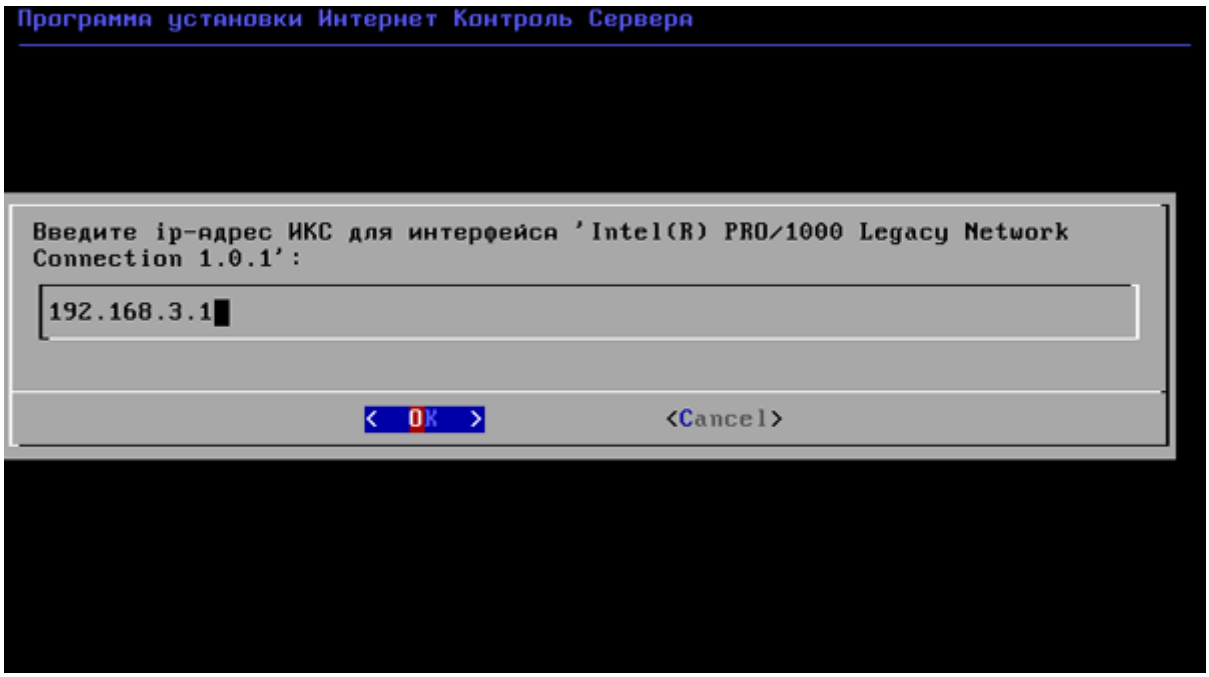


Рисунок 43. Указание IP-адреса для выбранного интерфейса

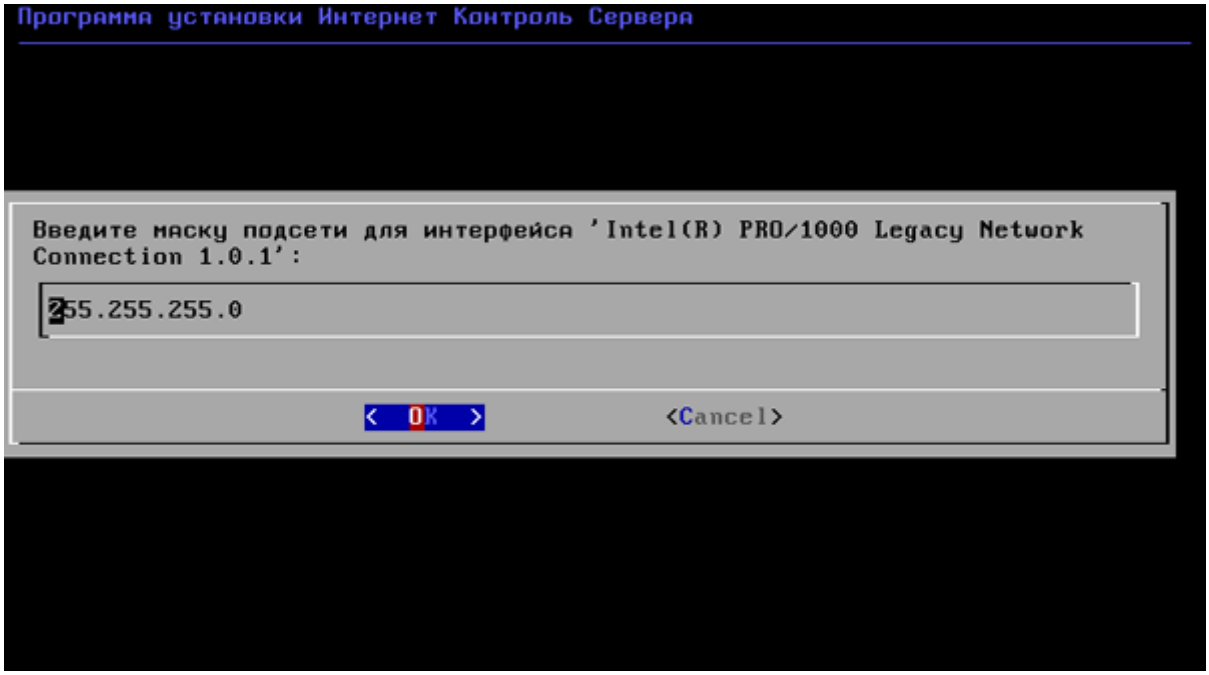


Рисунок 44. Задание маски сети

После подтверждения всех заданных настроек и выбора жёсткого диска для установки, программа установки сама разобьёт и отформатирует жёсткий диск, а затем установка продолжится. По окончании установки, будет показано сообщение-напоминание какие данные необходимо использовать для подключения к веб-консоли межсетевого экрана ИКС.

5.3. Функциональность и работа с межсетевым экраном ИКС.

Основным средством управления межсетевым экраном ИКС является веб-интерфейс (рис. 45).

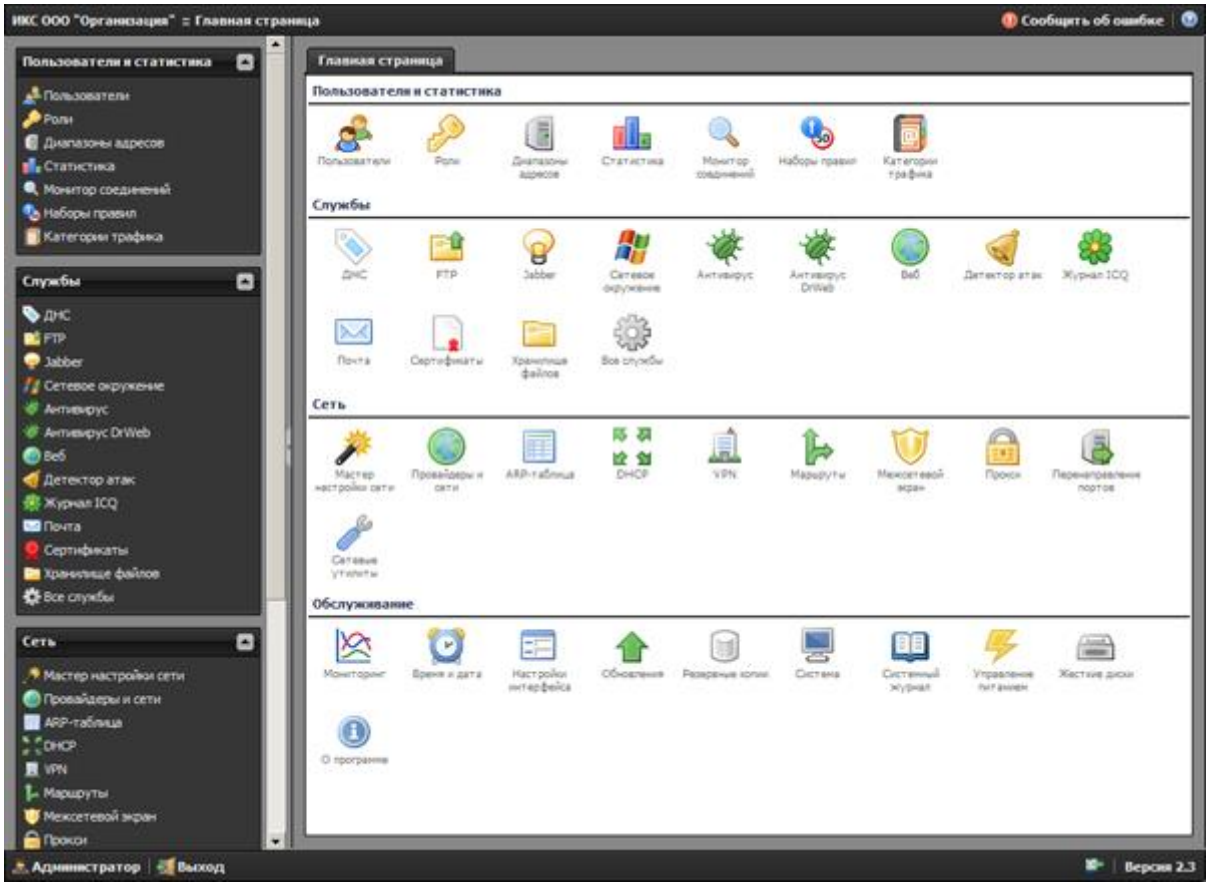


Рисунок 45. Главная страница веб-интерфейса межсетевого экрана ИКС

Сам веб-интерфейс оставляет приятное впечатление. Для облегчения навигации и доступа к нужным сервисам и пунктам меню, используется четыре логических раздела: «Пользователи и статистика», «Службы», «Сеть» и «Обслуживание».

Раздел «Пользователи». В этом разделе сгруппированы модули управления пользователями, группами пользователей, их ролями. А также модуль для работы с наборами правил (в том числе контентной фильтрации), модуль для управления категориями данных и модуль отображения детальной статистики работы пользователей в сети Интернет.

В разделе «Службы» отображается список запущенных служб межсетевого экрана ИКС. Щёлкнув на любой службе, можно увидеть окно состояния службы, а также получить доступ к дополнительным настройкам этой службы или остановить её работу. Модуль «Все службы» содержит в себе список всех сетевых сервисов, доступных в межсетевом экране ИКС.

Раздел «Сеть» содержит в себе средства управления сетевыми подключениями, управления маршрутизацией, межсетевым экраном, системой обнаружения вторжений, прокси-сервером, а также DHCP и VPN серверами, которые входят в состав межсетевого экрана ИКС.

А в разделе «Обслуживание» сгруппированы системные модули управления межсетевым экраном ИКС, в том числе и оборудованием, на котором он работает.

Для примера покажем окно состояния одной из служб межсетевого экрана ИКС (рис. 46).

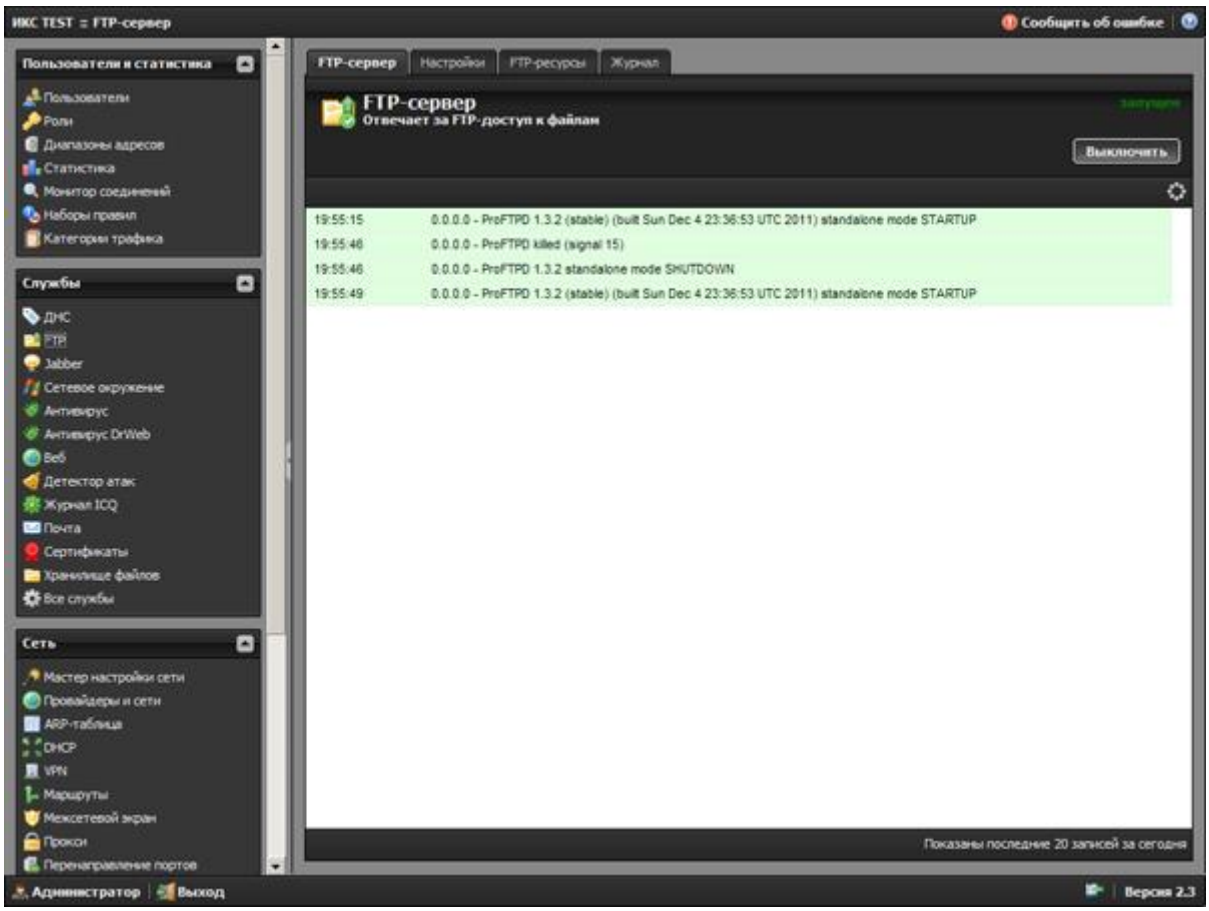


Рисунок 46. Окно состояния службы FTP межсетевого экрана ИКС

В первую очередь необходимо провести настройку сетевых интерфейсов, чтобы обеспечить межсетевому экрану ИКС доступ к сети Интернет, а затем провести обновление межсетевого экрана ИКС.

Легче всего провести настройку сети с помощью мастера настройки сети. Если необходимо провести более тонкую настройку с указанием дополнительных параметров, то это можно сделать вручную.

Мастер первоначальной настройки сети можно запустить из модуля Сеть, щёлкнув по соответствующему меню.

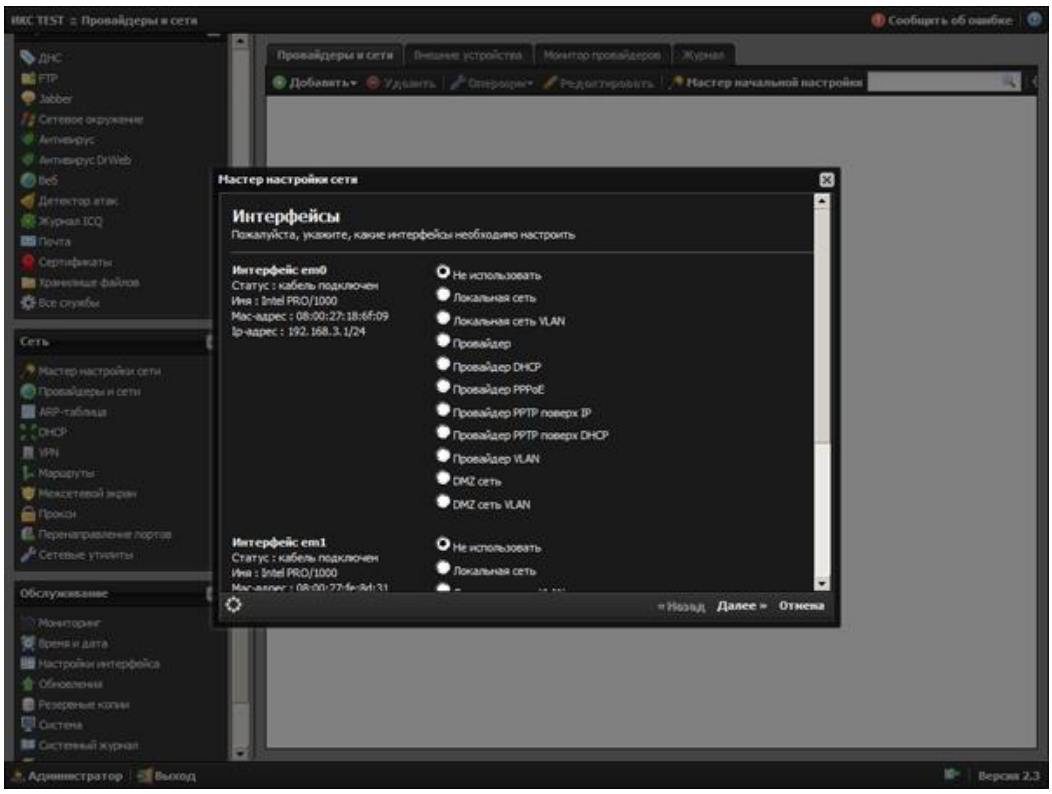


Рисунок 47. Запуск мастера первоначальной настройки сети межсетевого экрана ИКС

Как видим, нам предлагают широкий выбор вариантов подключений. Это позволяет использовать ФСТЭК версию ИКС практически с любыми типами провайдеров.

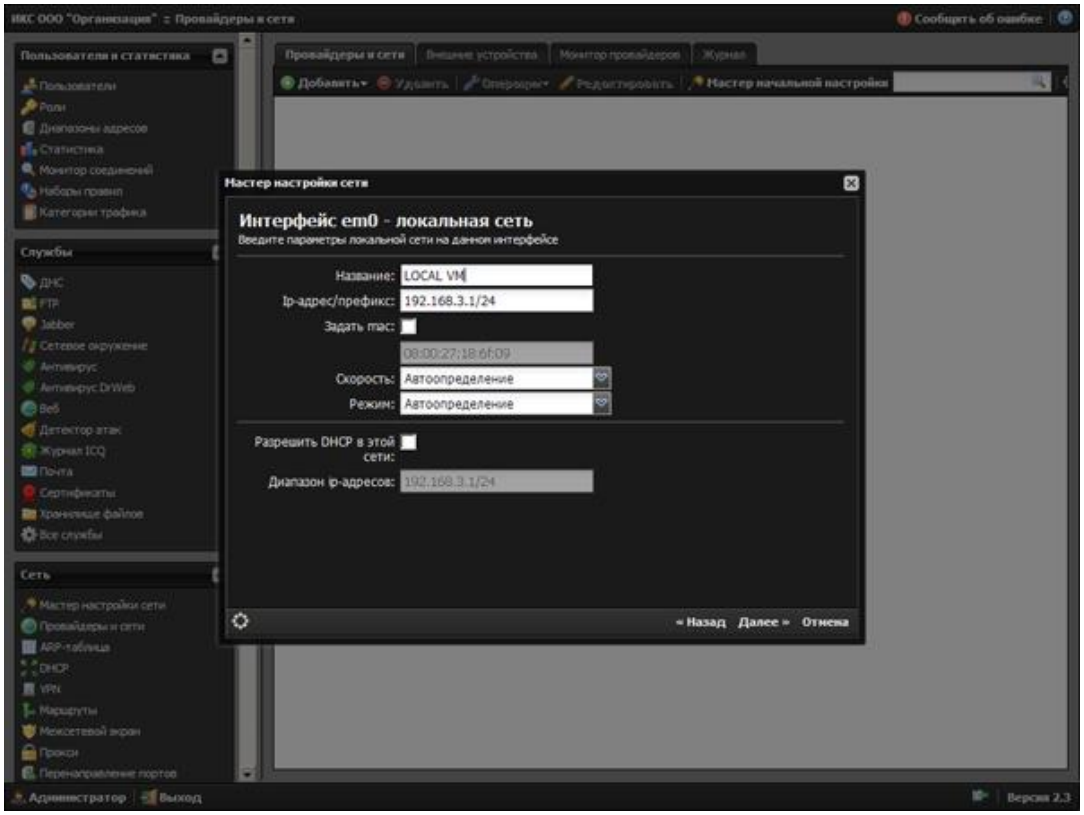


Рисунок 48. Настройка сетевых интерфейсов межсетевого экрана ИКС

Перед подтверждением настроек сетевых интерфейсов будет показана итоговая таблица изменений. Если какие-то параметры заданы неверно, можно вернуться на несколько шагов назад и подкорректировать настройки.

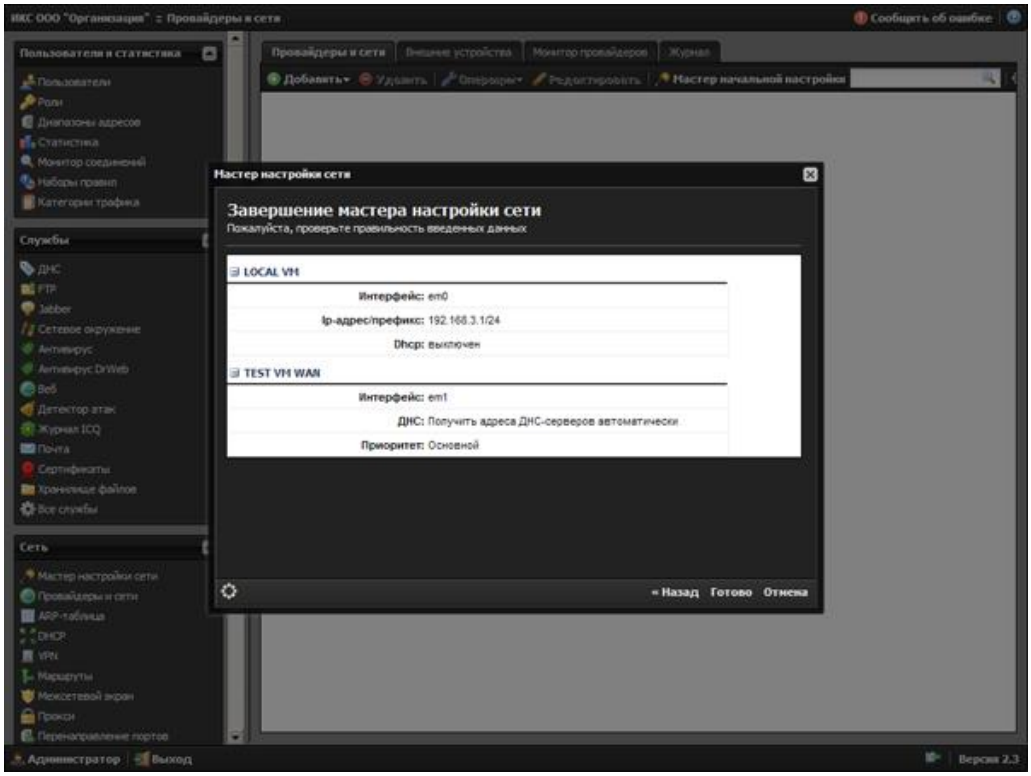


Рисунок 49. Итоговая таблица изменений настроек сетей и провайдеров межсетевого экрана ИКС

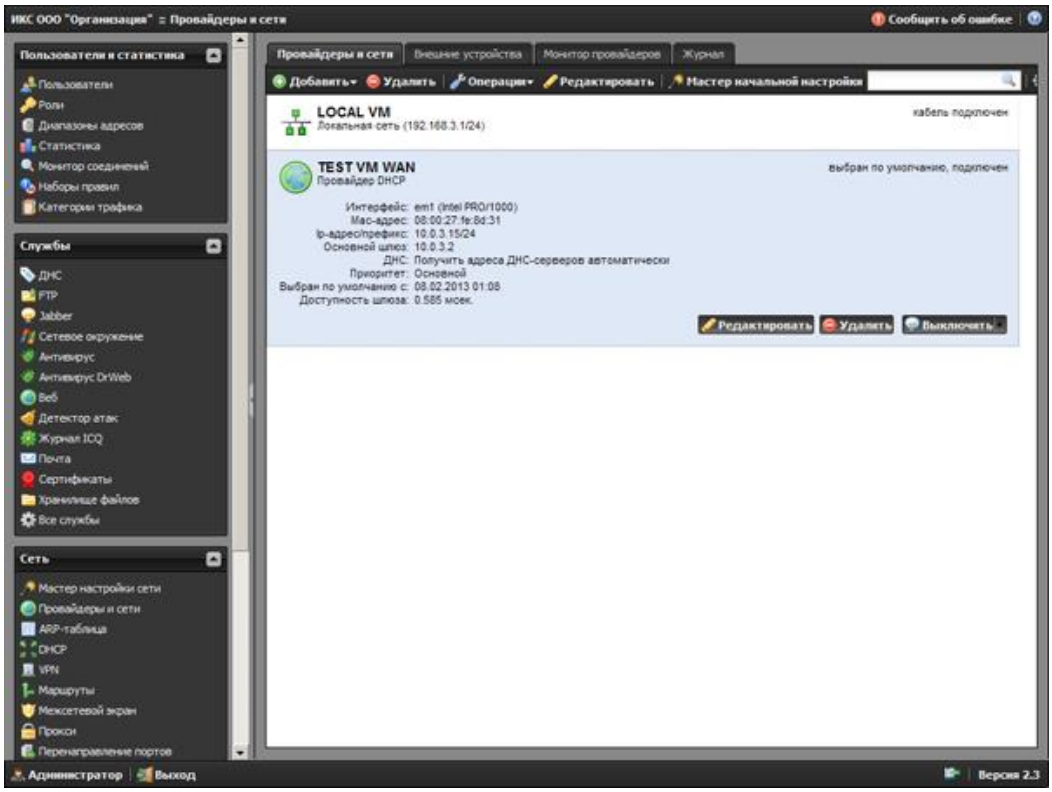


Рисунок 50. Список настроенных сетей и провайдеров межсетевого экрана ИКС

После того, как все настройки были подтверждены и применены, произойдёт автоматическая переадресация в меню «Провайдеры и сети» модуля «Сеть».

В этом меню можно посмотреть список и состояние сетевых интерфейсов, отключить или включить те или иные интерфейсы, провести их настройку. Также можно посмотреть журнал работы комплекса.

В правильности соединения с сетью Интернет можно убедиться, воспользовавшись стандартной утилитой Ping. Она доступна в меню «Сетевые утилиты» модуля «Сеть».

Если необходимо, можно сделать и трассировку, использовав утилиту traceroute, которая находится в том же меню.

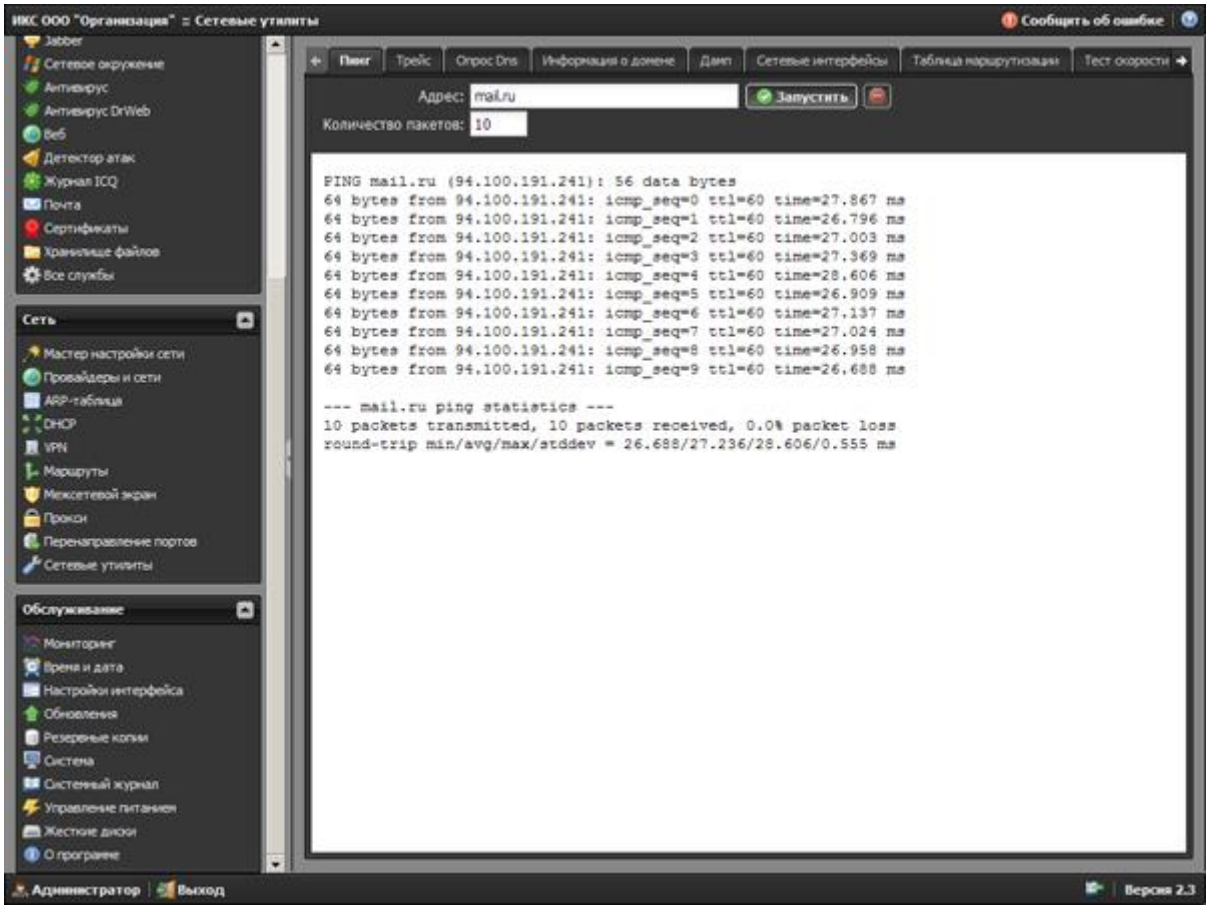


Рисунок 51. Результаты работы утилиты ping межсетевого экрана ИКС

В целом, настройка сетевых интерфейсов трудностей не вызывает.

После того, как мы смогли подключиться к сети Интернет, нужно проверить наличие обновление. Сделать это можно щёлкнув на пункт меню «Обновления» модуля «Обслуживание».

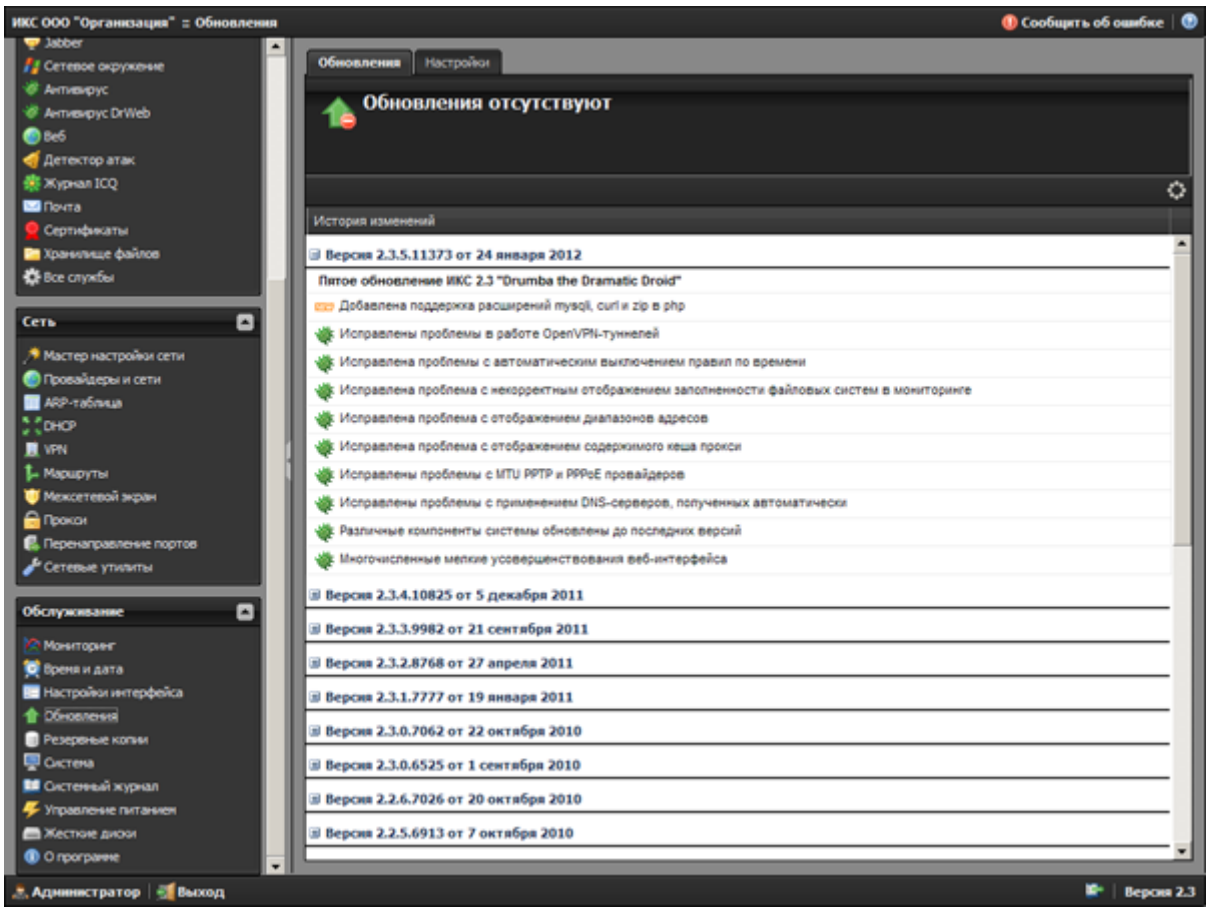


Рисунок 52. Результат проверки обновлений межсетевого экрана ИКС

Как видим, какие-либо обновления отсутствуют.

На этом краткую первоначальную настройку ИКС можно считать оконченной.

Дальнейшая настройка межсетевого экрана ИКС зависит от конкретного сценария использования.

Межсетевой экрана ИКС обладает широкой функциональностью и содержит множество сетевых сервисов.

Так, межсетевой экран ИКС может выступать в роли полноценного:

- DHCP-сервера, для автоматической настройки сетевых параметров клиентских устройств локальной сети;
- FTP-сервера (Proftpd), для обеспечения доступа к файлам по протоколу FTP;
- WEB-сервера (Apache), с поддержкой виртуальных хостов, для размещения сайтов и обеспечения к ним доступа;
- Mail-сервера (Postfix), с возможностями сбора почты с других почтовых ящиков и встроенным спам-фильтром, для передачи и приёма электронной почты;
- DNS-сервера (Bind), для работы со службами разрешения имён;
- Сервера каталогов, для синхронизации с сетями Microsoft Windows и Microsoft Active Directory;
- HTTP прокси-сервера (squid), с поддержкой прозрачного проксирования, проверки трафика с помощью антивирусов ClamAV и DrWeb, учёт и фильтрация трафика по URL и mime-типам, кэширования страниц (для экономии трафика), а также авторизации для доступа к прокси-серверу по учётным данным пользователей межсетевого экрана ИКС или Active Directory;
- Socks5 прокси-сервера, для предоставления возможности прозрачного использования сервисов за межсетевым экраном;

- VPN-сервера, для предоставления клиентам удалённого доступа с помощью VPN-авторизации;
- Сервера времени, для возможности синхронизации времени клиентских устройств с сервером, что особенно актуально в сетях с Active Directory.

Как видим, межсетевой экран ИКС предоставляет широкие возможности для использования различных сетевых сервисов и построения конфигураций различно сложности, в зависимости от потребностей той или иной организации. К тому же, есть возможность задействования сервисов по мере роста потребностей, без использования дополнительного стороннего программного обеспечения и отдельных серверов для этих сервисов.

Так же, в межсетевом экране ИКС, помимо вышеперечисленного, есть ряд дополнительных возможностей. Рассмотрим и их.

5.4. Дополнительные функциональные модули межсетевого экрана ИКС

«Журнал ICQ». Этот сервис служит для перехвата сообщений ICQ и может использоваться как простой модуль DLP-системы для контроля переписки сотрудников и установления факта утечки конфиденциальной информации. «Журнал ICQ» работает не со всеми сторонними клиентами службы ICQ и не перехватывает зашифрованные сообщения.

Если провайдер предоставляет динамический ip-адрес, а доступ к серверу из сети Интернет необходим, то можно воспользоваться модулем «DynDNS» (динамический DNS). Предварительно нужно зарегистрироваться на сайте http://dyndns.org/ или http://no-ip.com, и зарегистрировать своё собственное доменное имя. После чего указать учётные данные в модуле «DynDNS» для доступа к учётной записи, указать провайдера и ip-адрес, который будет меняться, и задать имя хоста. Удобная функция, если нет возможности получить статический ip-адрес, но, к примеру, хочется, чтобы свой собственный сайт на своём сервере был доступен в сети Интернет.

Если в организации используются аппаратные маршрутизаторы фирмы Cisco, то межсетевой экран ИКС может подключаться к ним по протоколу Netflow v.5 для сбора и обработки статистической информации. Что может использоваться для более полного учёта объёмов трафика, анализа посещаемых ресурсов и прочее.

В состав межсетевого экрана ИКС включен модуль «Сертификаты», для создания и управления цифровыми сертификатами. Цифровые сертификаты необходимы для того, чтобы обеспечить возможность работы сетевых сервисов межсетевого экрана ИКС с использованием протокола SSL. SSL (Secure Sockets Layer — уровень защищённых сокетов) — криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером. Использование протокола SSL может быть продиктовано желанием повысить безопасность работы с данными и повышением уровня надёжности и защищённости сетевых сервисов.

Для дополнительного контроля над безопасностью межсетевого экрана ИКС, используется модуль «Монитор файлов», который позволяет отслеживать изменения в важных системных файлах и файлах конфигурации. Это может быть полезно в том случае, если злоумышленник смог каким-либо образом получить доступ к межсетевому экрану ИКС и произвёл подмену файлов или же изменил их. В таком случае в журнале будет запись о том, что есть изменения в тех файлах, которые отслеживаются.

Хорошим подспорьем в работе системному администратору послужит модуль «ARP-таблица», который позволяет отслеживать появление в сети новых устройств (по MAC-адресу), соответствие IP и MAC адресов, а также осуществлять привязку и отвязку IP адресов к MAC адресам. Особенно полезен будет этот модуль в большой сети. А также для отслеживания недобросовестных пользователей, которые могут изменять mac-адрес своих сетевых устройств, что создаёт дополнительные проблемы IT-персоналу.

В дополнение к этому, в межсетевом экране ИКС есть модуль «Сетевые утилиты», в котором собраны наиболее часто используемые сетевые утилиты для контроля состояния сети и диагностики сетевых неполадок, а именно:

- Ping, для проверки соединения;
- Traceroute, для отображения маршрута прохождения запроса до нужного хоста;
- Dig, утилита для тестирования работы DNS, путём посылки разных запросов к ним;
- Whois, для получения информации о владельце домена или диапазона ip-адресов;
- Route, для отображения текущей таблицы маршрутизации межсетевого экрана ИКС;
- Ifconfig, показывает текущую настройку сетевых интерфейсов межсетевого экрана ИКС;
- Tcpdump, отображает заголовки пакетов, которые проходят через заданную сетевую карту. Это позволяет детально анализировать проблемы с сетевым оборудованием и настройками межсетевого экрана ИКС.

Также доступно ARP-сканирование сети (на доступность локальных устройств в сети) и сканирование на проверку открытых портов в сети. Это позволяет повысить безопасность сети в целом, путём выявления проблем в настройках программного обеспечения, которое работает с сетью. Для обеспечения этих возможностей используется широко известное программное обеспечение Nmap.

Модуль «Маршруты» позволяет создавать гибкие правила маршрутизации трафика. В межсетевом экране ИКС поддерживается маршрутизация TCP/UDP, ICMP, GRE.

5.5. Функциональные модули защиты от атак

Как и полагается комплексу подобного класса, для защиты от сетевых атак извне используется межсетевой экран и детектор обнаружения атак.

Управление межсетевым экраном и работа с правилами очень простые, благодаря продуманности веб-консоли. При установке межсетевого экрана ИКС, ряд правил добавляется автоматически, для корректного функционирования ряда сетевых сервисов.

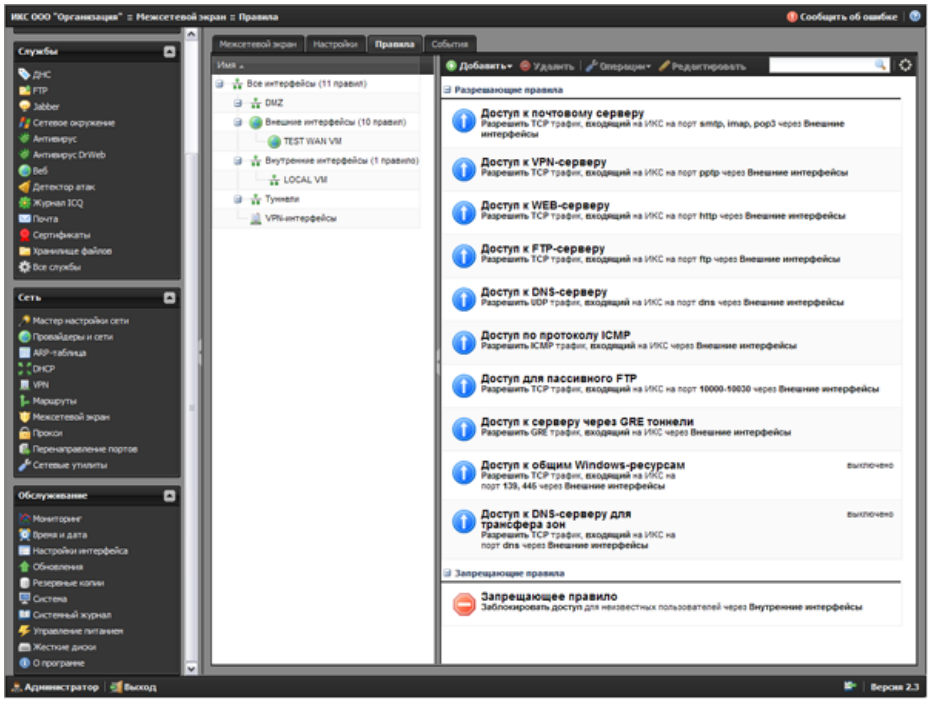


Рисунок 53. Список предустановленных правил межсетевого экрана

Помимо обычных разрешающих и запрещающих правил, можно задавать правила маршрутизации, правила ограничения полосы пропускания и правила приоритезации трафика. Это позволяет построить очень гибкую систему обработки сетевого трафика. Управление приоритетом трафика очень полезно в случае высокой загруженности каналов или наличия в сети критически важных сетевых сервисов, для которых важно обеспечить постоянную доступность. К примеру, если есть веб-сервер, на котором размещён сайт организации и важно, чтобы клиенты всегда имели к нему доступ, то можно задать правило обработки трафика, согласно которому будет обрабатываться трафик этого сервера в первую очередь. А вот почтовому трафику или FTP, можно задать и пониженный приоритет.

К тому же, правилам можно задавать время действия, что само по себе очень удобно. И предоставляет ещё большую гибкость в плане управления сетевым трафиком.

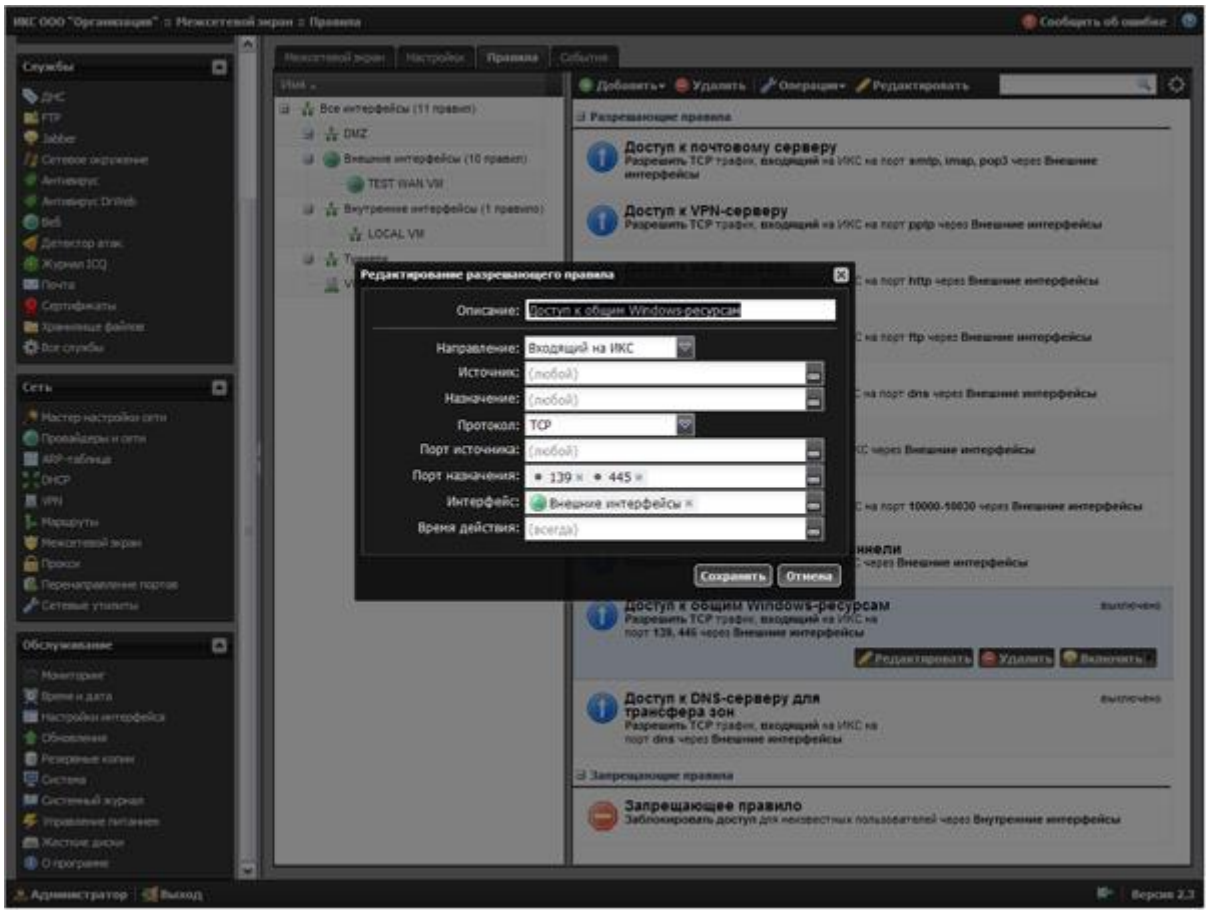


Рисунок 54. Пример редактирования правила межсетевого экрана

Для обеспечения дополнительных возможностей управления сетевым трафиком, межсетевой экран обеспечивает возможность перенаправления портов.

Для дополнительной защиты от сетевых атак используется модуль «Детектор атак», реализованный с помощью известной IPS Snort, способной выполнять регистрацию пакетов и в режиме реального времени осуществлять анализ трафика в IP сетях. IPS Snort выполняет протоколирование, анализ, поиск по содержимому, а также широко используется для активного блокирования или пассивного обнаружения целого ряда нападений и зондирований, таких как переполнение буфера, стелс-сканирование портов, атаки на веб-приложения, SMB-зондирование и попытки определения ОС.

Для корректной работы этого модуля необходимо установить правила для системы обнаружения атак.

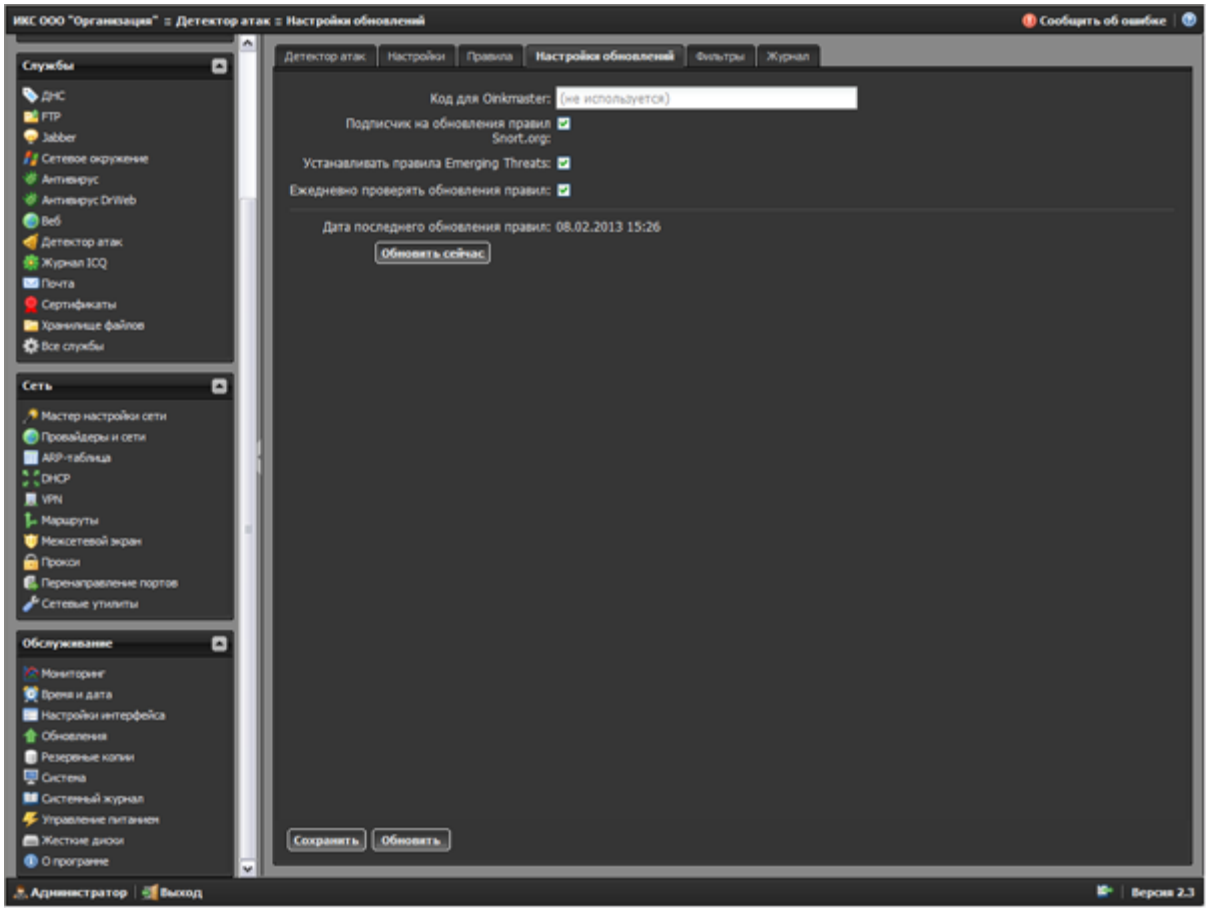


Рисунок 55. Настройка обновления списков правил модуля «Детектор атак»

Для получения и постоянного обновления первого списка правил, необходимо зарегистрироваться на сайте snort.org, получить код Oinkcode для скачивания правил и ввести его в поле «Код для Oinkcode».

Второй список правил распространяется свободно без регистрации.

После того, как нужные источники списков правил отмечены в чекбоксах, можно нажать кнопку «Обновить» и дожидаться обновления списков правил. После чего система обнаружения вторжений готова к работе.

Также можно указать дополнительные настройки для этого модуля, список защищаемых портов, сетевые интерфейсы и прочее.

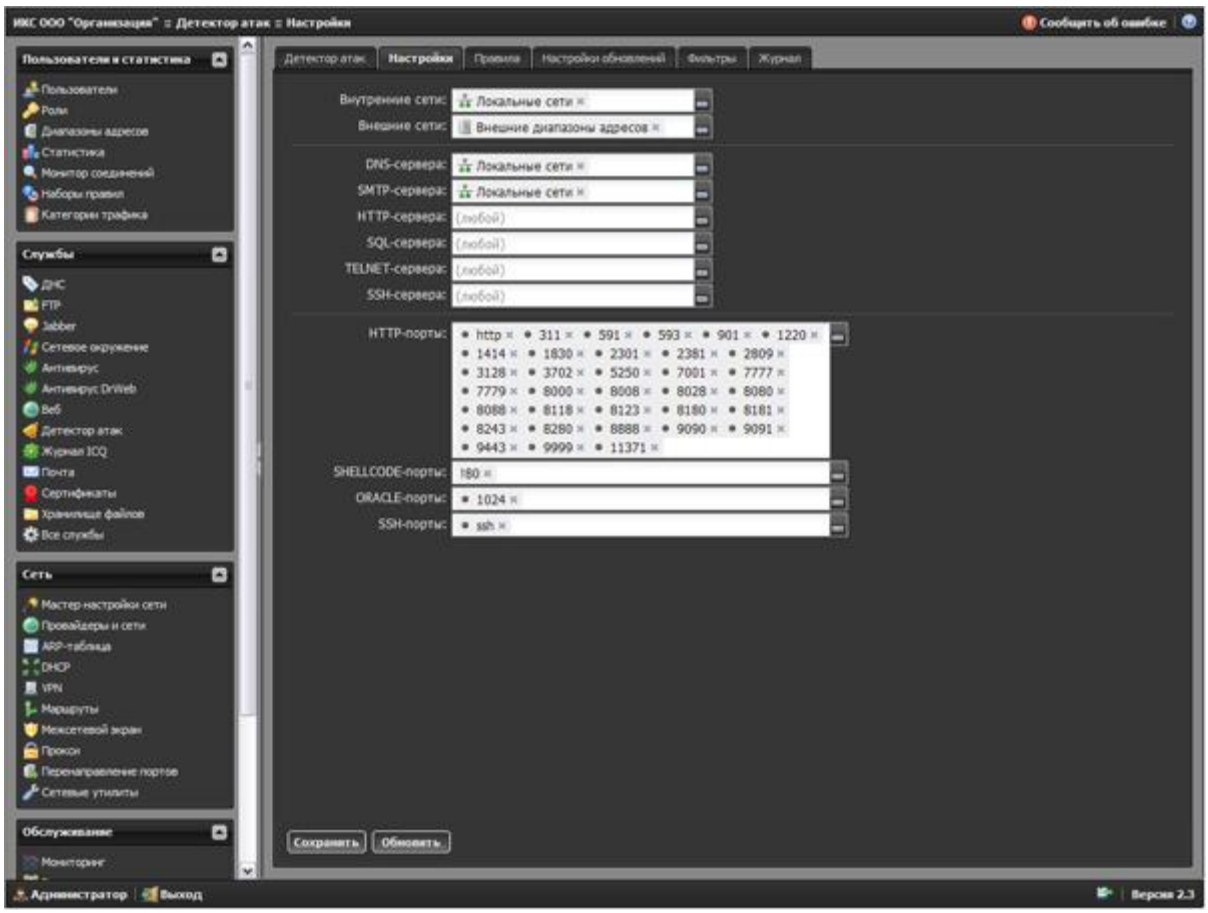


Рисунок 56. Окно настроек модуля «Детектор атак»

Стоит отметить, что Snort является довольно мощной системой предотвращения вторжений и широко распространена.

Для проверки трафика на наличие вредоносного кода, в межсетевом экране ИКС используется два антивирусных продукта. Это широко известные ClamAV (является бесплатным программным обеспечением) и российский Dr.Web (для работы требуется приобретение отдельной лицензии). Использование антивирусных продуктов на шлюзе, позволяет сильно повысить безопасность в локальной сети. При этом возможны несколько сценариев организации безопасности:

- сетевой трафик сканируется на интернет-шлюзе, на рабочих местах используется антивирусное программное обеспечение без модуля проверки трафика;
- сетевой трафик сканируется на интернет-шлюзе, на рабочих местах используется антивирусное программное обеспечение другого производителя с модулем проверки трафика;
- сетевой трафик сканируется на интернет-шлюзе, на выбранных рабочих местах используется антивирусное программное обеспечение другого производителя с модулем проверки трафика.

Как видим, межсетевой экран ИКС имеет в своём составе мощные средства противодействия сетевым и вирусным атакам. Что позволяет создать мощную инфраструктуру информационной безопасности организации или свободно интегрировать его в существующую и повысить уровень безопасности в целом.

5.6. Контроль доступа к ресурсам Интернет

Теперь рассмотрим, каким образом осуществляется контроль доступа пользователей к различным ресурсам сети Интернет.

В наше время, контроль доступа к ресурсам сети Интернет необходим по разным причинам. Это может быть и желание администрации повысить производительность труда путём блокирования развлекательных ресурсов, социальных сетей и прочего. Или повышение уровня безопасности в локальной сети путём блокировки известных вредоносных ресурсов. Или же блокирование доступа к нежелательным ресурсам в детских образовательных учреждениях согласно Федеральному закону от 29 декабря 2010 г. №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Естественно, база таких ресурсов должна постоянно пополняться.

Такая возможность реализована в межсетевом экране ИКС. Для такого контроля есть предустановленные категории трафика.

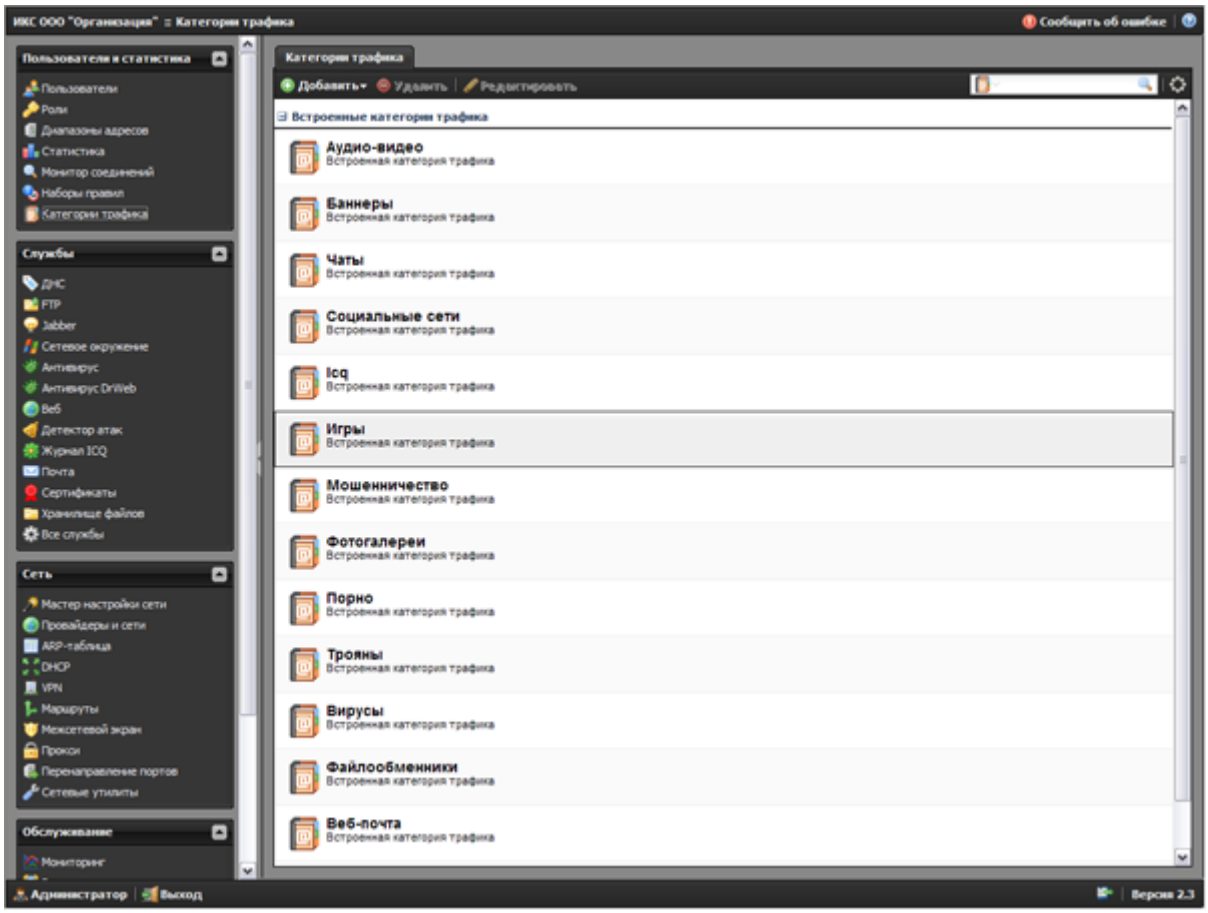


Рис. 57. Категории трафика межсетевого экрана ИКС

Стоит отметить, что эти список ресурсов в этих категориях очень обширен.

Для более гибкого и полного контроля над доступом к ресурсам сети Интернет, в межсетевом экране ИКС предусмотрена возможность создания собственных категорий и автоматических категорий.

Автоматические категории удобны тем, что системный администратор может сам вести списки требуемых ресурсов, либо же брать готовые, указывать межсетевому экрану ИКС месторасположение файлов со списком ресурсов, а потом указать период автоматического обновления этой категории. Таким образом, если в файл со списком будут внесены новые данные, они автоматически загрузятся в нужную категорию на сервере.

Для того, чтобы реализовать контроль доступа к ресурсам сети, применяются правила и наборы правил для пользователей в сети. Для работы с правила служит модуль «Наборы правил» раздела «Пользователи и статистика».

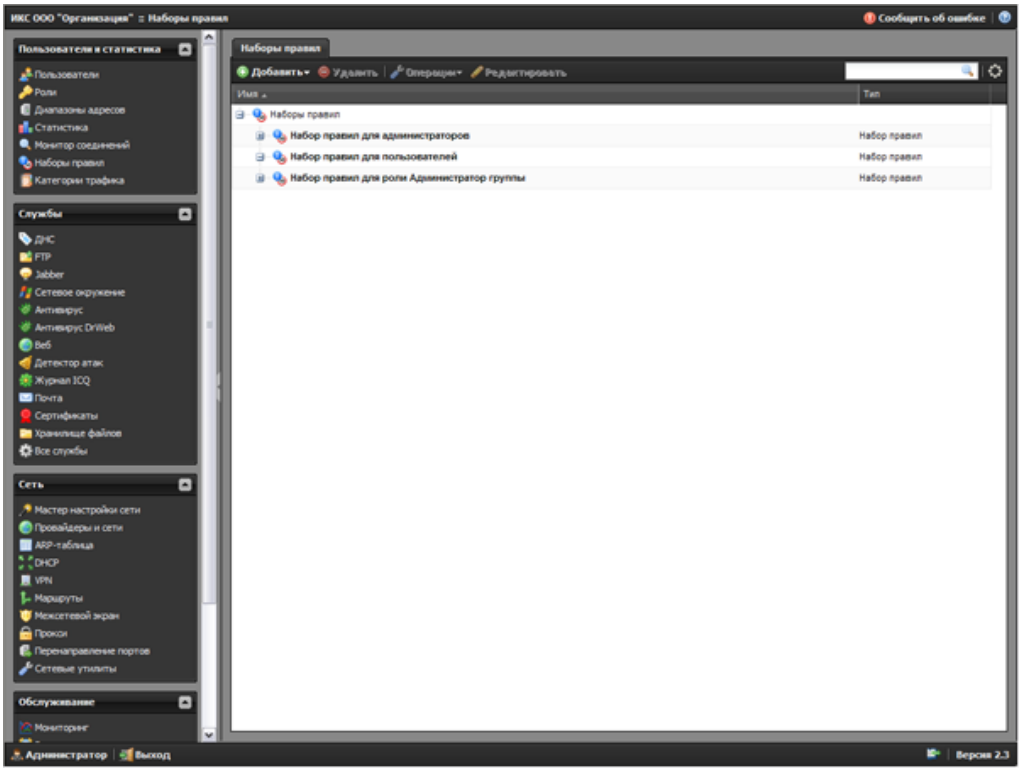


Рисунок 58. Модуль «Наборы правил» межсетевого экрана ИКС

Есть три предустановленных набора правил (по умолчанию сами правила там отсутствуют), а также можно создавать свои наборы, для большей наглядности и упрощения работы.

К примеру, можно создать набор правил «Школа», где создать правила запрещающие посещать те или иные категории ресурсов нежелательных для детей.

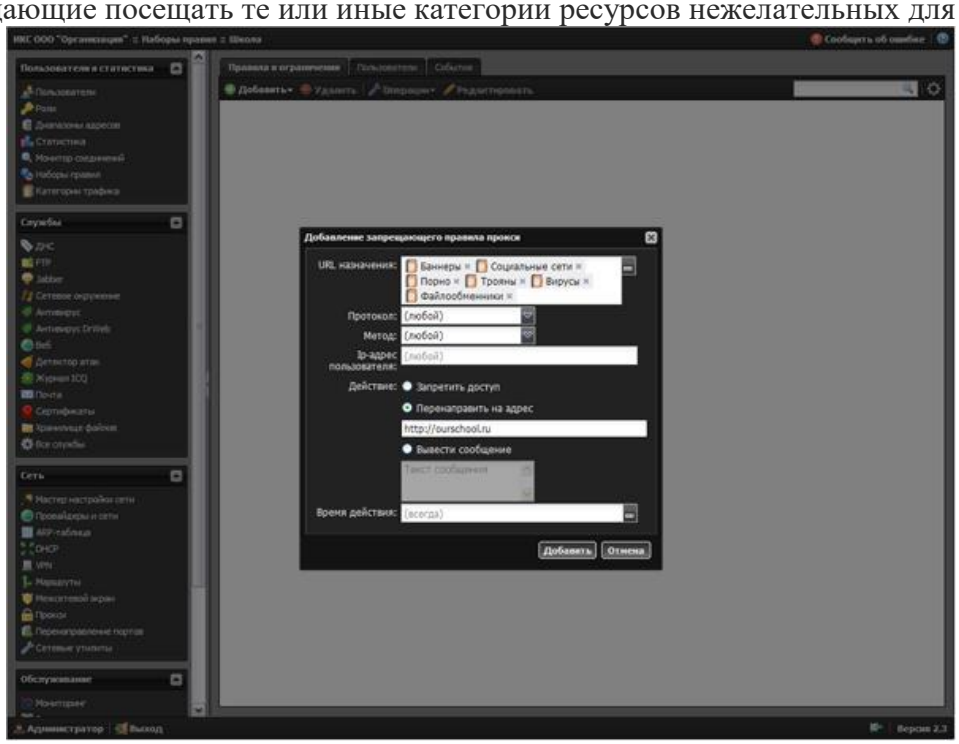


Рисунок 59. Пример создания запрещающего правила для выбранного набора правил

Доступ к ресурсам из указанных категорий можно запретить или, при попытке посетить ресурс из запрещённой категории, перенаправить на нужный сайт. К примеру, на сайт школы.

Правила могут иметь определённое время действия, которое можно задать. Это позволяет гибко управлять контролем доступа к ресурсам в зависимости от времени суток. К примеру, можно запретить посещение социальных сетей в рабочее время, но разрешать посещать в обеденный перерыв.

Кроме правил контроля доступа, можно создавать правила управления шириной пропускания канала для отдельных пользователей, групп пользователей и диапазонов адресов.

Также, в межсетевом экране ИКС предусмотрена возможность просмотра детальной статистики посещения ресурсов сети, объём потреблённого трафика и прочей статистической информации.

Таким образом, межсетевой экран ИКС, предоставляет возможность контролировать работу пользователей в сети Интернет в полном объёме. С учётом контроля доступа к ресурсам сети, ограничения на объём потребляемого трафика и управления загрузкой каналов.

5.7. Мониторинг и управление системой

Помимо всех вышеперечисленных возможностей, межсетевой экран ИКС позволяет в реальном времени контролировать состояние оборудования, на котором он установлен, просматривать загрузку каналов, качество связи, контролировать состояние операционной системы и многое другое.

Для контроля всех этих параметров служит модуль «Мониторинг» (рис. 60).

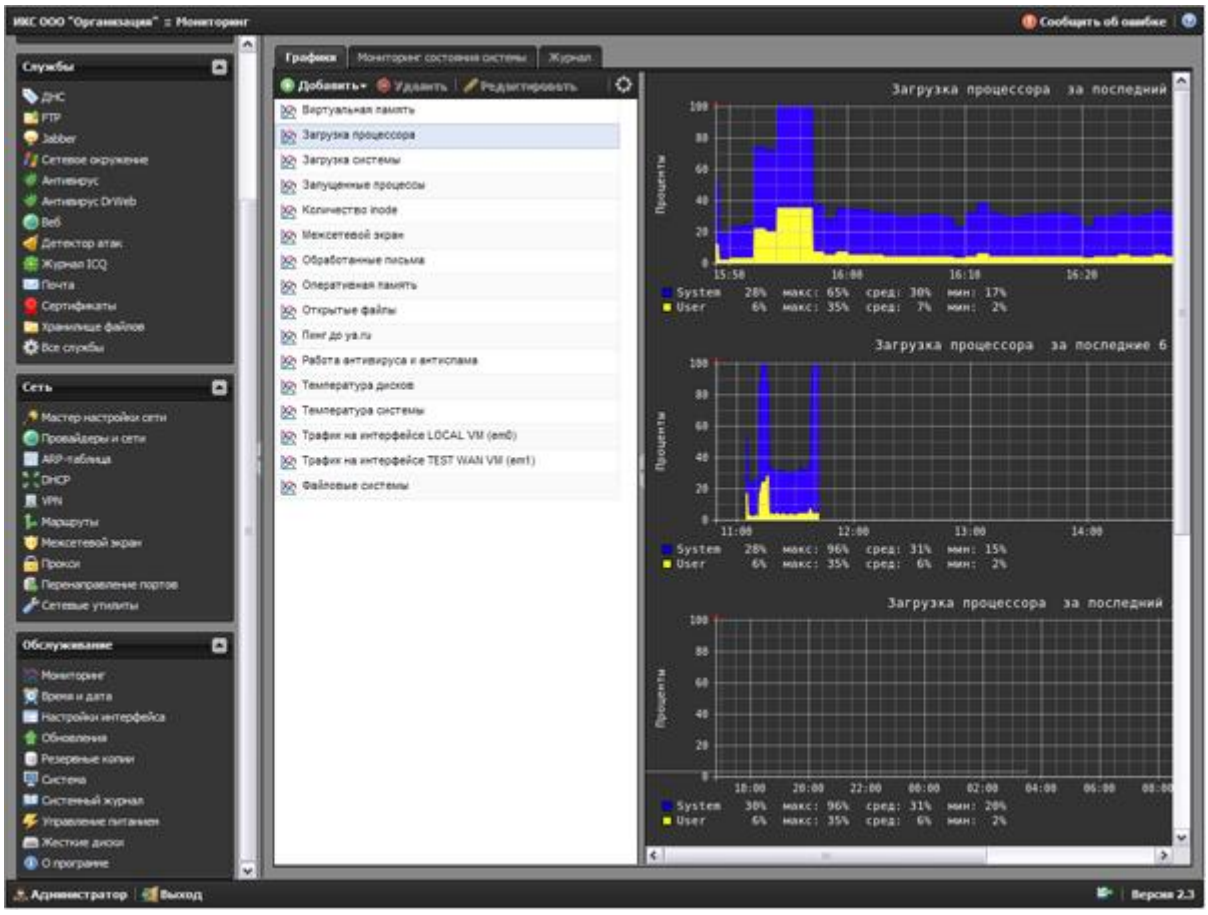


Рисунок 60. Модуля «Мониторинг» межсетевого экрана ИКС. Контроль загрузки процессора

Данные сортируются по временным интервалам: последний час, последние 6 часов, последний день, неделя и месяц. Это даёт системному администратору возможность следить за состоянием системы в целом, её отдельных параметров, отслеживать пиковую нагрузку для возможной оптимизации работы системы и предотвращение отказа в обслуживании.

Для облегчения восстановления системы после сбоя (от подобного не застрахован никто), в межсетевом экране ИКС предусмотрена возможность автоматического создания резервных копий настроек системы, а также полного резервного копирования системы. Помимо локального хранения резервных копий, предусмотрена возможность сохранения резервных копий на флэш-накопитель и на удалённый FTP-сервер. Что сильно повышает возможность быстрого восстановления работы, в случае если локальные резервные копии были утеряны или повреждены. Настройку резервного копирования можно провести в модуле «Резервное копирование».

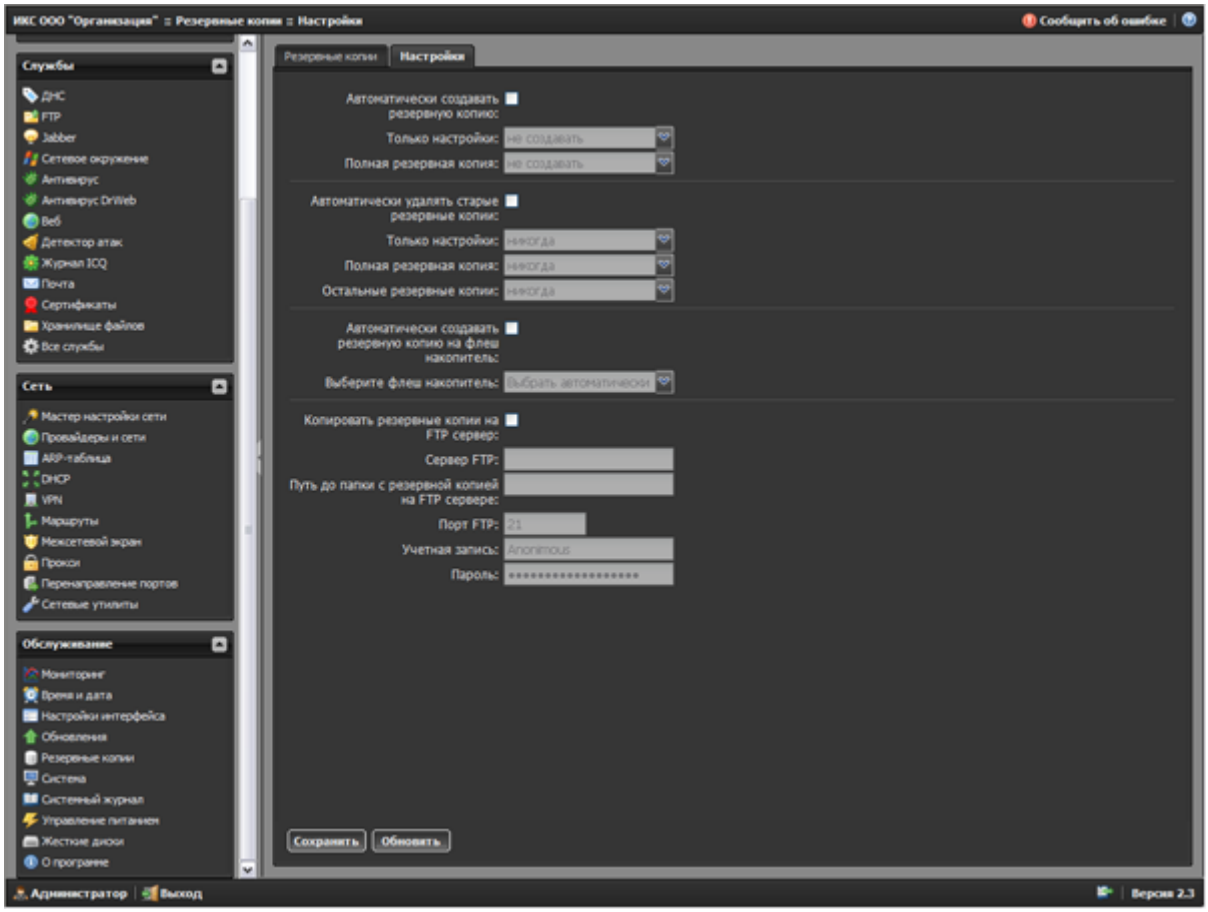


Рисунок 61. Модуль «Резервное копирование», настройка создания резервных копий

Для дополнительного контроля межсетевого экрана ИКС предусмотрен модуль «Системный журнал». В модуле «системный журнал» отображаются сообщения о действиях пользователей, изменениях в статусах сервисов и ошибках системы. Для того, чтобы не пропустить какое-либо очень важное событие, в этом модуле предусмотрена система отправки уведомлений ответственному лицу. Уведомление может быть отправлено по электронной почте, а также с помощью Jabber или ICQ.

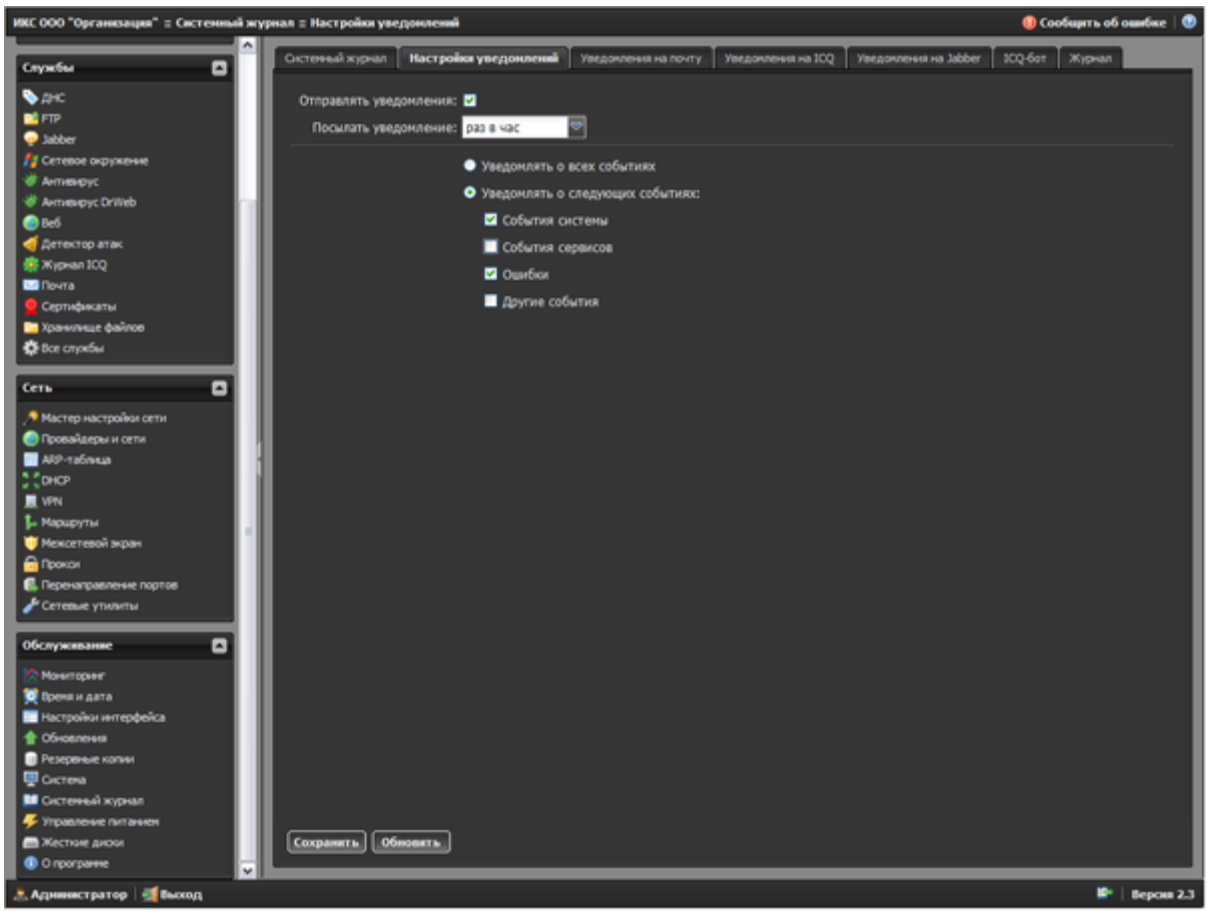


Рисунок 62. Настройка категорий уведомлений для отправки

Таким образом, нет необходимости постоянно следить за журналом событий, что, в целом, затруднительно. Такая возможность обеспечивает своевременное уведомление о тех или иных событиях, без постоянного отвлечения внимания.

Модуль «Жёсткие диски» предназначен для управления дисковой подсистемой сервера с установленным межсетевым экраном ИКС. Довольно часто получается так, что объёма установленных жёстких дисков перестаёт хватать. Для этого и была введена возможность лёгкого добавления новых жёстких дисков, создания дополнительных разделов и прочего в межсетевом экране ИКС.

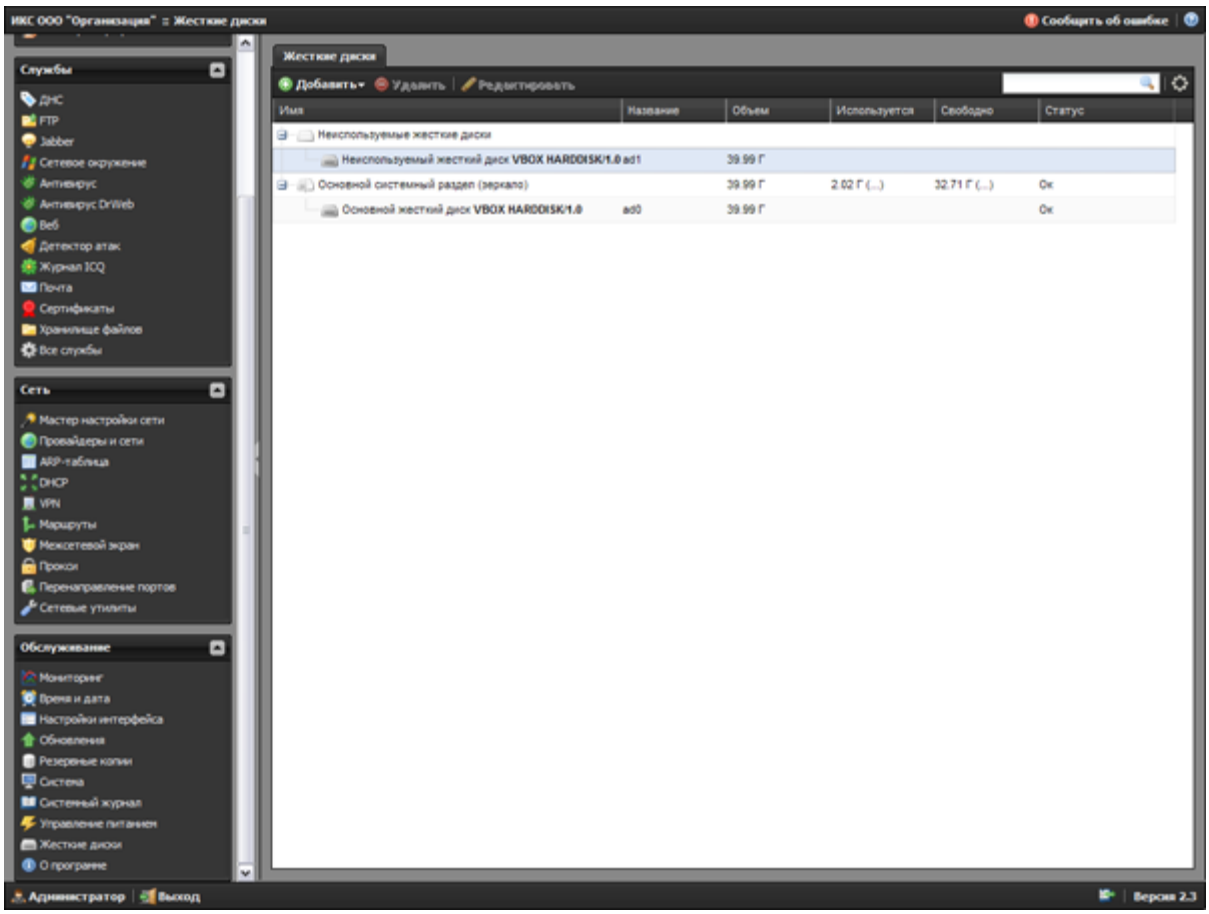


Рисунок 63. Управление жёсткими дисками в межсетевом экране ИКС

Для тех случаев, когда доступ к межсетевому экрану ИКС невозможен с помощью веб-интерфейса, предусмотрена консоль восстановления, которую можно активировать нажатием клавиши F2, на клавиатуре, которая подсоединена к серверу с установленным межсетевым экраном ИКС. С помощью консоли восстановления можно изменить настройки сетевых интерфейсов, изменить таблицу маршрутизации, изменить пароли доступа к межсетевому экрану ИКС, настроить дисковую подсистему, перезагрузить или выключить сервер.

На этом мы заканчиваем обзор сертифицированного межсетевого экрана ИКС и переходим к выводам.

5.8. Выводы

Межсетевой экран ИКС оставил приятное впечатление. Это хорошо продуманный программный продукт с очень широкими возможностями. Его легко освоить персоналу, который впервые сталкивается с подобным классом продуктов или же не имел достаточного опыта работы. Для опытных системных администраторов в межсетевом экране ИКС предусмотрена возможность сколь угодно тонкой настройки параметров, а также широкий выбор сетевых сервисов для построения системы высокой сложности. Что даёт возможность наиболее полно учесть требования той или иной организации в создании сетевой инфраструктуры.

Достоинства:

- Использование в качестве основы операционной системы FreeBSD.
- Большое количество сетевых сервисов, в том числе FTP, Web, DNS, DHCP, VPN, прокси, почтовый и jabber сервера, LDAP, и другие.
- Использование популярной и хорошо зарекомендовавшей себя IPS Snort.

- Возможность проверки трафика с помощью антивирусов ClamAV, который является бесплатным и Dr.Web, для работы с которым нужно приобрести отдельную лицензию.
- Возможность построения гибкой системы правил обработки сетевого трафика, в том числе возможность контентной фильтрации, приоритезация трафика, маршрутизация, перенаправление портов, указание временных диапазонов работы правил обработки трафика, управление полосой пропускания и прочее.
- Поддержка работы на виртуальных машинах. Но преднастроенные образы отсутствуют.
- Система мониторинга оборудования, компонентов межсетевого экрана ИКС и самой системы.
- Простота и наглядность в настройке, удобный веб-интерфейс.
- Пробный период использования составляет 35 дней.
- Бесплатная техническая поддержка и хорошая документация.
- Наличие сертификации ФСТЭК (сертификат ФСТЭК №2623 от 19 апреля 2012 г.).
- Пожизненная лицензия, не ограниченная по времени использования.

Недостатки:

- Использование в качестве основы операционной системы FreeBSD. Да, это как плюс, так и минус. Минус в плане поддерживаемого оборудования. У операционной системы FreeBSD есть определённые проблемы в этом направлении. К сожалению, операционная система FreeBSD немного отстаёт, в плане поддержки нового оборудования, от Linux и, тем более, от Microsoft Windows. Поэтому, мы рекомендуем перед установкой межсетевого экрана ИКС убедиться, что оборудование поддерживается операционной системой FreeBSD.
- Отсутствие в качестве провайдера Wi-Fi соединения. С учётом развития беспроводных сетей – это актуально. Разработчики добавили поддержку Wi-Fi соединений в версии ИКС 4.4, которая на момент публикации обзора проходит сертификацию ФСТЭК.
- В процессе подготовки обзора были проблемы с использованием сетевого адаптера PCnet FAST III в виртуальной машине Virtualbox. Система корректно заработала только с сетевым адаптером Intel.
- Модуль «Обновления» сообщает об отсутствии обновлений, не смотря на то, что новое обновление в списке есть.
- Проблемы работы с консолью в некоторых менее популярных браузерах. Например, Internet Explorer 8 довольно часто предлагал остановить сценарий выполнения на странице, при работе с веб-интерфейсом;
- Консоль восстановления довольно ограничена в возможностях. Например, желательно иметь возможность попасть в стандартную оболочку, для прямой работы с операционной системой межсетевого экрана ИКС в особо тяжёлых случаях;
- Хотелось бы иметь возможность дополнительной установки пакетов программного обеспечения, из списка поддерживаемых разработчиками, с интеграцией в веб-интерфейс. Это расширило бы возможности продукта в целом.

Явные преимущества этого решения в том, что можно бесплатно использовать полнофункциональную версию на 8 пользователей.

Лицензия на 100 пользователей обойдется всего в 6.600 рублей для образовательных организаций. Для сравнения, аналогичный продукт от компании Ideco стоит 45.150 рублей. В комплекте есть все, что нужно и даже больше. Установка и настройка не вызывает проблем, все интуитивно понятно. Из функционала можно использовать Jabber для общения, папки общего доступа и встроенный WEB-сервер. Очень удобно отключать пользователей от сети Интернет, например, кабинет информатики чтобы дети не сидели в интернете во время перемены. Можно настроить график автоматического

включения/выключения пользователей. Порадовала функция ограничения скорости, с небольшим каналом и большим количеством компьютеров она просто жизненна необходима, плюс можно настроить квоты на объем трафика. Очень понравилось, что можно в реальном времени наблюдать кто и что ищет в сети Интернет. По каждому пользователю доступна полная статистика: посещенные сайты, объем трафика, поисковые запросы.

Контентную фильтрацию можно настроить в несколько уровней. *Первый уровень* фильтрации — встроенные категории трафика. Есть готовые списки сайтов и регулярных выражений, только указал к какому пользователю или группе применять и все работает. Можно создать свои категории фильтрации, указав конкретные сайты или ключевые слова. *Второй уровень* — поддержка сервиса SkyDNS. Нужно указать в настройках шлюза использовать их DNS-сервер и иметь внешний статический IP-адрес. Управление категориями блокировки осуществляется только через сайт SkyDNS. *Третий уровень* — встроенный контент-фильтр, который блокирует по содержимому. Уже заложены списки от Министерства юстиции РФ и Госнаркоконтроля.

5. Веб - фильтр Remparo

Данный фильтр является принципиально новым решением, которое с помощью технологий лингвистического анализа с высокой точностью определяет тематику содержимого любых страниц, что позволяет блокировать только нежелательные страницы, а не целые сайты. Основной модуль системы контетной фильтрации автоматически с высокой точностью определяет тематические категории текста, т.е. о чем идет речь на странице. Информация о всех запросах пользователей и результатах их обработки веб-фильтром протоколируется. С помощью отчетов можно получить информацию о том, какие страницы, в какое время и с каким результатом посещали пользователи. Веб-фильтр Remparo предоставляет широкий выбор политик фильтрации: порнография, наркотики, алкоголь, насилие и жестокость, нецензурная лексика, самоубийства, азартные игры, социальные сети, сайты знакомств и др. При необходимости пользователей можно разделить на группы. Для разных групп можно задавать разные политики фильтрации и расписание (дни недели и время) применения выбранных политик фильтрации.

Установка программного обеспечения производится на оборудовании образовательной организации. Программно-аппаратный комплекс Remparo Education Edition – это сервер (на платформе Linux или Windows) с установленным программным обеспечением.

6. ContentKeeper Express

В ContentKeeper Express реализована SaaS-модель (Software as a Service – программное обеспечение как услуга). Последовательно рассмотрим, в чем заключается суть данной модели, и какие преимущества она обеспечивает.

Вначале рассмотрим, какие основные технологии фильтрации контента используются на настоящий момент в продуктах аналогичного назначения (таблица 1).

Таблица 1. Используемые технологии фильтрации

№	Используемые технологии	Описание
1.	«Черные» и «белые» списки	Доступ только к проверенным ресурсам приводит к существенным ограничениям. Интернет «схлопывается» до набора сайтов, в результате чего теряется его универсальность.
2.	Системы репутации, созданные на основе оценки групп обычных пользователей или экспертов; использование разных видов анализа (например, лингвистического) в реальном времени.	Невозможность ручного контроля всего массива сайтов и веб-страниц приводит к тому, что получаемая защита становится фрагментарной. А использование методов анализа, работающих в реальном времени, приводит к задержкам в работе.
3.	Автоматическая фильтрация сайтов с использованием искусственного интеллекта и мощных систем обработки данных.	В совокупности с предыдущим технологиями позволяет построить достаточно эффективную систему фильтрации. Однако для такой системы необходимо наличие мощного оборудования, которое будет проводить постоянный анализ сайтов, и частая система обновлений категоризированной базы Web-ресурсов для клиентских программ.

Данные методы реализуются при построении двух основных технологических «видов» фильтрации:

- промышленной фильтрации корпоративного уровня, которая осуществляется на специальных серверах, входящих в периметр защиты локальных сетей;
- персональной фильтрации, которая выполняется на персональных компьютерах, в том числе и на домашних.

Соответственно, использование первых двух перечисленных технологий возможно при любом виде фильтрации, а третья технология доступна только в корпоративных решениях.

Однако постоянное развитие информационных технологий позволяет построить систему фильтрации иным способом. Система анализа может размещаться в «облаке», на серверах компании, предоставляющей услуги по фильтрации контента. А на персональные компьютеры пользователей устанавливается только специальные агенты небольшого объема, использующие минимальный объём ресурсов компьютера.

Такой подход называется SaaS-модель («ПО как услуга») и позволяет экономить как финансовые ресурсы, за счет снижения цены решения и сложности администрирования (не надо покупать дорогостоящее оборудование), так и вычислительные ресурсы конечных компьютеров (вся ресурсоемкая работа вынесена в «облако»).

Именно такой подход реализован в ContentKeeper Express. На конечных точках устанавливаются только небольшие клиентские программы, в которых реализуется прозрачная для пользователя фильтрация, блокирующая запрещенный администратором контент. Администратор может создавать профили безопасности на основе своих собственных настроек, а также правил и баз, загружаемых с серверов ContentKeeper Express Technologies. Указанные правила и базы создаются в результате работы искусственного интеллекта и располагаются в «облаке» на серверах компании.

Для создания правил безопасности и баз используется технология, которая называется производителем «Коллаборативная фильтрация замкнутого цикла» (Closed Loop Collaborative Filtering). Это система так называемого «замкнутого цикла», которая осуществляет сбор, анализ и категоризацию URL-адресов сайтов по всем сегментам сети

Интернет. Обработанные URL помечаются как относящиеся к одной или нескольким категориям - «азартные игры», «насилие», «новости» и т.д. После этого производится рассылка выработанных решений всем узлам фильтрации, расположенным в сети SaaS, как в случае ContentKeeper Express, либо установленным у клиентов, как в случае ContentKeeper Web, и обрабатывается обратная связь от них. Данный процесс происходит непрерывно, новые обновления поступают каждый час, что позволяет реагировать на новые угрозы практически в масштабе реального времени. В описании своих продуктов ContentKeeper Technologies использует следующую иллюстрацию принципов работы своей технологии.

Рисунок 64. Иллюстрация работы «Коллаборативной фильтрации замкнутого цикла»

Администрирование ContentKeeper Express осуществляется через веб-интерфейс. Для настройки параметров фильтрации на ПК в организации администратор должен зайти на сайт ContentKeeper Technologies и зарегистрироваться в панели управления устройством под своей учетной записью.

6.1.Функциональные возможности ContentKeeper Express

В ContentKeeper Express реализованы следующие основные возможности:

1. Фильтрация контента. Поддерживается фильтрация с использованием классификационных списков ContentKeeper Technologies, а также на основе «черных» и «белых» списков. Осуществляется многофакторное управление доступом (URL, категории сайтов, ключевые слова, типы загружаемых файлов, управление по времени). Также поддерживается режим ограниченной функциональности - при отсутствии доступа к Интернету фильтрация может осуществляться по сайтам внутренней сети провайдера.
2. Контроль программ для мгновенно обмена сообщениями. Отслеживаются и контролируются сообщения, отправленные клиентами программ данного типа коммуникации.
3. Составление отчетности. В течение всей работы программы может протоколироваться активность всех пользователей. Полученные данные представляются в виде графических отчетов по заданным администратором критериям (конкретный пользователь, временной период, группа сайтов и т.д.).
4. Обновления. Модуль обновлений при наличии доступа в Интернет работает автоматически. Загрузка новых баз в узлы фильтрации осуществляется с частотой раз в час.

5. Администрирование. Для управления используется ролевой принцип, при котором для каждой учетной записи на одном компьютере и для всех контролируемых компьютеров может быть назначен индивидуальный или общий набор фильтров.

6.2.Процесс установки ContentKeeper Express

Процесс установки ContentKeeper Express достаточно прост и не отличается от установки большинства других программ. Версия клиента для установки заказывается на сайте производителя по адресу: http://express.contentkeeper.com, ссылка для закачки приходит на указанный пользователем e-mail. Инсталляционные пакеты являются индивидуальными для каждого заказа, т.е. для каждого набора инсталляций, имеющих общий аккаунт администратора (e-mail и пароль). При заказе продукта на сайте производителя необходимо заполнить регистрационную форму. Заданный адрес электронной почты и пароль в этой форме будут в дальнейшем использоваться в качестве логина и пароля для входа в Web-администрирование ContentKeeper Express.

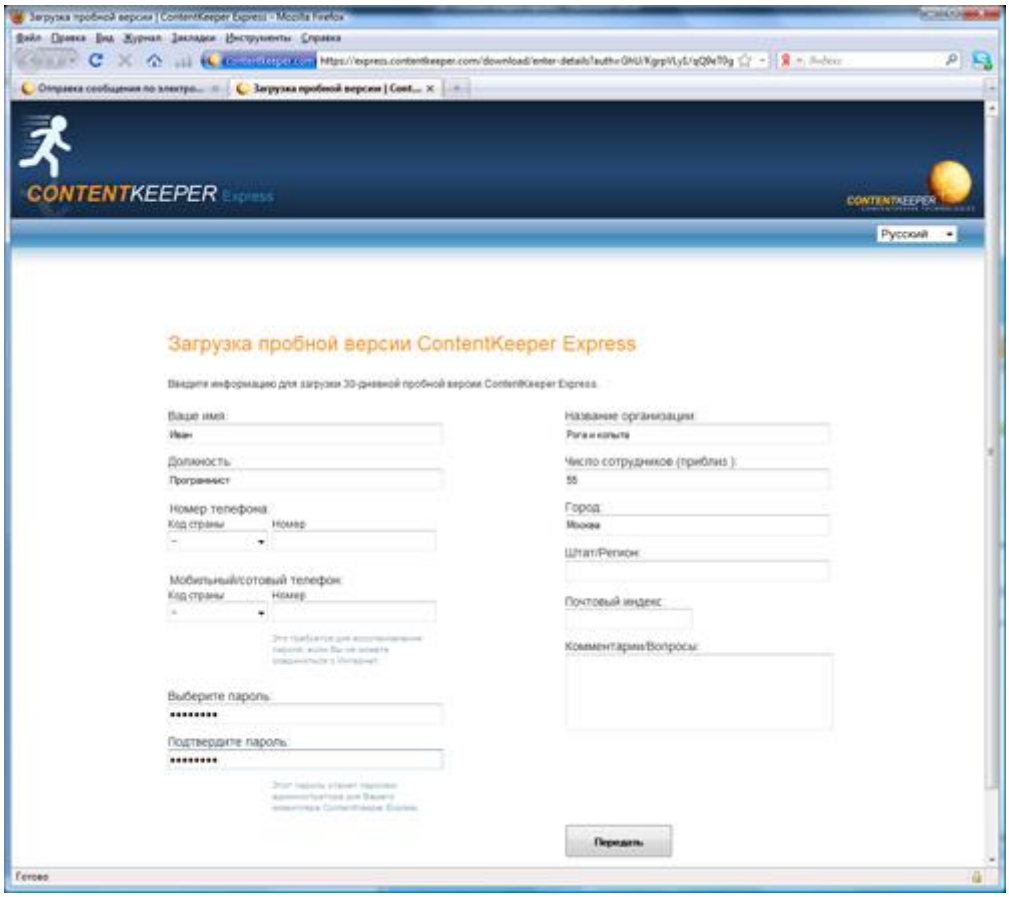


Рисунок 65. Заполнение регистрационной формы для скачивания клиента ContentKeeper Express

После запуска инсталляционного файла мы видим окно, в котором предлагается выбрать язык установки программы. Выбрав язык, жмем кнопку «ОК».

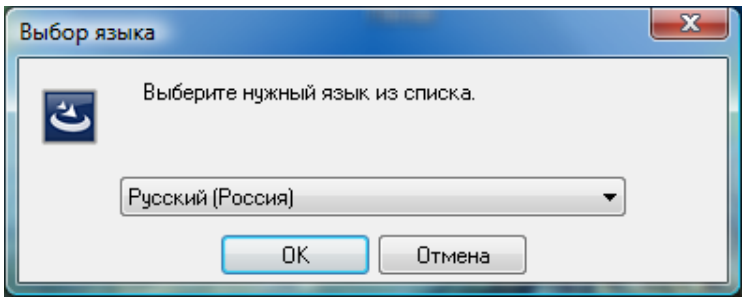


Рисунок 66. Выбор языка ContentKeeper Express

После этого появляется начальное окно мастера установки с рекламой программы. Жмем «Далее» (рис. 67).

Рисунок 67. Приветственное окно мастера установки ContentKeeper Express

В следующем окне мы можем ознакомиться с лицензионным соглашением. Внимательно его читаем, выбираем пункт «Я принимаю условия лицензионного соглашения» и жмем «Далее» (рис. 68).

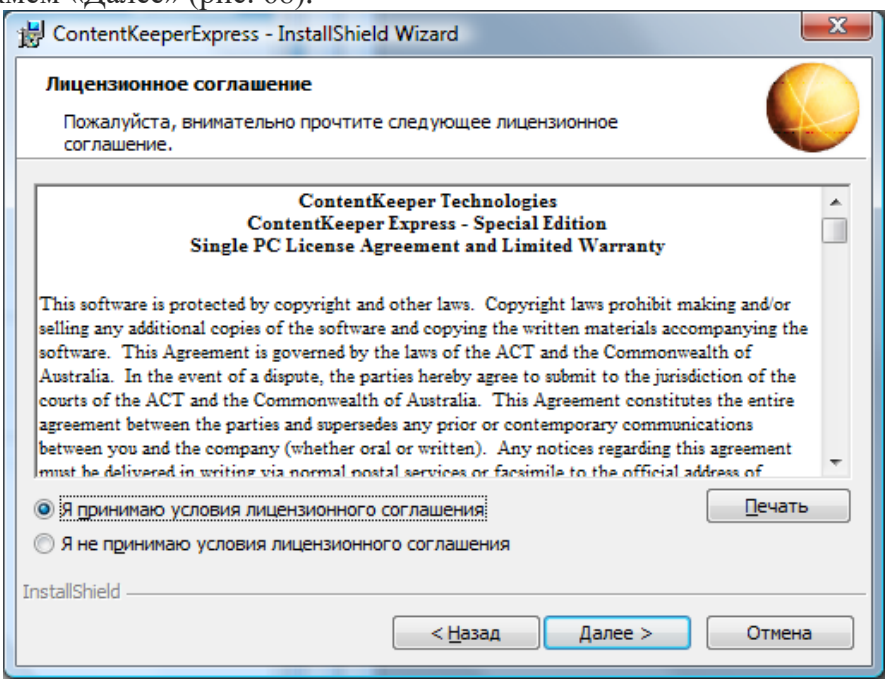


Рисунок 68. Подтверждение лицензионного соглашения ContentKeeper Express

В следующем окне выводится сообщение о том, что программа готова к началу установки. Нам рекомендуют закрыть все работающие приложения и проверить наличие соединения с Интернетом. Сделав это, нажимаем кнопку «Установить» (рис. 69).

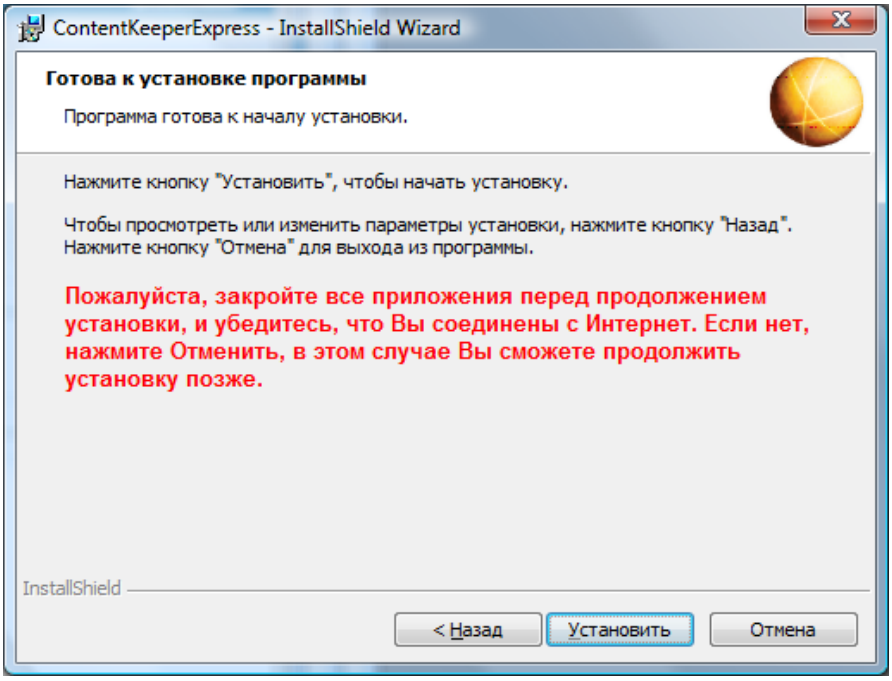


Рисунок 69. Запуск установки ContentKeeper Express

После окончания установки программы нужно запустить процесс ее конфигурирования. Для этого жмем кнопку «Далее» (рис. 70).

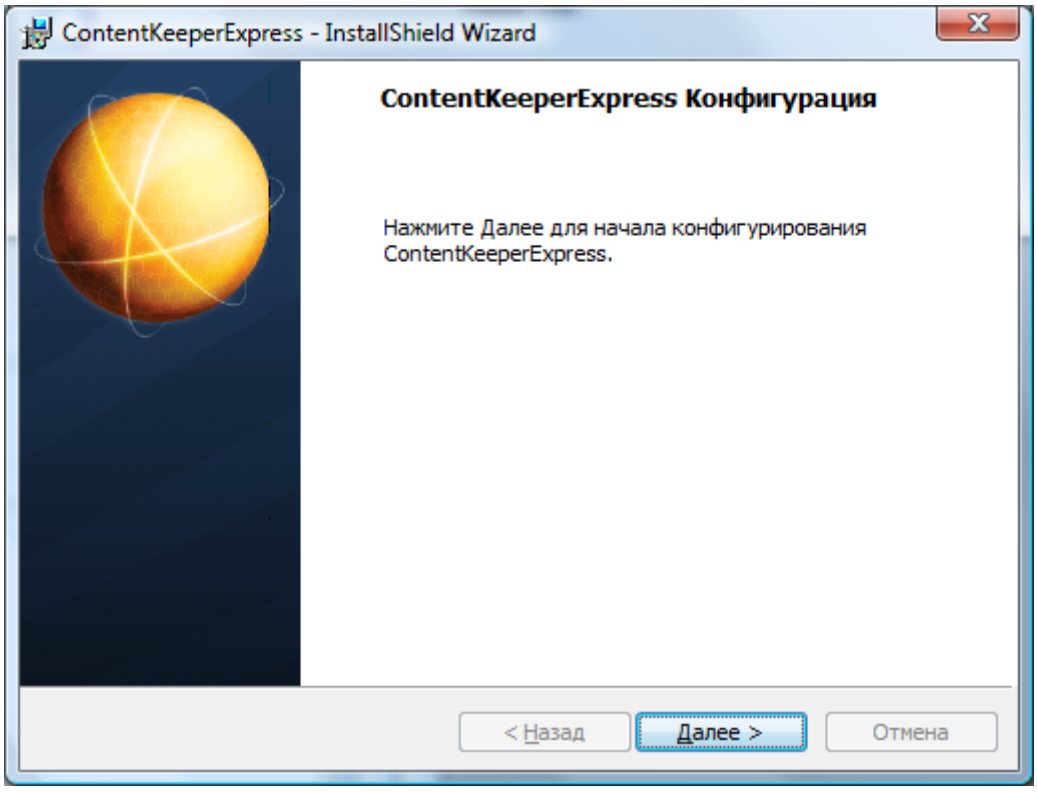


Рисунок 70. Запуск конфигурирования ContentKeeper Express

На этом процесс установки завершен.

6.3.Работа с продуктом

Теперь мы можем приступить непосредственно к работе с программой. В трее нажимаем пиктограмму с изображением «бегущего человека». После этого запускается браузер, выбранный в системе «по умолчанию», открывается страница http://express.contentkeeper.com и выводится окно для входа в Web-администрирование. В нем мы вводим адрес электронной почты в качестве логина и пароль, которые мы задали на этапе скачивания инсталляционного пакета программы.

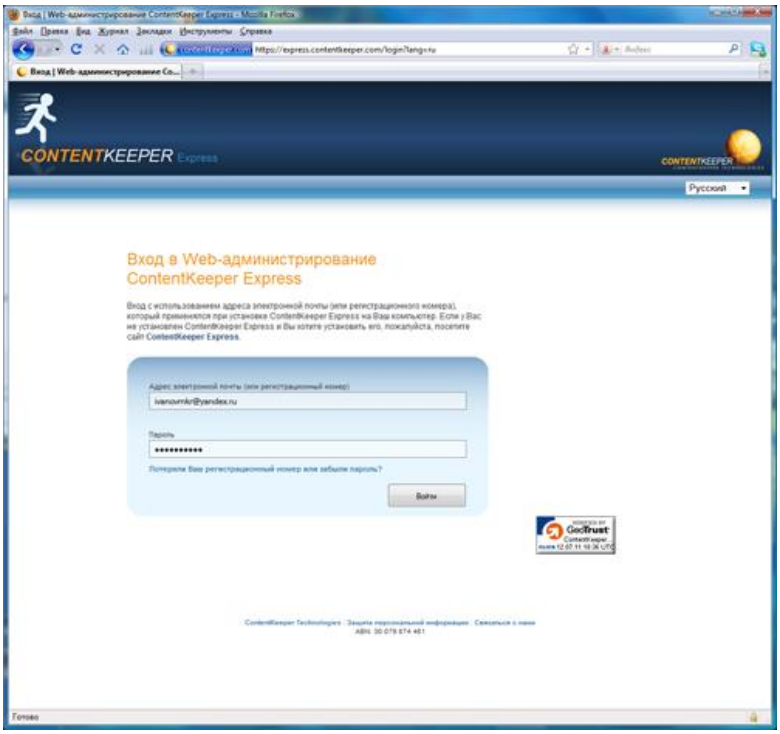


Рисунок 71. Вход в Web-администрирование ContentKeeper Express

После входа открывается главное окно программы, которое состоит из заголовка и двух панелей: панели управления (расположена в левой части окна) и информационной панели (расположена в правой части окна). Панель управления содержит четыре вкладки (выполненных в виде раскрывающихся списков с набором пунктов) – «Мой профиль», «Пользователи», «Настройки фильтрации» и «Мониторинг».

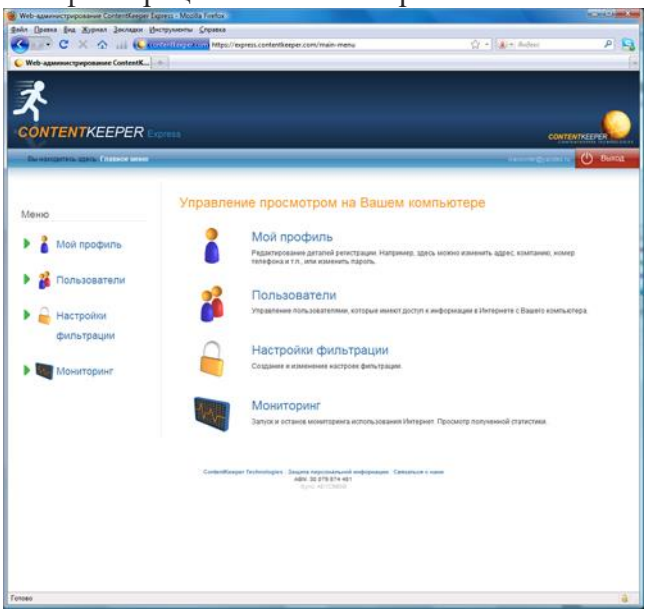


Рисунок 72. Главное окно ContentKeeper Express

Последовательно рассмотрим функциональность, доступ к которой мы можем получить при помощи каждой вкладки.

Вкладка «Мой профиль» предназначена для редактирования данных об администраторе.

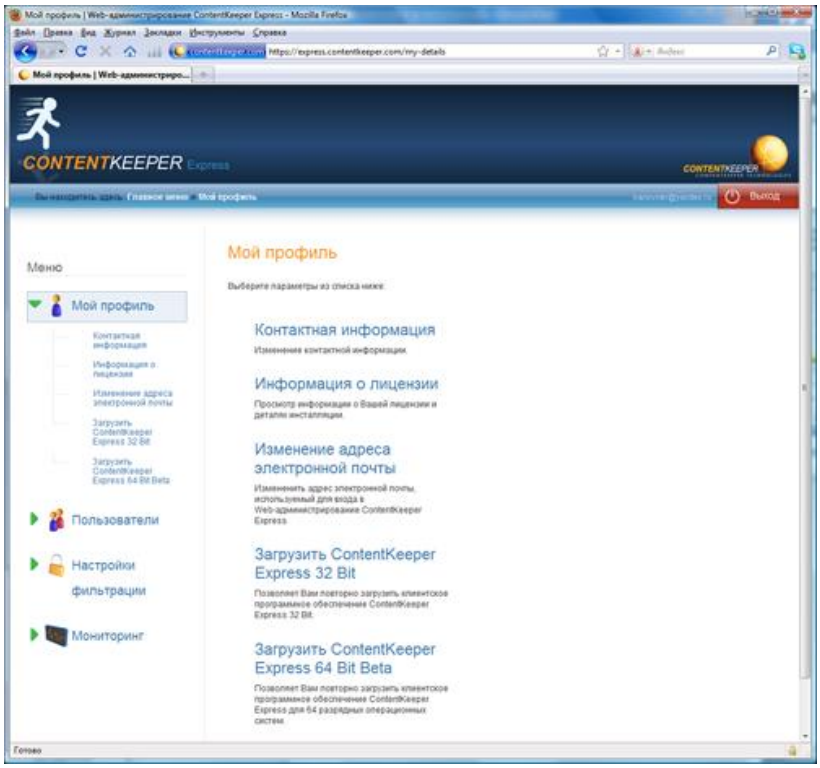


Рисунок 73. Вкладка «Мой профиль»

В разделе «Контактная информация» можно изменить свои данные, которые были указаны при регистрации. Данное окно отображалось не корректно в каждом из четырех заявленных для использования браузеров.

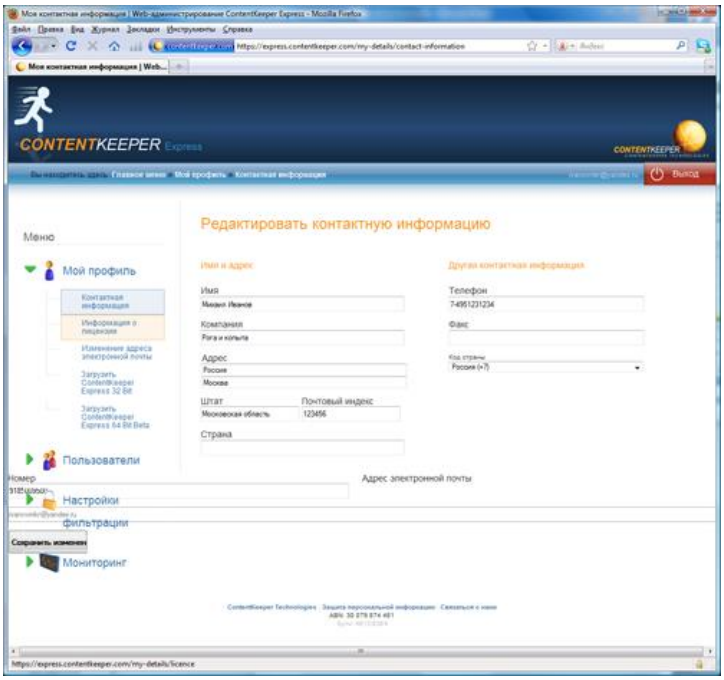


Рисунок 74. Раздел «Контактная информация»

Раздел «Информация о лицензии» содержит сведения о типе лицензии (пробная или полная), сроках ее действия, количестве инсталляций, а также сведения о деталях установки (имя и IP-адрес компьютера, дата инсталляции, версия программы и т.д.). В данном разделе мы можем купить или обновить лицензию, нажав соответствующие кнопки (рис. 75).

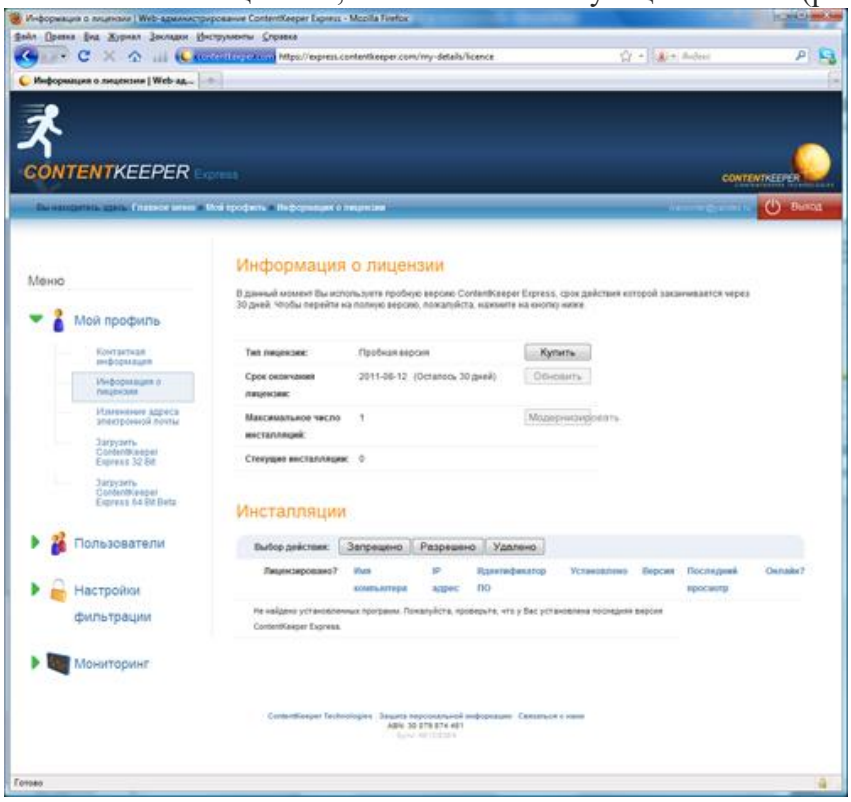


Рисунок 75. Раздел «Информация о лицензии»

В разделе «Изменение адреса электронной почты» можно изменить e-mail, который Вы используете для входа в Web-администрирование ContentKeeper Express.

Разделы «Загрузить ContentKeeper Express 32 Bit» и «Загрузить ContentKeeper Express 64 Bit Beta» позволяют скачать новые версии ContentKeeper Express для работы в 32-х и 64-х разрядных операционных системах.

Вкладка «Пользователи» предназначена для настройки доступа к Интернету для каждой учетной записи на всех контролируемых компьютерах.

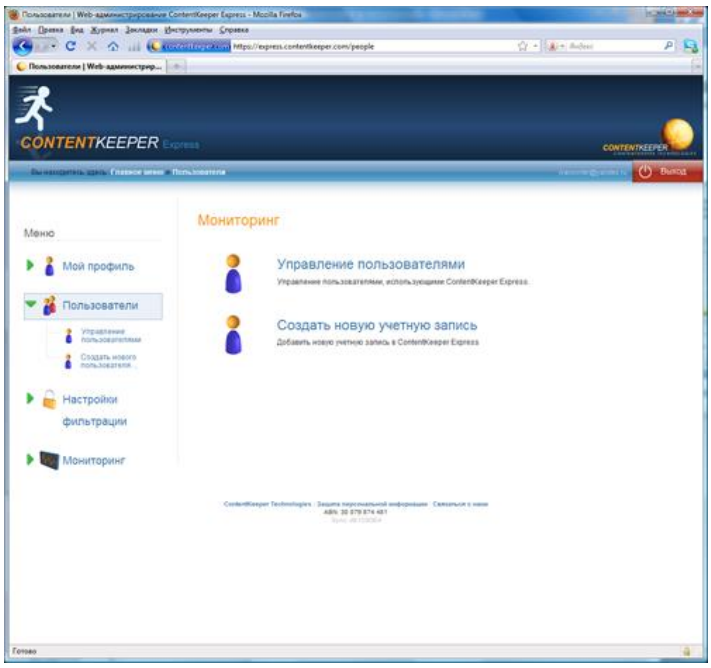


Рисунок 76. Вкладка «Пользователи»

В разделе «Управление пользователями» Вы можете задать набор фильтров для каждой учетной записи или создать новую учетную запись. При начале работы с программой набор фильтров сильно ограничен, поэтому для решения конкретных задач нужно создавать свои собственные (пользовательские) фильтры.

При создании нового пользователя нам необходимо задать его имя, используемый пароль, тип учетной записи (администратор или пользователь Интернет) и применяемый для него набор фильтров. Создавать учетные записи с правами администратора не рекомендуется, так как из-под такой учетной записи можно удалить клиент ContentKeeper Express.

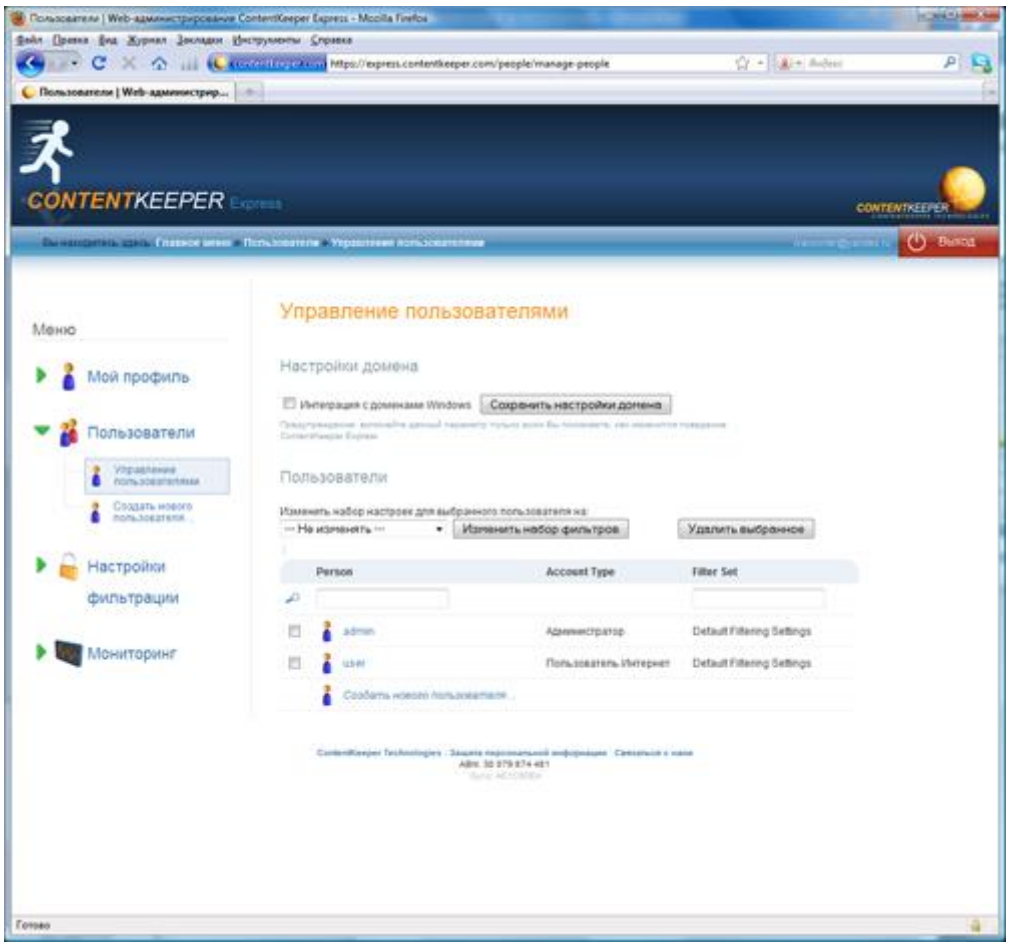


Рисунок 77. Раздел «Управление пользователями»

Раздел «Создать нового пользователя…» дублирует функции создания новой учетной записи из предыдущей вкладки. Смысл дублирования функциональности не понятен.

Вкладка «Настройки фильтрации» позволяет редактировать, удалять или создавать новые наборы фильтров. Производителем заданы четыре набора фильтров, сконфигурированных заранее (их конфигурация также может быть изменена пользователем):

- «Education Only» (работа только с образовательными ресурсами);
- «No Facebook Or MySpace» (блокирование доступа к социальным сетям);
- «Block All Access» (блокирование любого доступа в Интернет);
- «Default Filtering Settings» (настройка «по умолчанию»). Блокируются сайты с порнографией, азартными играми и сайты, связанные с наркотиками.

Рисунок 78. Вкладка «Настройки фильтрации»

Рассмотрим, какие настройки фильтрации мы можем задавать, на примере набора фильтров «Education Only».

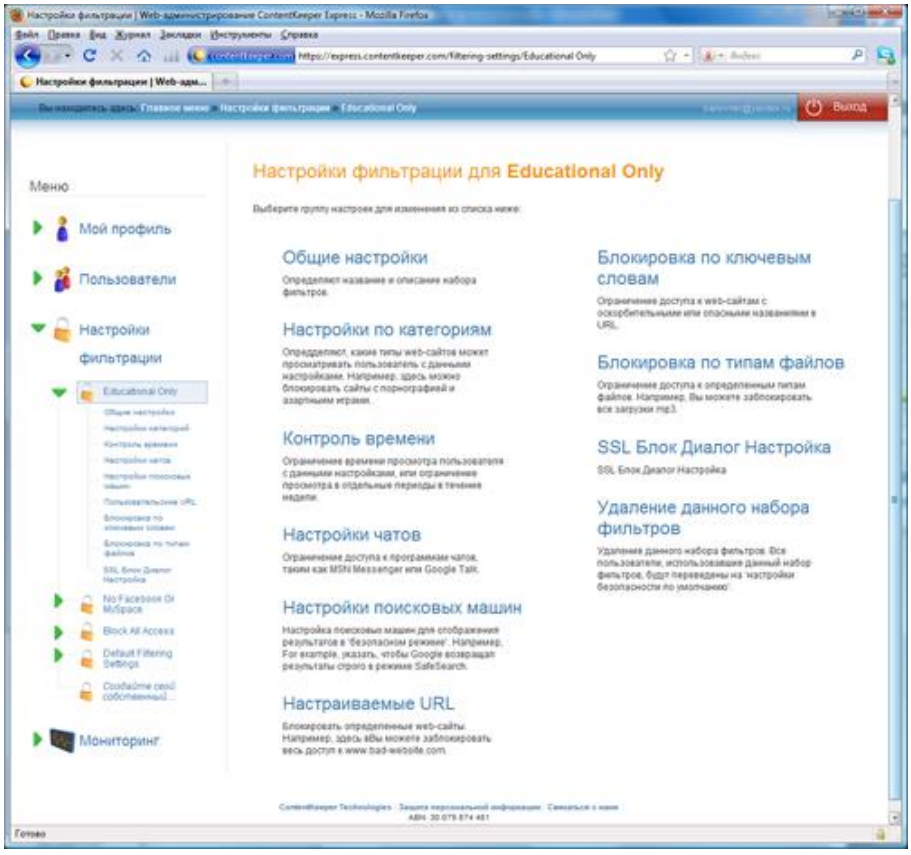


Рисунок 79. Настройки набора фильтров «Education Only»

В окне «Общие настройки» мы можем задать название и описание фильтра. Также в данном окне мы можем блокировать весь доступ к Интернету или включить использование доступа с фильтрацией при помощи соответствующего переключателя (рис. 80).

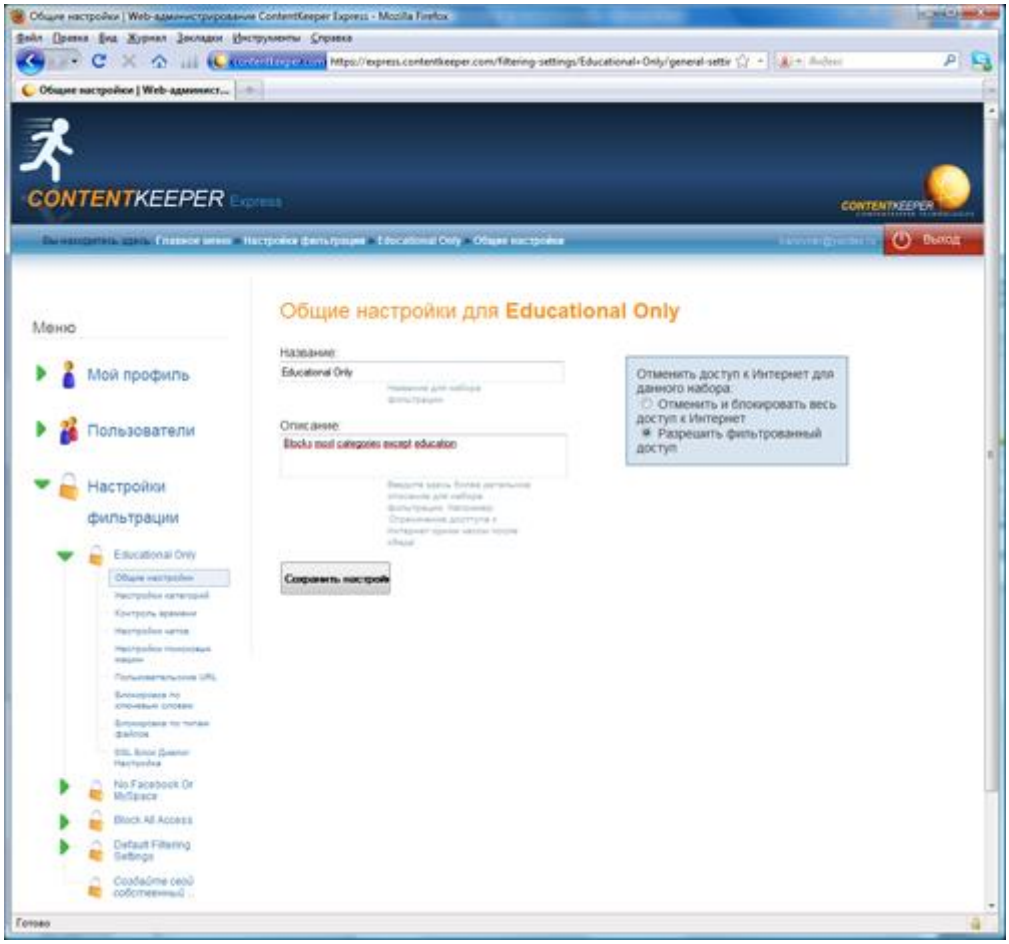


Рисунок 80. Общие настройки набора фильтров «Education Only»

В окне «Настройки категорий» Вы можете выбрать категории сайтов, которые хотим блокировать, а также указать действия для сайтов, не попавших в данные категории (разрешить показ или блокировать). Всего доступно 32 категории, позволяющие ограничить доступ к сайтам, которые могут отвлечь сотрудников от работы, нанести вред психике детей и подростков или привести к непосредственным угрозам безопасности компьютеру. Большинство категорий выбраны достаточно логично, однако некоторые из них вызывают удивление. Например, сложно представить, что блокирование сайтов с купальниками и женским бельем является такой большой проблемой, чтобы под нее выделять отдельную категорию. Название категории «Загрузка музыки» не правильно отражает логику фильтрации, на самом деле при включении этого фильтра фильтруется загрузка любого мультимедийного контента (аудио и видео файлов). Также мешает работе отсутствие сортировки категорий по какому-нибудь отдельному критерию, например, по типам угроз или просто по алфавиту.

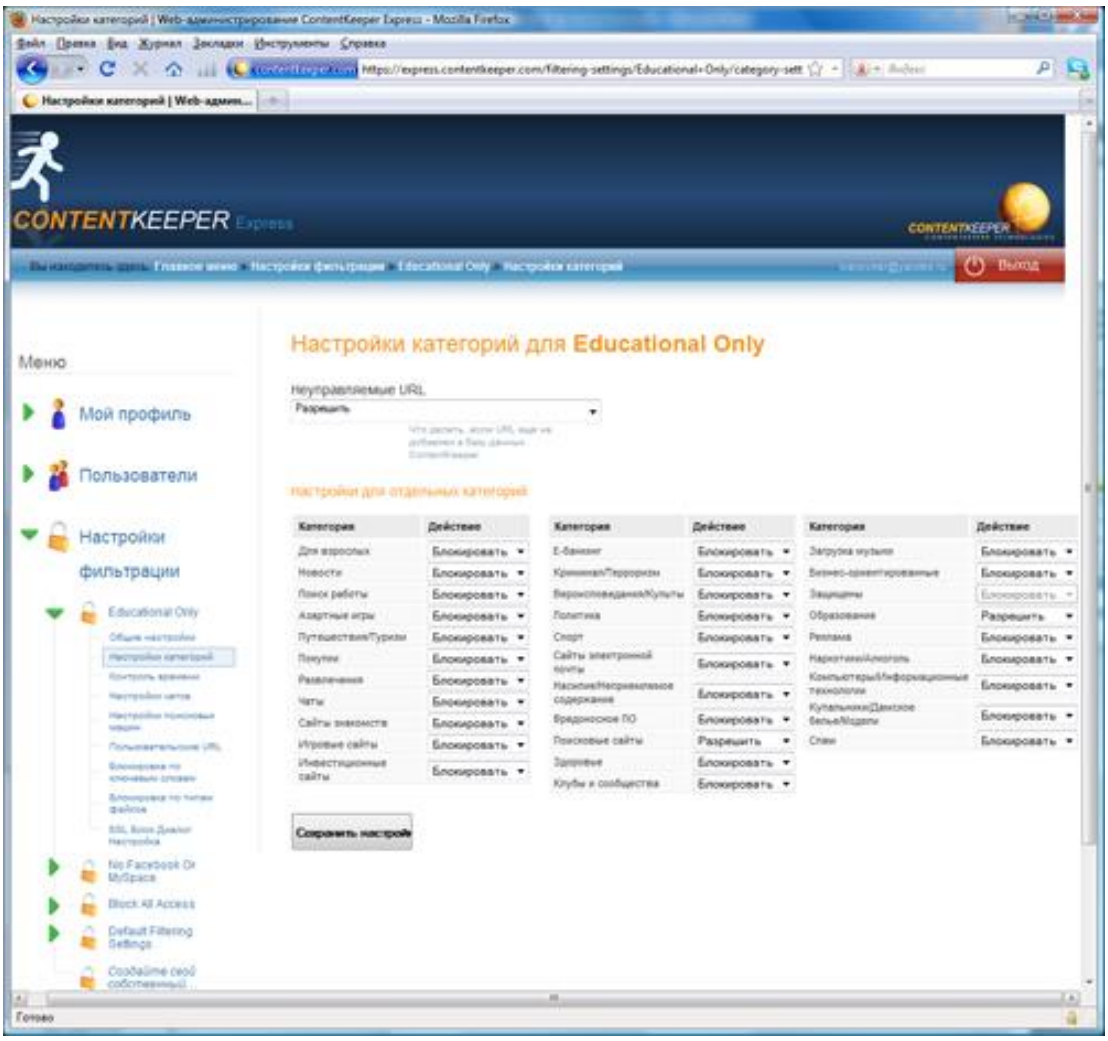


Рисунок 81. Настройки категорий для набора фильтров «Education Only»

В окне «Контроль времени» Вы можете задать день недели и временной интервал, в течение которого для пользователя блокируется доступ в сеть Интернет. Сутки разбиты на интервалы по 30 минут, что позволяет достаточно дифференцировано ограничивать доступ. Следует сказать, что временные метки сделаны неудобно, за основу взята 12-ти часовая система времени, при которой сутки делятся на два интервала – «до полудня» и «после полудня». Именно такая система применяется в Австралии, где и располагается компания ContentKeeper Technologies. Соответственно, необходимо внимательно следить, чтобы временной интервал «7.00-7.30», который мы задаем, относился именно к утру, а не к 19 часам вечера. И именно к утру понедельника, а не воскресенья, т.к. неделя в данной программе начинается с этого выходного дня. При локализации логичнее было бы использовать принятый в России 24-часовой формат времени.

В окне «Настройки чатов» мы можем выбрать режим работы для каждой из контролируемых программ для обмена мгновенными сообщениями – запретить, разрешить или разрешить с ведением отчета обо всех сообщениях. Список контролируемых программ достаточно небольшой и не включает в себя многие популярные в России программы (ICQ, Miranda, QIP).

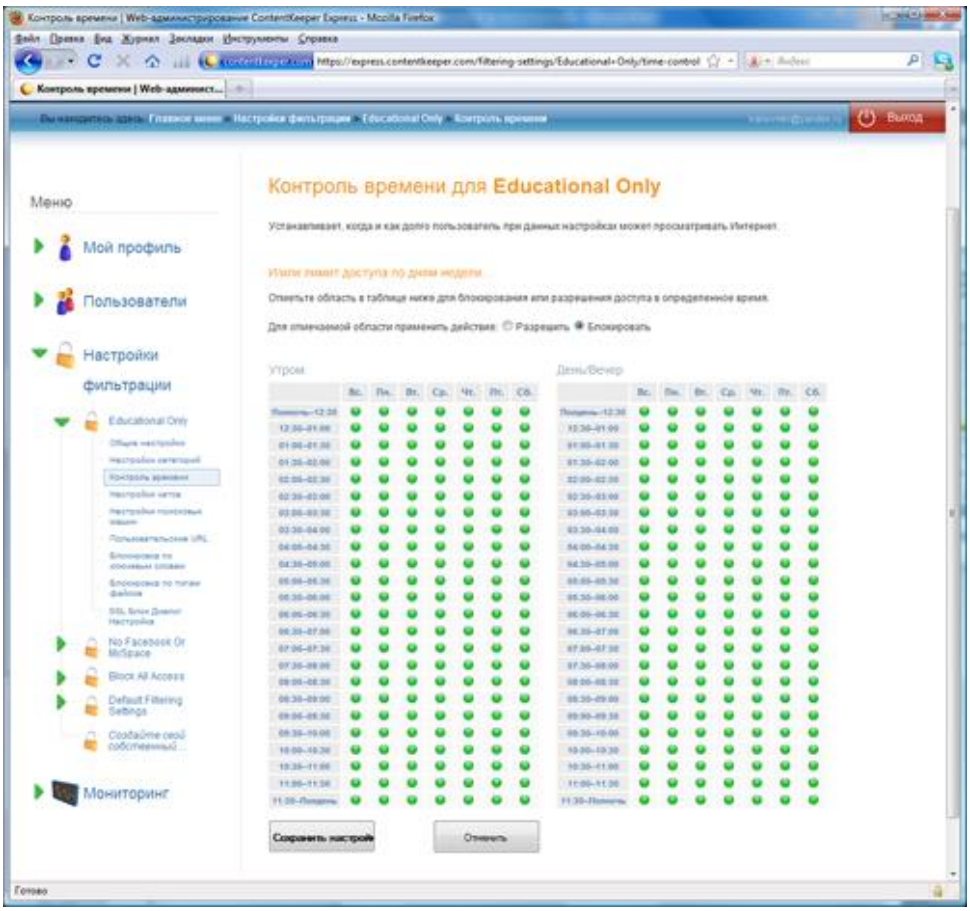


Рисунок 82. Контроль времени для набора фильтров «Education Only»

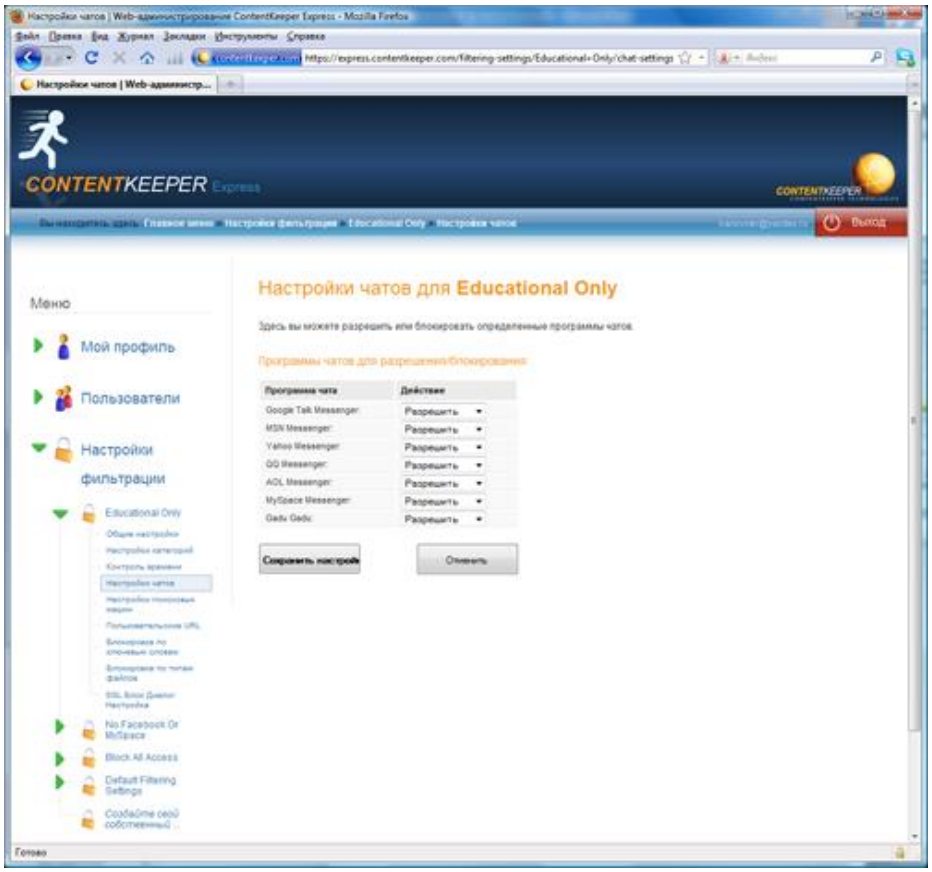


Рисунок 83. Настройки использования программ для обмена мгновенными сообщениями для набора фильтров «Education Only»

Окно «Настройки поисковых систем» позволяет выбрать поисковые системы, которые будут работать в режиме «Безопасного поиска». В этом режиме не отображаются результаты поиска по ключевым словам, которые относятся к заблокированным категориям. Список поисковых систем включает в себя Google, AltaVista, DogPile, Yahoo, Lycos, MSN/Live, а также поиск по сайту Youtube.com. Список поисковиков ограничен и не включает в себя такие популярные в России поисковые системы как Yandex.ru, Rambler.ru и Mail.ru.

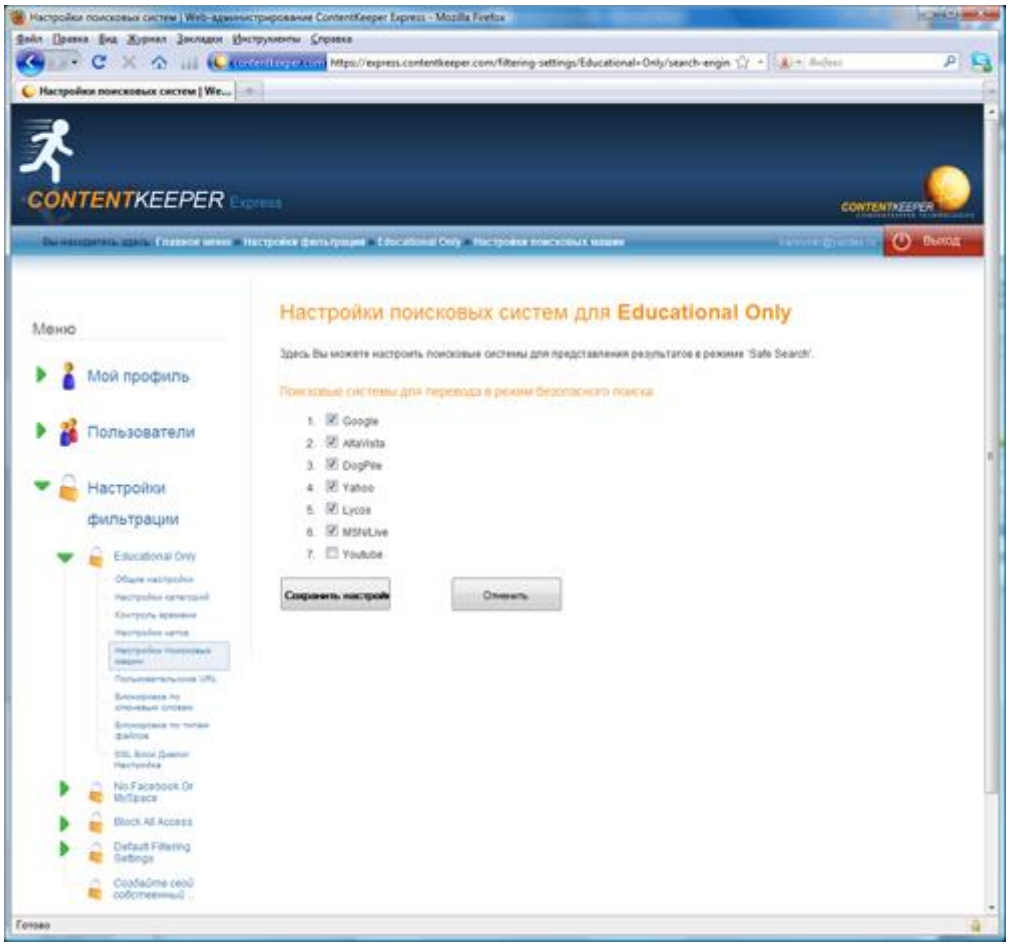


Рисунок 84. Настройки поисковых систем для набора фильтров «Education Only»

В окне «Редактировать пользовательские URL» Вы можете создать «белый» и «черный» список веб-сайтов. Для создания списка достаточно добавить набор URL-адресов с меткой «Заблокировать» или «Разрешить». Если же Вы хотите работать в строго ограниченной среде, когда доступ разрешен только к определённому кругу сайтов, то нужно установить флаг «Блокировать все web-сайты за исключением списка разрешенных».

В окне «Блокировка по ключевым словам» Вы можете включить или выключить блокировку сайтов, содержащих специально очерченный набор слов. Посмотреть ключевые слова мы не можем, программа только указывает, что задаются они на основе выбранных нами категорий сайтов для блокировки. Данная возможность выглядит странно, так как нам предлагают блокировать то, о чем у нас нет информации. Было бы логично в данном окне разрешить администратору задавать свои ключевые слова.

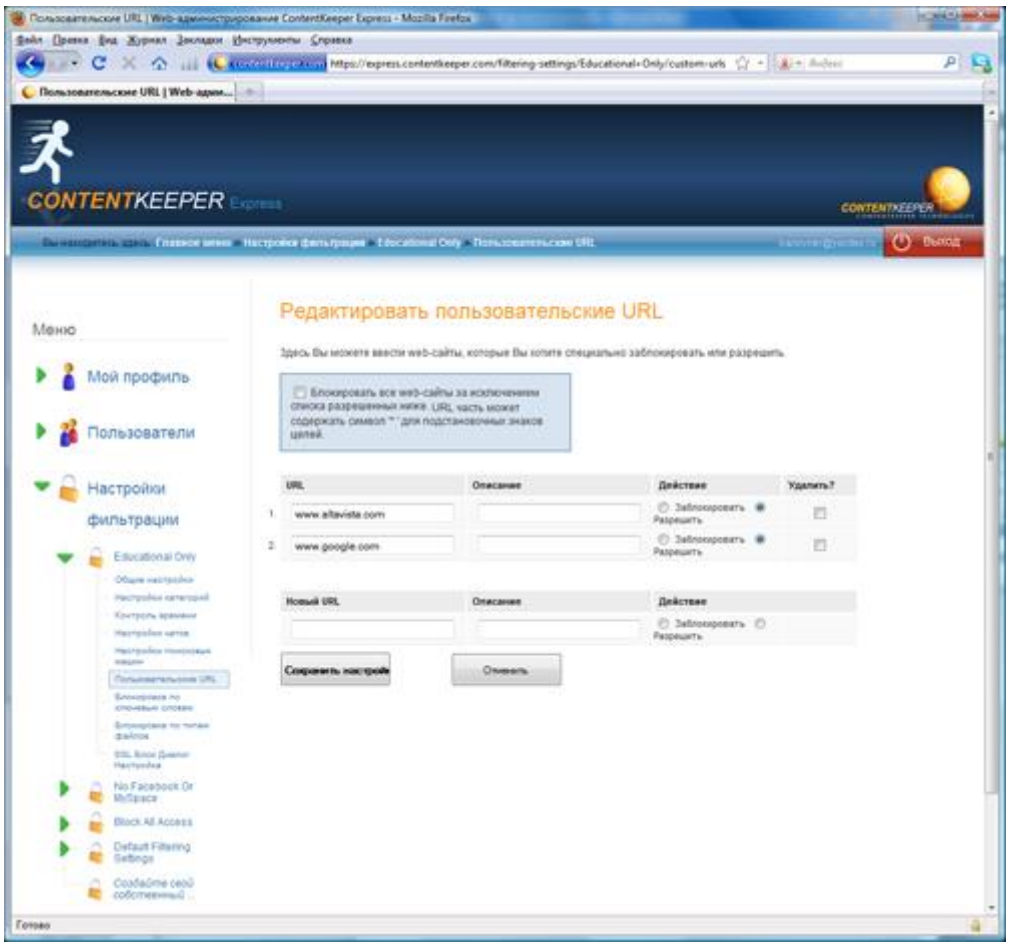


Рисунок 85. Формирование «белых» и «черных» списков URL

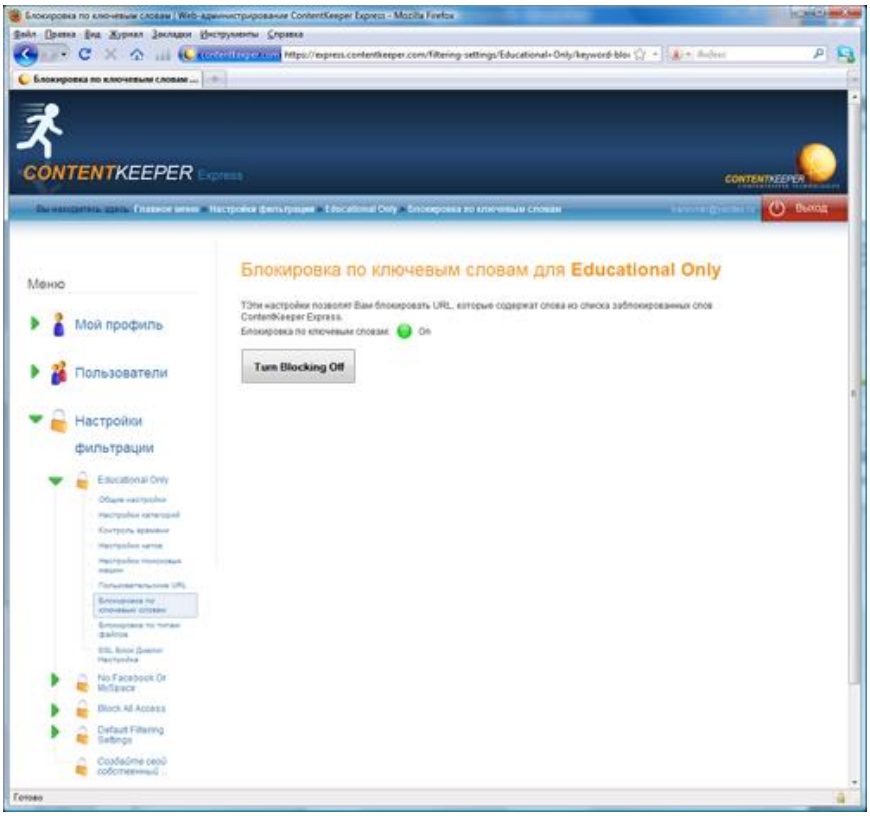


Рисунок 86. Окно «Блокировка по ключевым словам для набора фильтров «Education Only»

В окне «Настройки блокировки по типам файлов» Вы можете разрешить или заблокировать загрузку определенных типов файлов. Количество типов файлов достаточно большое, Вы можете заблокировать загрузку аудио и видео файлов, исполняемых файлов, инсталляторов, архивы и т.д. Для каждого из типов файлов мы можем выбрать конкретные расширения файлов, которые будут блокироваться.

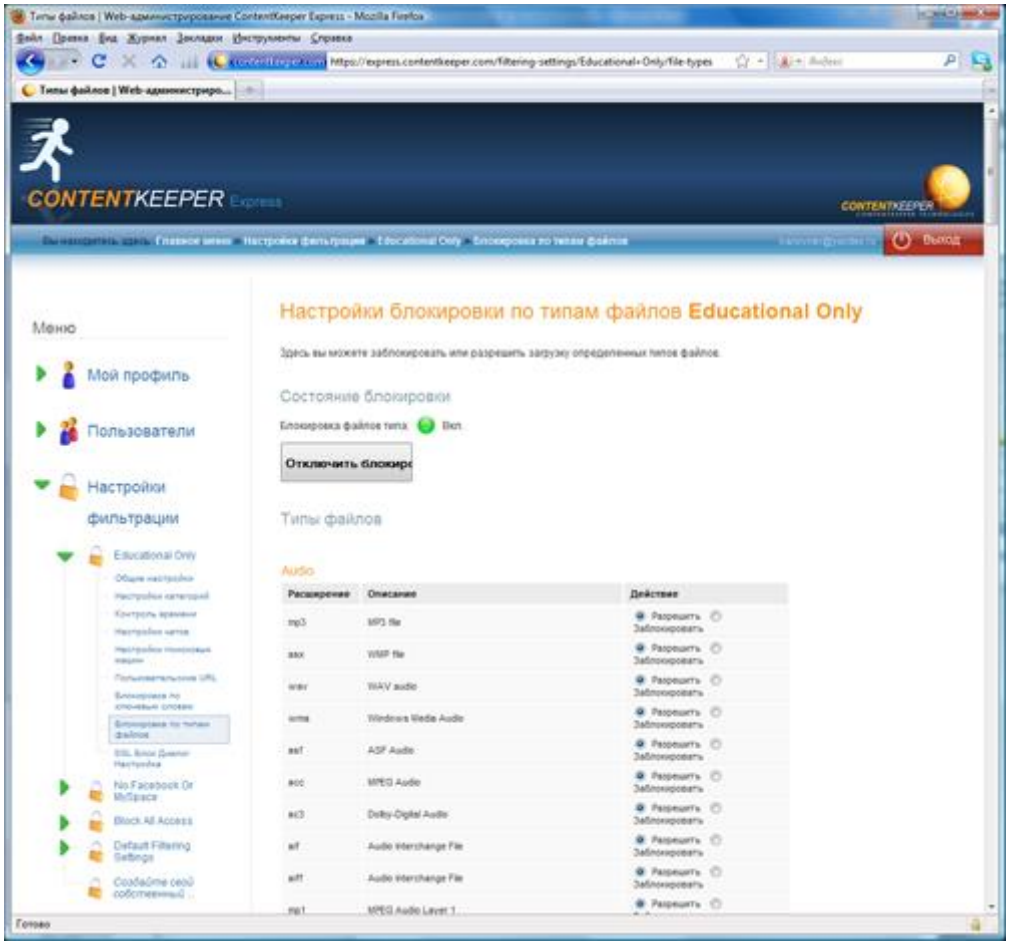


Рисунок 87. Окно «Настройки блокировки по типам файлов»

В окне «SSL Block Dialog Setting» Вы можете включить контроль и блокировку данных, передаваемых по протоколу SSL (Secure Sockets Layer, уровень защищённых сокетов). Замечанием к данному окну является отсутствие перевода заголовка окна и совершенно не адекватный перевод в тексте окна. Например, фраза «SSL Block Dialog Setting» переведена как «SSL Блок диалог Настройка».

Рассмотрев все настройки набора фильтров необходимо отметить, что для применения сделанных изменений в каждом окне нужно нажимать кнопку «Сохранить настройки».

При создании новых наборов фильтров Вам необходимо будет при помощи мастера последовательно настроить все описанные выше параметры.

Далее рассмотрим последнюю вкладку – «Мониторинг», предназначенную для настройки сбора статистики использования Интернета, а также формирования и просмотра отчетов. Вкладка содержит два раздела: «Отчеты» и «Контроль».

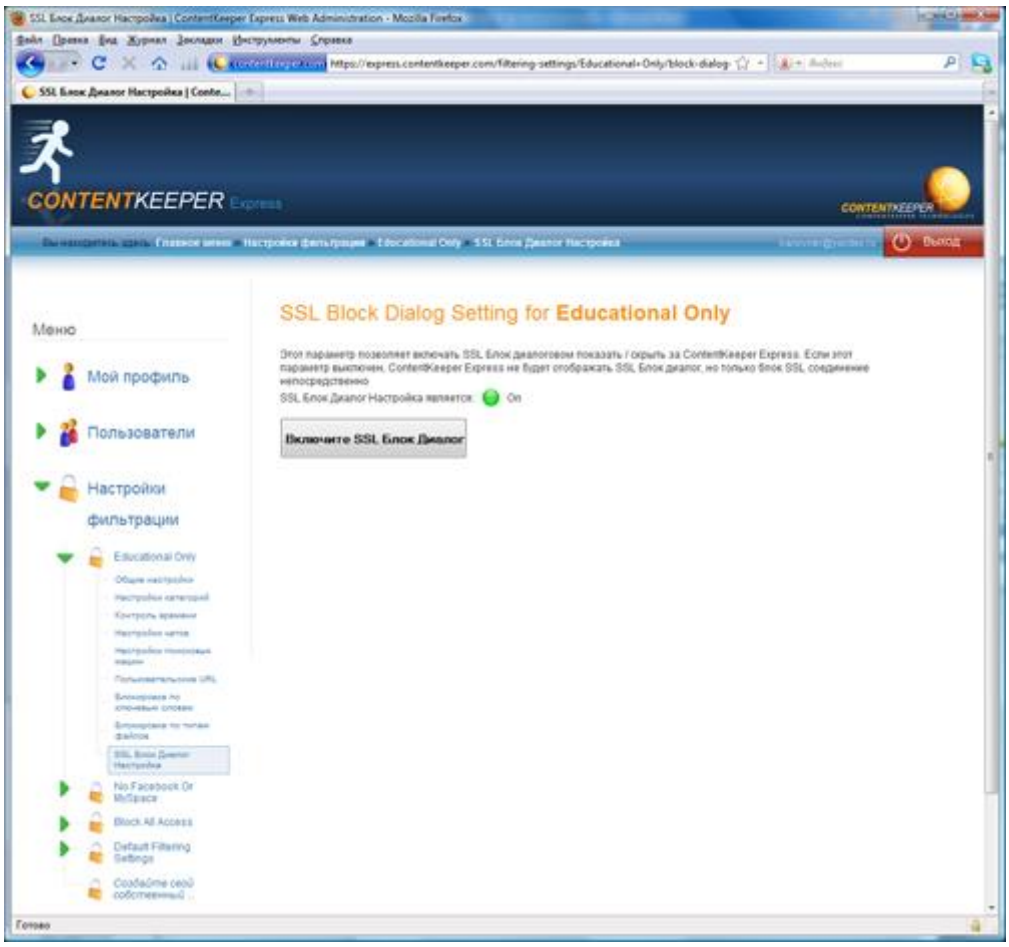


Рисунок 88. Окно «SSL Block Dialog Setting»

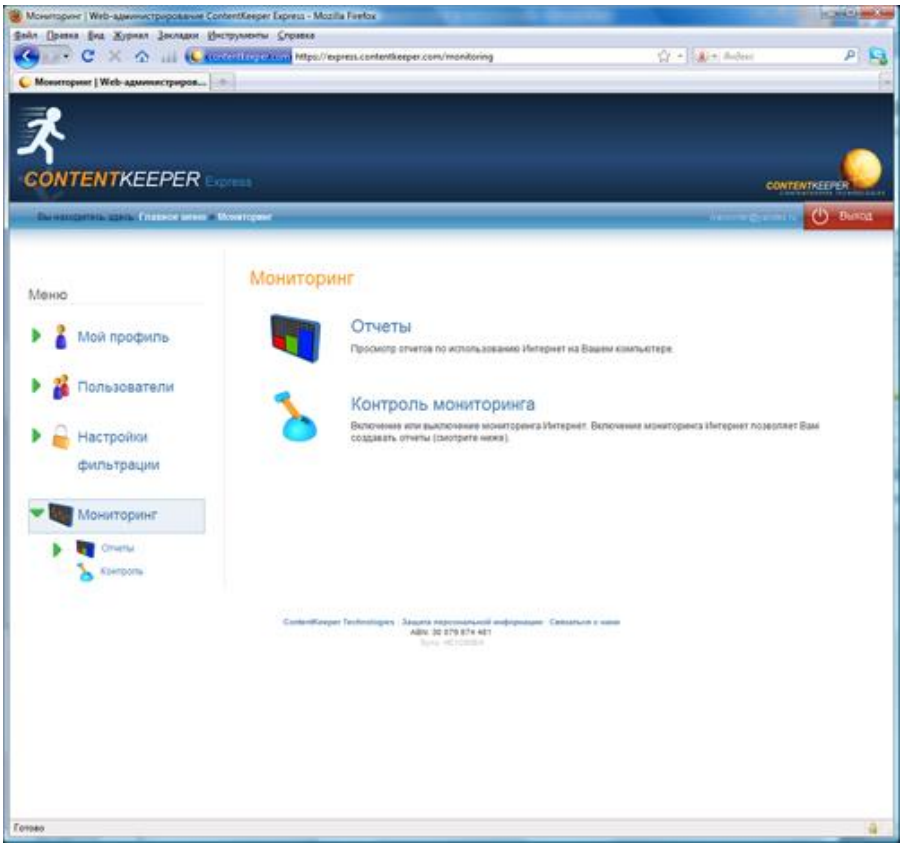


Рисунок 89. Вкладка «Мониторинг»

Раздел «Мониторинг» предоставляет два вида отчетов: «Просмотренные категории» и «Часто посещаемые Web-сайты».

В окне «Просмотренные категории» в виде круговой диаграммы отображается статистика посещений пользователем сайтов для каждой контролируемой категории. Вы можете выбрать пользователя, о котором будет выводиться информация, и указать интересующий временной интервал. Диаграмма отражает относительные значения, а таблица ниже – количество посещений сайтов из каждой категории (рис. 90). Инструмент достаточно нагляден и удобен.

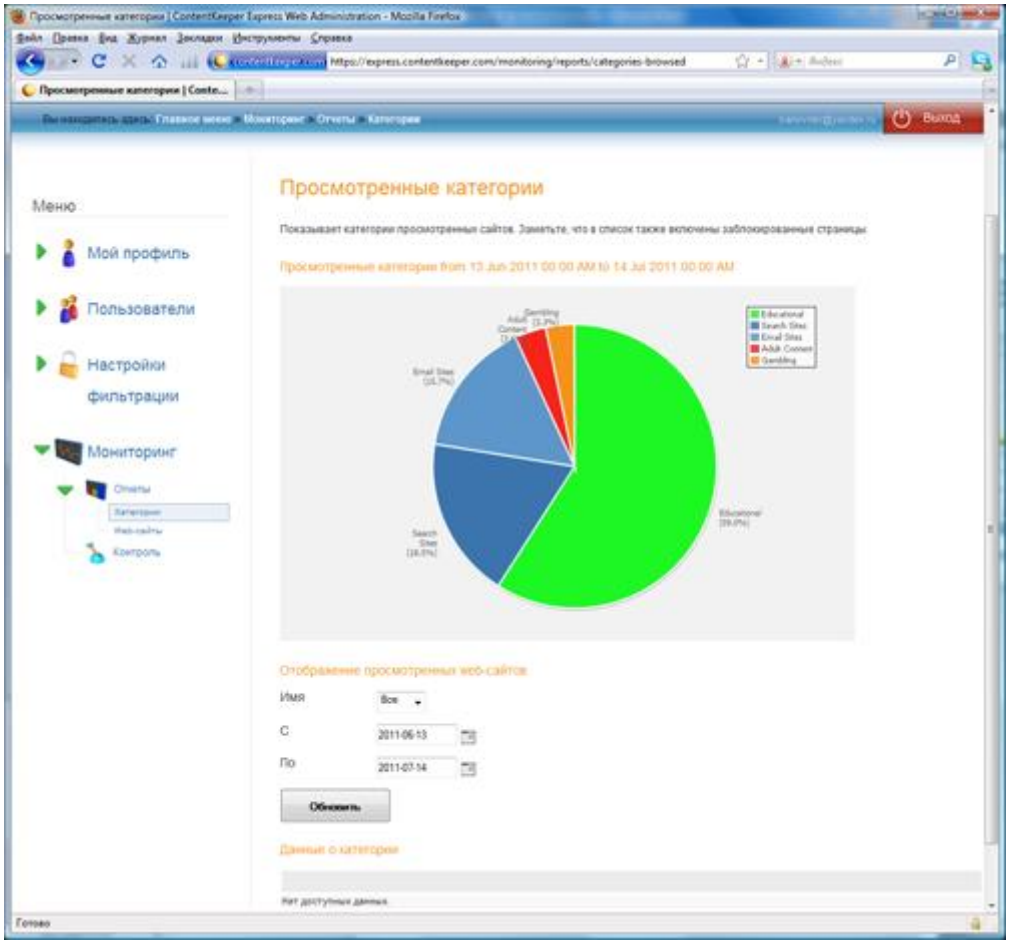


Рисунок 90. Окно «Просмотренные категории»

В окне «Часто посещаемые Web-сайты» отображаются 10 самых посещаемых сайтов. Как и в предыдущем окне, Вы можете выбрать имя пользователя, действия которого нас интересуют, и указать нужный временной интервал.

В разделе «Контроль» Вы можете включать и выключать мониторинг. При включении мониторинга Вам предлагают указать, на сколько минут его следует включить (от 5 до 30). Также в данном окне отображаются данные о последней зарегистрированной активности в Интернете (рис. 91).

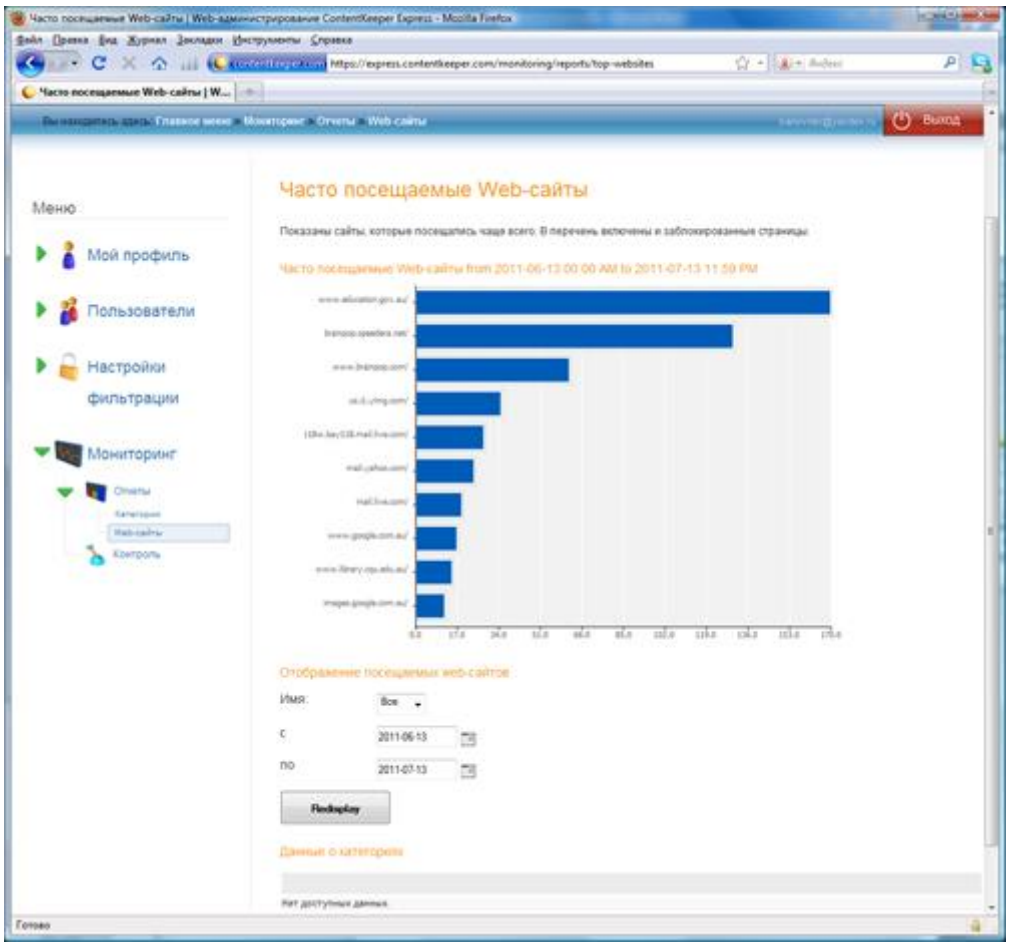


Рисунок 91. Окно «Часто посещаемые Web-сайты»

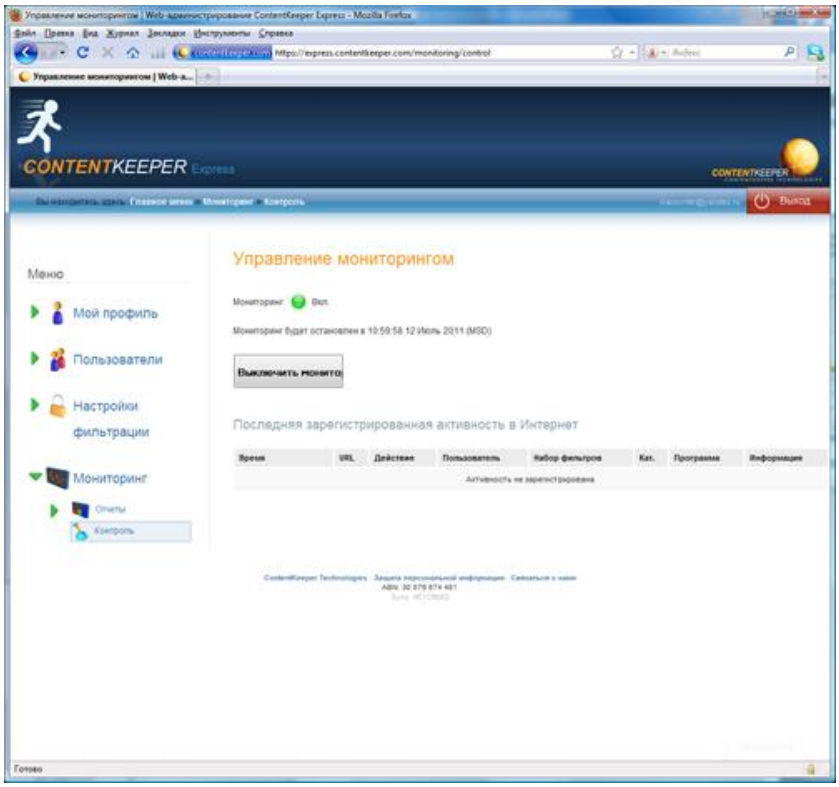


Рисунок 92. Окно «Управление мониторингом»

После настройки и применения администратором ограничений для каждого пользователя начинается работа ContentKeeper Express. Для пользователя работа программы практически не заметна и проявляется только в виде блокировки какого-нибудь ресурса.

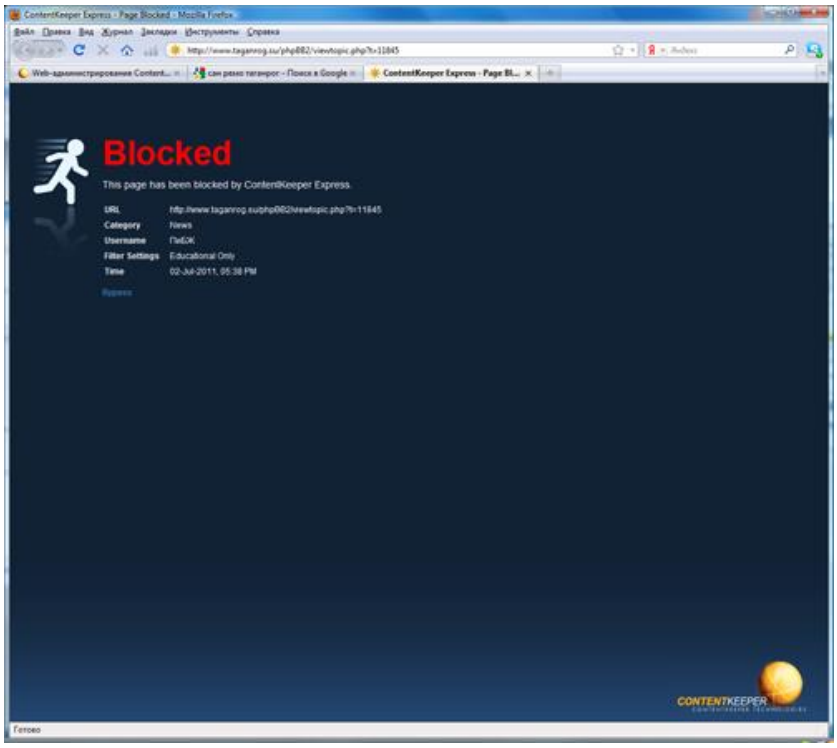


Рисунок 93. Окно с сообщением о блокировки сайта

Создав собственный фильтр с максимально жесткими настройками, мы протестировали, как ContentKeeper Express проводит блокировку сайтов. Результат нас удовлетворил – были заблокированы все заданные нами 50 сайтов в домене «.ru», которые попадали под указанные в настройках категории. Можно констатировать, что программа выполняет свою задачу.

6.4.Выводы

Закончив описание ContentKeeper Express, мы можем перейти к подведению итогов. В целом программа вызвала неоднозначные впечатления. С одной стороны, используются мощные технологии для категоризации сайтов, пользовательский интерфейс достаточно прост и понятен, с другой стороны, локализация программы оставляет желать лучшего.

Также следует отметить, что при покупке или продлении лицензии пользователь должен указать только адрес электронной почты и имя пользователя. Это позволяет использовать программу, не раскрывая своих личных данных.

Плюсы

1. Использование «облачных» технологий в совокупности с мощностями ContentKeeper Technologies позволяет с минимальными затратами на приобретение и сопровождение получить систему фильтрации корпоративного класса.
2. Результаты работы. Было проведено краткое тестирование – открывались первые 20 адресов, выданных Google.ru на ключевые слова из заблокированных категорий (секс, спорт, новости, поиск работы и т.д.). ContentKeeper Express заблокировал все адреса из всех категорий, которые указывались как «запрещенные». Пользовательский интерфейс сделан в минималистском стиле, работа в нем не вызывает затруднений. Для работы с программой практически не требуется знаний в области информационных технологий.
3. Отчеты. Представление информации выполнено просто и наглядно.

Минусы

1. Проблемы с локализацией. Отсутствует контроль популярных в России поисковых систем и программ мгновенного обмена сообщениями (ICQ, Miranda, QIP), временные метки при блокировании доступа по расписанию сделаны на основе 12-ти часового формата времени (не учтён 24-часовой рабочий формат), многие надписи не локализованы или локализованы некорректно.
2. Нарушение целостности «ментальной» модели программы у пользователя. К этому приводит дублирование функций и нелогичная группировка разделов. Например, создание новой учетной записи возможно и в разделе «Управление пользователями», и на вкладке «Создать нового пользователя». В два раздела вынесены функции скачивания двух разных версий программы, хотя их логично включить в один раздел. Присутствуют разделы, в которых можно включить функции, параметры которых скрыты (настройка фильтрации по ключевым словам). Мешает работе отсутствие сортировки категорий для блокировки по какому-либо критерию.

7. Net Police Pro

Программа Netpolice Pro представляет собой эффективный и надежный способ анализа всей информации, поступающей через сеть Интернет. Пользователь программы с помощью комплекса гибких настроек может определить уровень доступности информации. Установленная на компьютер пользователя, программа Netpolice Pro в соответствии с настройками блокирует ресурсы и слова, относящиеся к категории запрещенных, разрешая пользователю просматривать лишь нужную информацию.

Большим плюсом этой программы является функция обеспечения безопасного серфинга в сети Интернет для локальной сети. Эта особенность делает возможным использование фильтра как в различных организациях, школах, так и при домашнем использовании.

Программа Netpolice Pro использует регулярно обновляемую базу ресурсов. Фильтрация применяется не только к категории сайта, но также проверяется его содержимое в соответствии с настройками.

У программы довольно простой и интуитивно понятный интерфейс, навыки работы с ней приобретаются быстро.

В интерфейсе программы присутствует русский язык. Важным преимуществом программы является и то, что кроме ярко выраженных негативных тематик можно производить блокировку конкретных сайтов. Предлагается также ввести «черные» и «белые» списки.

Программа устанавливается непосредственно на компьютер пользователя и в соответствии с выбранными настройками блокирует сайты и слова, относящиеся к запрещённым категориям. Количество категорий фильтрации, а их в программе NetPolice Pro более 70, обеспечивает эффективный доступ в сеть Интернет, разрешая просмотр только необходимой и полезной информации. Для удобства пользователей некоторые категории объединены в группы, что упрощает процесс настройки программы.

После запуска программы появляется регистрационная форма. Вначале необходимо установить парольную защиту на доступ к настройкам программы. Рекомендуем к этому пункту отнестись внимательно и не устанавливать легкие ключевые слова, так как современные дети весьма «продвинуты» в компьютерном плане и могут попытаться обойти защиту. На указанные в поле e-mail («Электронный адрес») будут отправляться события, сообщающие об изменении настроек программы. Но и это еще не все. Для редактирования важных параметров продукта необходимо авторизоваться. Программа фиксирует каждое посещение панели управления. При неправильном вводе пароля или удалении программы система рассылки уведомлений Netpolice Pro отправляет на почтовый адрес пользователя сообщения с указанием всех попыток внести изменения в настройки фильтра.

После заполнения анкеты можно приступить к рассмотрению основных возможностей программы. Знакомство следует начать с главного окна приложения. Для настройки фильтра не требуются какие-то специальные знания, так как все управление программой осуществляется с помощью инструментов, распределенных по группам – вкладкам (рис. 94.). Давайте подробнее рассмотрим каждую.

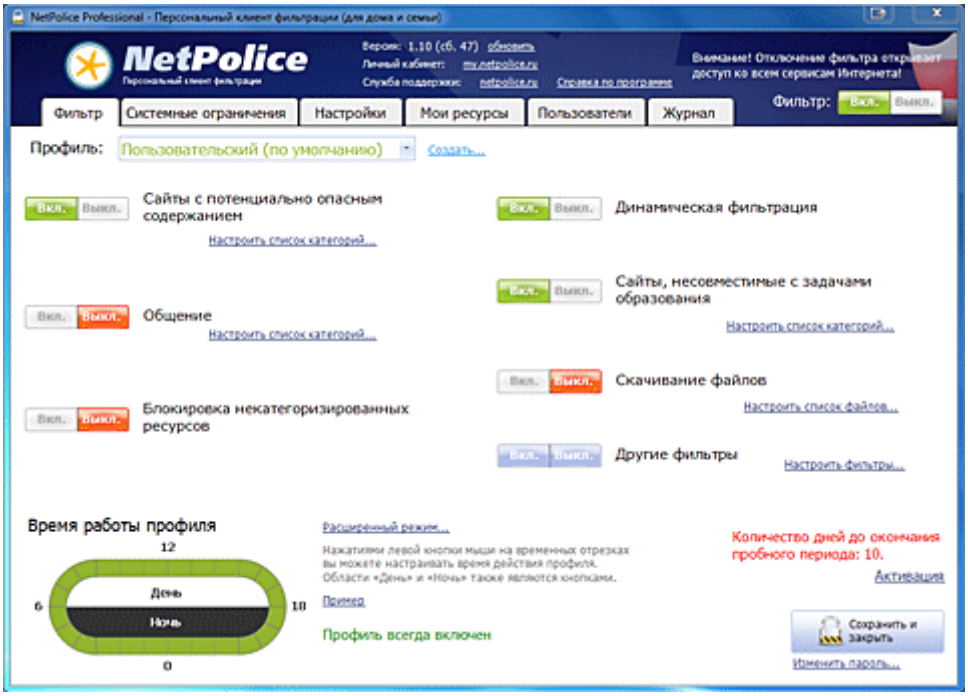


Рисунок 94. Выбор профиля для ограничения доступа к нежелательным сайтам

Вкладка «Фильтр» содержит несколько профилей для ограничения доступа к нежелательным сайтам. Перечень готовых шаблонов включает несколько уровней: «Все разрешено», «Все запрещено», «Для общения», «Для детей», «Пользовательский». В начале списка находится предустановка, разрешающая доступ ко всем интернет-ресурсам. Ниже располагается профиль, который, наоборот, все запрещает. Остальные же заготовки настроены иначе, в соответствие с поставленными задачами.

Другими словами, у разработчика есть специальная база, куда вносятся все сайты – «хорошие» и «плохие». Они оцениваются по содержанию и получают рейтинг доверительности. В момент перехода пользователя по ссылке программа обращается к этой базе, анализирует оценку этого сайта и сравнивает ее с настройками программы – фильтрами. Например, установка профиля «Для детей» откроет доступ только к тем ресурсам, которые несут образовательную функцию. Примечательно, что существует возможность создания собственного профиля. И, что немаловажно, некоторые разделы фильтров предоставляют возможность более тщательно подойти к редактированию категорий.

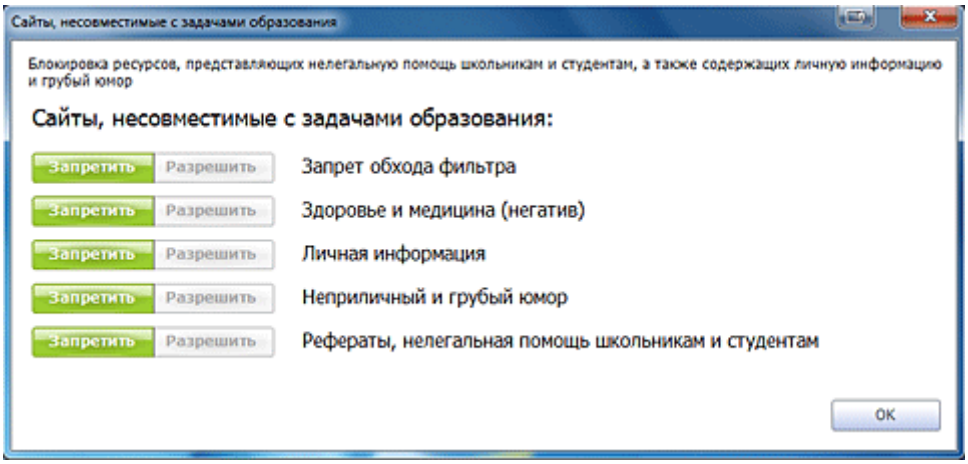


Рисунок 95. Редактирование категории «Сайты, несовместимые с задачами образования»

Раздел «Ограничение на скачивание файлов» уменьшит нагрузку на входящий трафик, а также убережет Ваш компьютер от возможного заражения вирусами. Не секрет, что чаще всего вредоносные программы можно «подцепить», загружая файлы с развлекательных порталов и сайтов, предоставляющих «халявное» (**нелицензионное**) ПО. Нередки случаи, когда ничего не подозревающий ребенок может извлечь из архива не только искомый документ, но и вирус, который причинит вред компьютеру, незащищенному антивирусным средством.

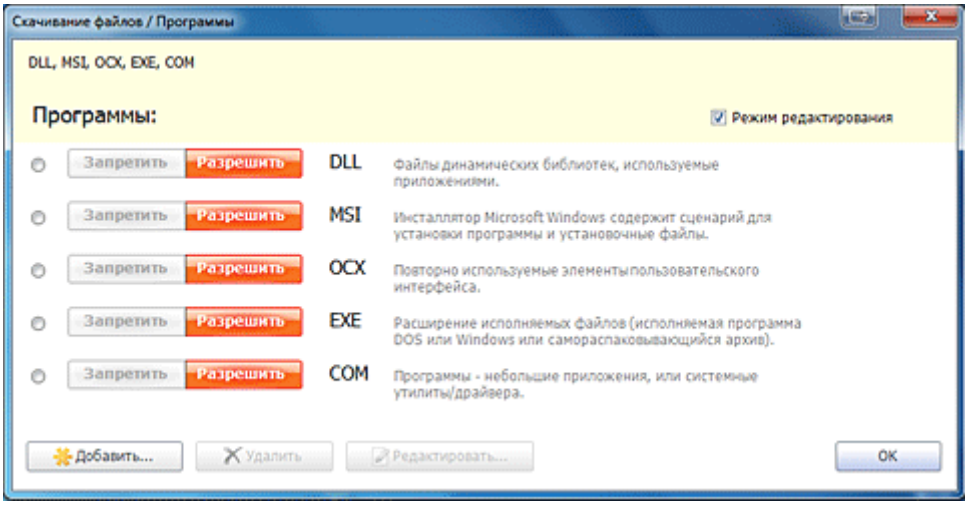


Рисунок 96. Настройка раздела «Ограничение на скачивание файлов»

Функция «Время работы профиля» позволяет настраивать продолжительность активности фильтра. По умолчанию профиль всегда включен. Для указания интервала времени необходимо перейти в расширенный режим настройки. Установить время фильтрации можно двумя способами. Первый вариант предполагает, что всю неделю фильтр будет работать одинаково. Второй способ подразумевает формирование отдельного расписания на каждый день недели. В обоих случаях активация профиля осуществляется выбором ячеек в таблицах расписаний. Отмеченные ячейки окрашиваются в зеленый цвет (рис. 97).

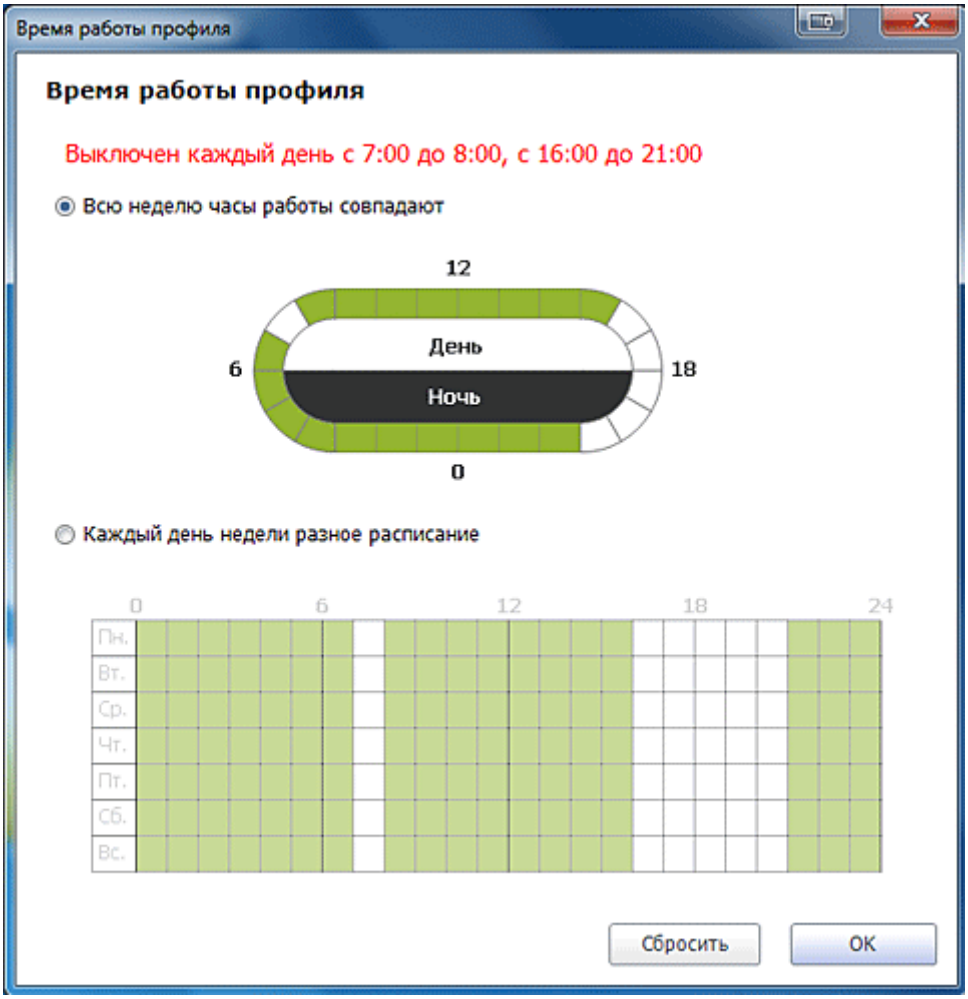


Рисунок 97. Функция «Время работы профиля»

Используя возможности функций, расположенных на вкладке «Системные ограничения», можно предотвратить изменения системных настроек. Активировать нужные опции очень просто. Для этого потребуется лишь перевести нужные пункты с описанием блокирующей команды во включенное состояние.

С помощью функции «Запрещенные программы» можно блокировать запуск приложений. Особенно полезен этот инструмент для родителей, чьи дети неудержимо играют в компьютерные игры или общаются в сети Интернет. Если у Вас есть программы, доступ к которым необходимо прикрыть, следует добавить в список заблокированных приложений файл запуска, имеющего расширение .exe.

Если в семье компьютер один и им пользуются как взрослые, так и дети, то может возникнуть необходимость в защите личных данных. Функция «Защита папок» не позволит любопытным детям просмотреть файлы, предназначенные для взрослых. Только пользоваться этой функцией очень неудобно. Для защиты папки ее необходимо добавить в окно программы «Системные ограничения», затем внести в список защищенных каталогов и в завершение сохранить настройки. При попытке открыть такую директорию мы получим «вежливый отказ». Разблокировка каталога происходит по такому же принципу, как и блокировка. Для этого необходимо удалить из списка папку, которую вы хотите просмотреть. Однако было бы удобно организовать доступ к защищенному каталогу через парольную форму.

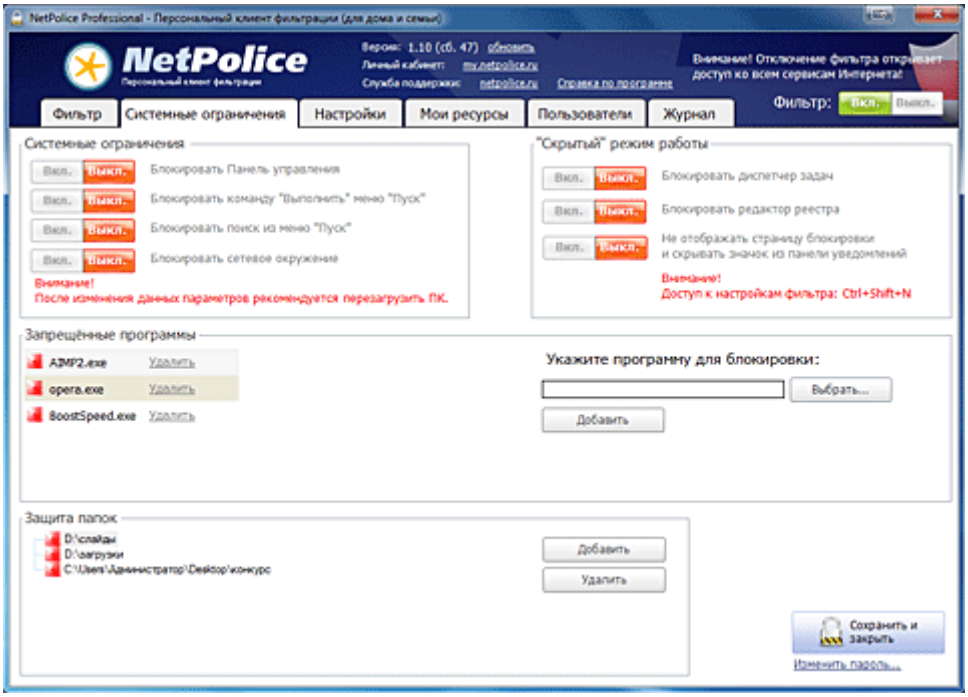


Рисунок 98. Вкладка «Системные ограничения»

Следующая вкладка, «Настройки», содержит много полезных возможностей. Приостанавливая работу фильтра на некоторый промежуток времени, функция «Будильник» по истечении указанного значения вернет фильтр в прежнее состояние. Например, если отключить работу фильтра на полчаса, то в области панели уведомлений на рабочем столе появится сообщение: «Через 30 минут фильтр будет включен». К тому же программа еще раз проинформирует пользователя о включение фильтра за 5 минут. Среди прочих разделов привлекает внимание пункт «Страница блокировки Интернета». Упомянутая опция позволяет указать адрес интернет-ресурса, на который «перебросит» пользователя при попытке перейти на запрещенный сайт. Примечательно, что здесь присутствует готовая страница блокировки, снабженная предупреждением и безопасным поисковиком.

Несмотря на то, что база ресурсов программы Netpolice Pro регулярно обновляется, существует вероятность, что система не успеет отследить рождение новых сайтов с непристойным содержанием. Поэтому на следующей странице настроек «Мои ресурсы» пользователю предлагается ручным способом редактировать каталог «белых» и «черных» сайтов. Количество веб-проектов для добавления в собственные списки фильтрации неограниченно.

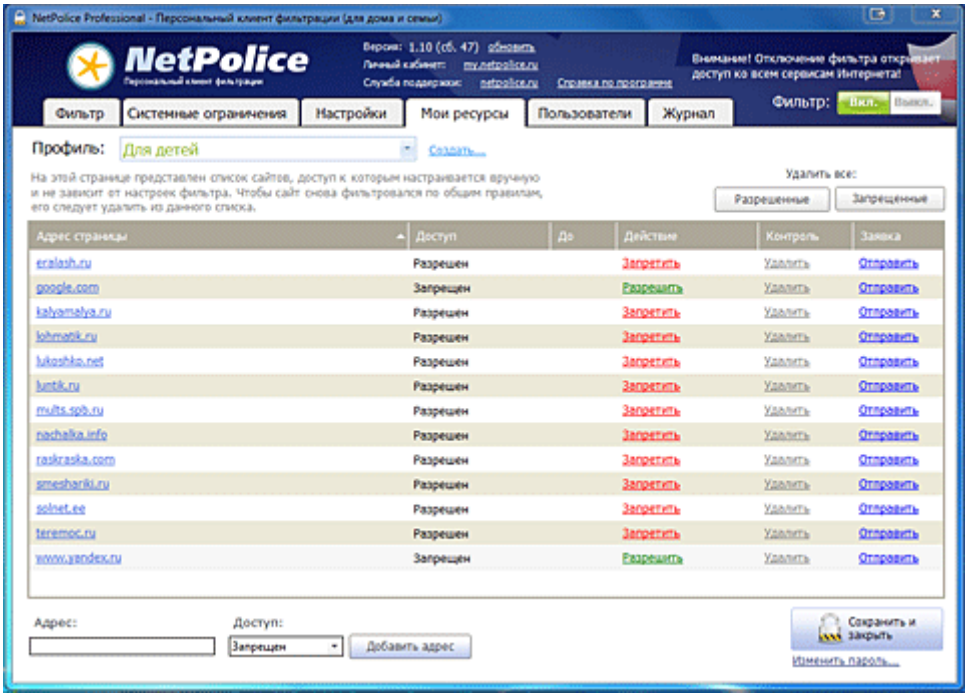


Рисунок 99. Редактирование каталога «белых» и «черных» сайтов

На следующей вкладке, которая называется «Пользователи», можно управлять учетными записями. Ее возможности применяются в том случае, если необходимо отдельным пользователям присвоить персональные уровни доступа в сеть Интернет (профиль фильтрации). Если учетная запись не относится ни к одному из профилей, то к ней применяется предустановка, имеющая статус «по умолчанию».

На последней вкладке, «Журнал», можно просмотреть статистику посещения веб-сайтов. Благодаря этому администратор Netpolice Pro будет знать адреса сайтов, которые открывали пользователи Интернета, а также объем входящего и исходящего интернет-трафика. Оценив сайт и удостоверившись в его полезности, можно здесь же присвоить ему статус «Разрешить». Сведения о посещении веб-ресурсов можно отобразить за разные периоды: за сегодняшний или вчерашний день, за текущую или прошедшую неделю, текущий или прошедший месяц (рис. 100).

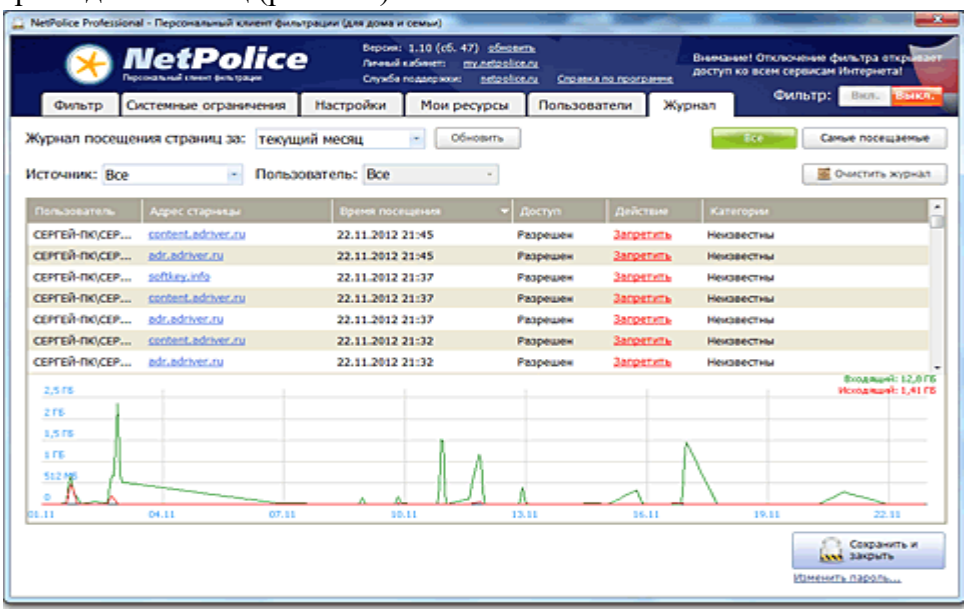


Рисунок 100. Статистика посещений веб-сайтов

Стоимость составляет 490 рублей на компьютер в год. В итоге на 100 компьютеров конечная стоимость составит 49 000 рублей в год.

Список используемых источников

1. **http://www.anti-malware.ru –независимый информационно-аналитический центр**
2. **http://habrahabr.ru/sandbox/79659/ - контентная фильтрация в образовательных организациях**
3. **http://www.entensys.com/ru - Entensys: Интернет - безопасность и фильтрация контента**
4. **http://www.kindergate.ru/ru - Родительский контроль- безопасный интернет и контроль доступа**
5. **http://www.remparo.ru – эффективная система контентной фильтрации**