УДК 004

Организация безопасного выхода в интернет с помощью программного обеспечения «Трафик инспектор» на примере Линейного отдела МВД России г. Находка

Пасюков Александр Андреевич
Приамурский государственный университет имени Шолом-Алейхема
студент

Баженов Руслан Иванович
Приамурский государственный университет имени Шолом-Алейхема
Кандидат педагогических наук, доцент, зав. кафедрой информационных систем, математики и методик обучения

Аннотация
Данная статья описывает настройку межсетевого экрана для полного контроля трафика и безопасного выхода в сеть интернет по проводной и беспроводной линии связи. В статье описана полная настройка продукта от начала установки до его использования. Для выполнения данной задачи используется компьютер на операционной системе Windows Server 2008 с программным обеспечением Трафик инспектор на примере организации работы в Линейном отделе МВД России г. Находка.
Ключевые слова: Сервер, межсетевой экран, IP-адрес, маршрутизатор, Proxy-сервер.

Safe exit organization on the Internet with the help of the software «Traffic Inspector» on the example of the Line of the Interior Ministry Russia Nakhodka

Pasyukov Alexandr Andreevich
Sholom-Aleichem Priamursky State University
Student

Bazhenov Ruslan Ivanovich
Sholom-Aleichem Priamursky State University
Candidate of pedagogical sciences, associate professor, Head of the Department of Information Systems, Mathematics and teaching methods

Abstract
This article describes the firewall settings for a complete traffic control and secure access to the Internet over a wired and wireless network link. The article describes a complete product configuration by starting the installation prior to use. To perform this task using a computer running Windows Server 2008 operating

system software Traffic Inspector on the example of the organization of work in the department of the Russian Interior Ministry Linear Nakhodka.
Keywords: server, firewall, IP-address of the router, Proxy-server.

В наше время крупным организациям невозможно обойтись без современных технологий, в том числе без доступа к сетям интернет. Во избежание многочисленных межсетевых атак, в том числе спама, требуется обеспечить безопасный выход в интернет и полный контроль трафика. Для этих целей используются межсетевые экраны, которые являются основой обеспечения безопасности информационной сети. Благодаря правильному применению межсетевых экранов достигается достаточно высокий уровень безопасности межсетевых взаимодействий. Главные задачи межсетевых экранов - это проверка входящего и исходящего трафика на безопасность, обеспечение защиты данных о внутренней структуре сети, а также поддержка общих правил безопасности для пользователей интернетом.

В Линейном отделе МВД России г. Находка была поставлена задача организовать контроль и безопасный выход в интернет всех сотрудников организации, а также осуществить блокировку выхода во все соцсети, блокировать спам, рекламу, онлайн-игры, торренты и развлекательные сайты.

Исследованиями в области сетевого администрирования занимались многие российские и зарубежные исследователи. А.Е.Боршевников [1] рассмотрел угрозы сетевых атак и методы борьбы с ними. М.А.Кузнецов и И.А.Степаненко [2] рассмотрели систему удаленного проектирования. Описала технологию межсетевого проектирования Е.А.Васильева [3]. Р.Марков [4] показал шаги настройки сервера для общего доступа в интернет. Запись дистрибутива и настройке сервера m0n0wall исследовал С. Яремчук [5]. Г.А.Воскресенский и А.М. Чаплыгин [6] рассмотрели основные способы защиты сетевых карт от внешних атак. M.M.Eissa и др. [7] представили метод усилении защиты беспроводной сети WI-FI. T.Mekhaznia и A.Zidani [8] произвели детальный анализ безопасности сети WI-FI. Рассмотрели способы защиты информации корпоративных сетей Интернет А.Турский и С. Панов [9]

Для решения поставленной задачи было выбрано программное обеспечение Трафик инспектор. Трафик инспектор — универсальный шлюз безопасности, разрабатываемый российской компанией «Смарт-Софт». Основные задачи программы — организация доступа в Интернет, надежная сетевая защита, отчеты по использованию ресурсов сети Интернет, фильтрация контента, маршрутизация, биллинг, ограничение скоростей. Нужно подметить, что трафик инспектор сам по себе не раздает WI-FI, он раздает лишь IP адреса, и каждый системный администратор сам уже решает, подключить ПК на прямую, через маршрутизатор, либо организовать беспроводную сеть с помощью дополнительного оборудования.

Для начала требуется скачать дистрибутив с официального сайта программного обеспечения http://www.smart-soft.ru. Пробная версия работает

30 дней, срока хватит для тестирования продукта и ее активации. Пробная версия полностью функциональна.

В отличие от многих конкурентов, Трафик инспектор не требует выделенного сервера, а устанавливается на любую новую версию windows. В нашем случае программное обеспечение установлено на Windows Server 2008 R2.

Перед тем как перейти к настройке программы требуется настроить сетевые интерфейсы. Так как отсутствует «белый» IP адрес и получение IP адреса для внешнего интерфейса идет через маршрутизатор, получаем адрес 192.168.1.1. Требуется прописать этот адрес в основном шлюзе, а также присвоить внешнему интерфейсу IP адрес подсети 192.168.1.x. Внешний интерфейс - это интерфейс через который подключен сервер к интернету. В нашем случае прописываем адрес 192.168.1.2.

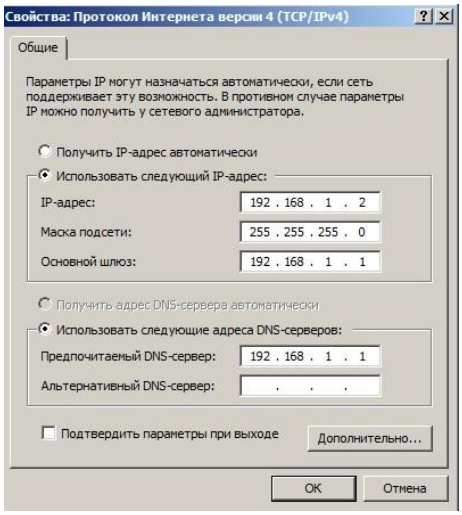

Рисунок 1 – Настройка внешнего интерфейса

Далее требуется произвести настройку внутреннего интерфейса. Внутренний интерфейс – интерфейс, через который подключены пользователи. Для этого требуется прописать IP адрес другой подсети, т.е. 192.168.x.x, в нашем случае 192.168.2.1.

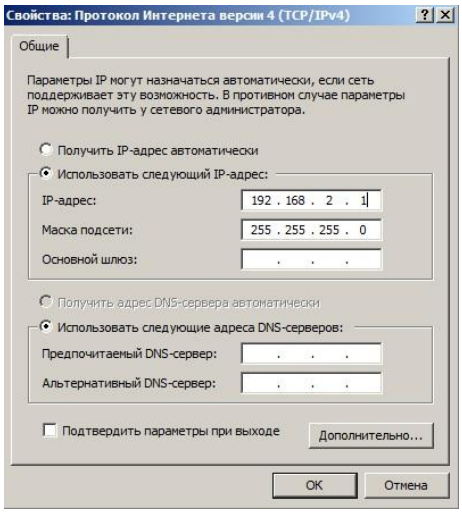

Рисунок 2 – Настройка внутреннего интерфейса

После настройки интерфейсов, переходим к настройке самого программного обеспечения. Так как работа сервера организовывается для локальной сети и не требуется удалённого подключения к серверу, то выбираем локальный сервер и нажимаем войти. При входе в программные обеспечения запустится окно быстрой настройки трафик инспектора. Первым делом требуется выбрать режим работы сервера. Для выполнения поставленной задачи выбираем «Сервер – сетевой шлюз» и нажимаем «Далее».

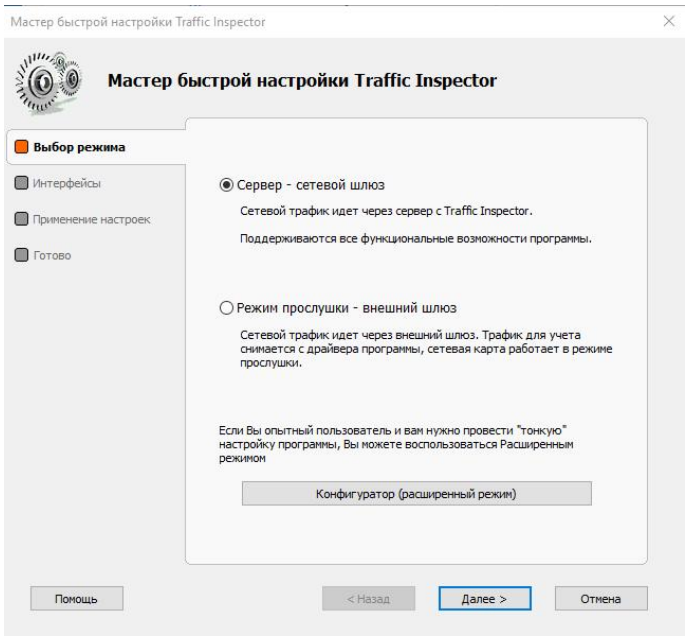

Рисунок 3 - Выбор режима трафик инспектора

После выбора режима требуется выбрать сетевые адаптеры для внешнего и внутреннего интерфейса. Для внутреннего интерфейса выбираем ранее настроенный «Ethernet 3», а для внешнего «Ethernet» и наживаем «Далее».

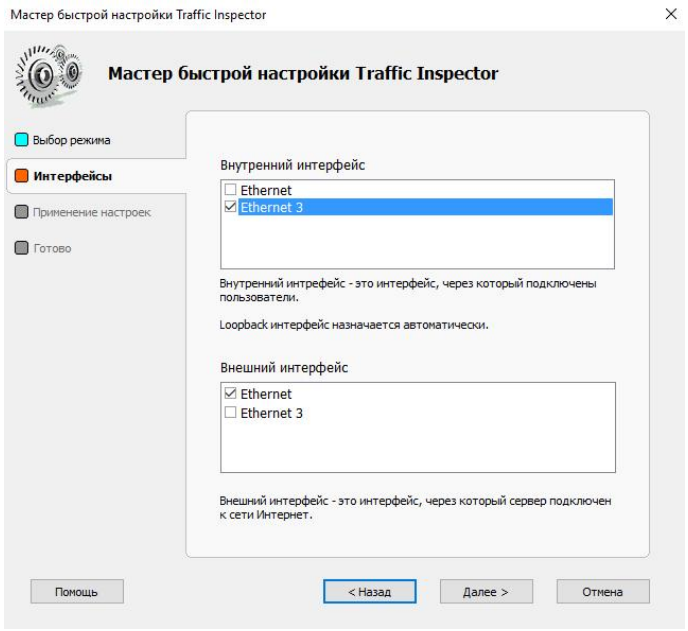

Рисунок 4 – Выбор интерфейсов

После выбора интерфейсов и применения настроек программа перенаправляет на страницу завершения быстрой настройки. Если нет в отчете никаких предупреждений, то все удачно настроилось и можно переходить к добавлению пользователей. Добавлять пользователей можно как вручную, так и с помощью сканирования сети. В нашем случае все пользователи будут изначально подключены к локальной сети, поэтому используем сканирование сети. Ставим галочку возле графы «Запустить импорт пользователей» и откроется окно импорта пользователей. Запускаем сканирование, сканирование происходит в подсети внутреннего интерфейса, т.е. сканирует подсеть 192.168.2.x.

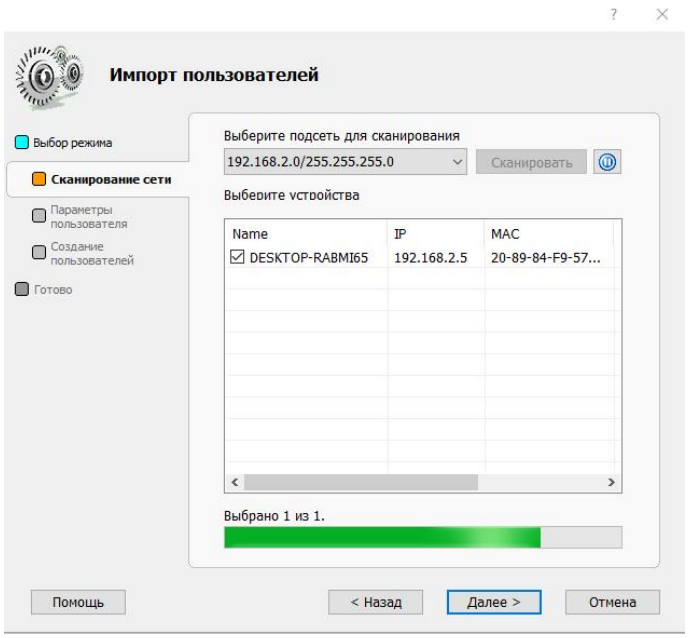

Рисунок 5 – Сканирование сети

В данный момент подключен всего 1 пробный пользователь, поэтому выбираем его и нажимаем «Далее» для продолжения. Требуется выбрать способ подключения пользователей. Изначально, подключение было по логину с паролем. Во избежание подключения к интернету с одной учетной записи нескольких пользователей было решено поставить подключение по IP+MAC адресу. В результате чего обезопасили локальную сеть, и позволило лучше контролировать трафик.

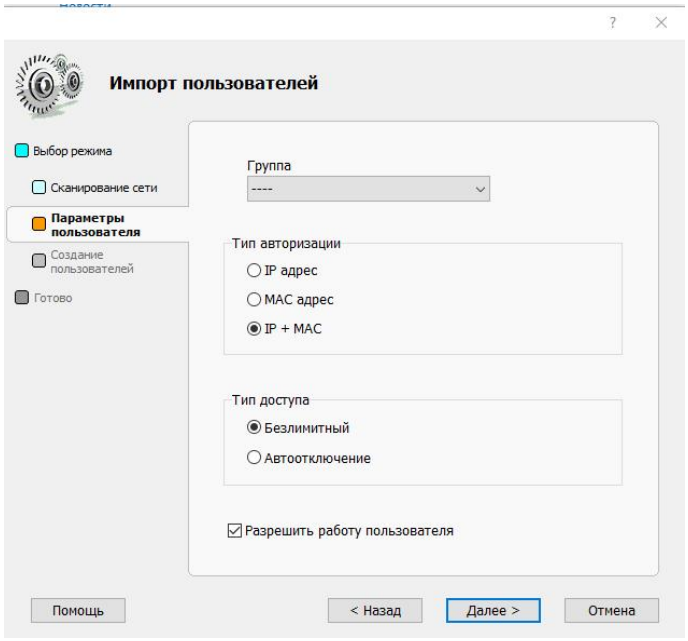

Рисунок 6 – Выбор способа подключения к сети

Для предоставления разных уровней доступа к интернету требуется использовать группы пользователей. Таким образом, для каждой группы можно настраивать своим правила и ограничения использования интернета. В нашем случае имеется две группы: сотрудники и руководство. Для добавления новой группы требуется перейти в меню «Пользователи и группы» и при нажатии кнопки «Добавить группу» программа откроет страницу добавления новых групп. В данном окне требуется ввести название новой группы, а также перейдя на вкладку «Использование модулей» указать какие модули использовать для работы с данной группой.

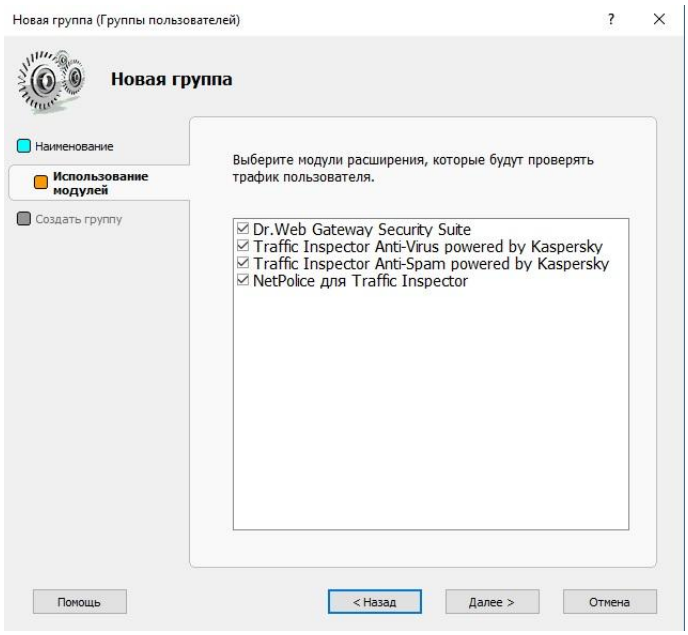

Рисунок 7 – Добавление новой группы

Для предоставления различных ограничений используется функция «Правила пользователей», таким образом при помощи правил для каждой группы пользователей можно настроить различные фильтры и ограничения выхода в интернет.

Одна из главных задач – блокировка соцсетей и развлекательных сайтов. Таким образом в разделе «URL-списки» разработчиками были созданы списки всех распространенных социальных сетей, сайтов онлайн игр и т.п. Кроме готовых списков, можно создать любой свой список с теми страницами, к которым требуется ограничить доступ. Для блокировки данного списка требуется в разделе «Правила пользователей» создать новое правило и на вкладке «Тип правила» выбрать «Трафик через прокси сервер» и на вкладке «Тип трафика» выбрать графу «Запретить», таким образом на вкладке «Проверка URL» выбираем готовый список, который требуется применить для блокировки и в свойства группы применить данное правило к нужной группе.

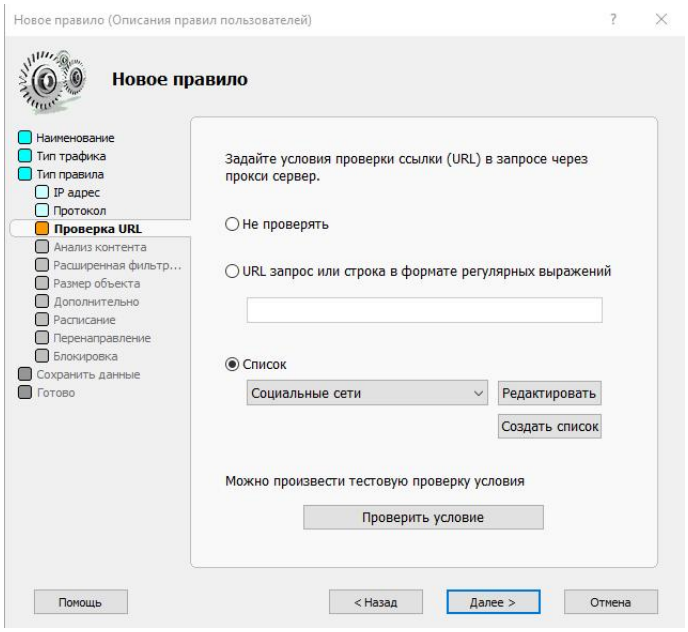

Рисунок 8 – Создание правила

Одной из главной задачи была – полная блокировка онлайн игр. Изучив систему подключения онлайн игр к сети интернет, было выявлено, что в онлайн играх нет возможности прописать Proxy-сервер. Поэтому было решено организовать подключение к интернету только через Proxy-сервер. Таким образом, смогли полностью заблокировать доступ к онлайн играм через рабочую сеть.

Кроме соцсетей и других развлекательных сайтов было решено с помощью модуля «NetPolice» заблокировать и другие тематики сайтов, такие как: онлайн-казино, наркотики и т.п. для обеспечения большего контроля над интернетом и, что бы сотрудники пользовались интернетом не в целях развлечения, а только по назначению. На вкладке «Условия» требуется запретить все тематики, к которым требуется запретить доступ и на вкладке

«Правило пользователей» выбрать действие правила, в нашем случае «Запретить».

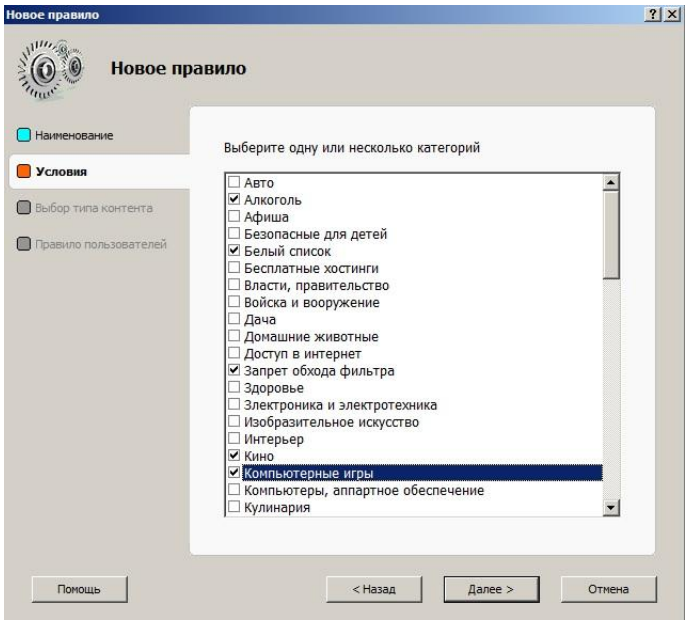

Рисунок 9 – Настройка модуля NetPolice

Для дополнительного обеспечения безопасности был активирован модуль «Dr.Web Gateway Security Suite», таким образом, при загрузке всех файлов и архивов сервер автоматически сканирует файлы на наличие вирусов и других вредоносных ПО, при нахождении, лечит их. На вкладке «Функции антивируса» было включена функция сканирования почтового и HTTP трафика и на вкладке «Настройка сканера» указали настройки для сканирования файлов.

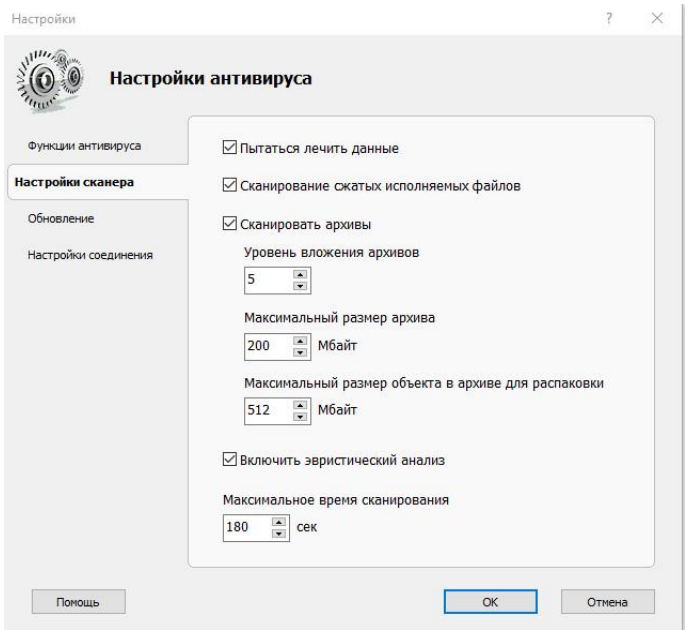

Рисунок 10 – Настройка модуля Dr.Web Gateway Security Suite

Кроме того, для группы «Сотрудники» требовалось полностью заблокировать все загрузки с торрентов и других сайтов. Так как торренты и

прочие сайты работают по многопоточной загрузке, поэтому было решено в настройках группы на вкладке «Ограничения» запретить многопоточную загрузку через Proxy-сервер, таким образом пользователи данной группы лишились возможности пользоваться торрентами и загружать файлы.

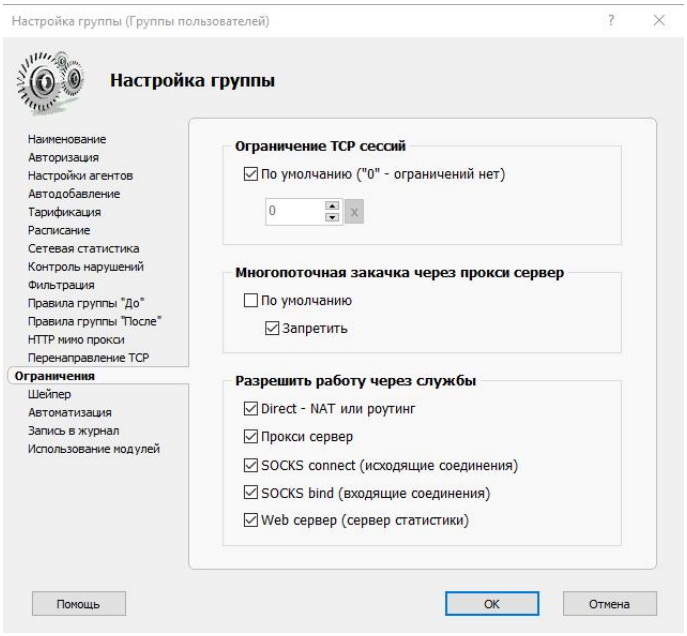

Рисунок 11 – Блокировка многопоточной загрузки

При подключении рабочих компьютеров к сети требуется настроить сетевую карту. Для этого требуется прописать IP адрес. Так как адрес внутренней сети 192.168.2.1, то требуется указывать адрес в диапазоне от 192.168.2.2 до 192.168.2.255. Основной шлюз и предпочтительный DNS-сервера делаем 192.168.2.1.

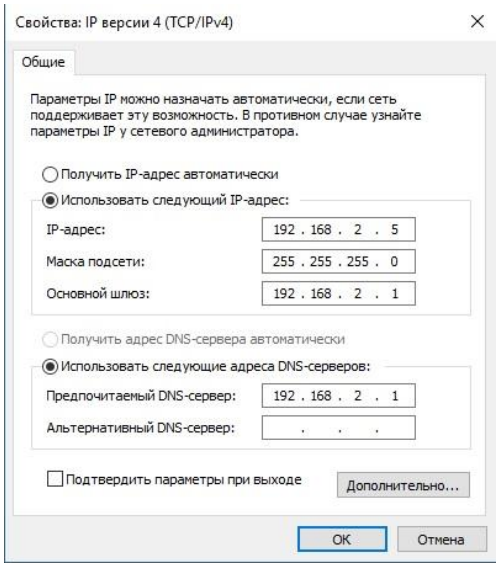

Рисунок 12 – Пример настройки сетевой карты рабочего компьютера

Для подключения к интернету через беспроводную сеть WI-FI был использован маршрутизатор cisco, который при помощи точек доступа по всему Линейному отделу организовал беспроводной выход в интернет.

В результате проведенной работы был организован сервер для на программном обеспечении Трафик инспектор для предоставления безопасного выхода в интернет сотрудникам организации по проводной и беспроводной линии связи. Кроме того, был организован полный контроль трафика, в том числе блокировка развлекательных сайтов, соцсетей, онлайн-игр, торрентов и других сайтов нарушающие правила. Изначально была установлена пробная версия продукта, по истечению срока которой была приобретена лицензия. В настоящее время система работает стабильно.

Библиографический список

1. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы // Современные тенденции технических наук: материалы междунар. науч. конф. (г. Уфа, октябрь 2011 г.). Уфа: Лето, 2011. С. 8-13.
2. Кузнецов М. А., Степаненко И. А. Проектирование системы удалённого администрирования серверов //Прикаспийский журнал: управление и высокие технологии. 2010. №. 3. С. 77-83.
3. Васильева Е. А. технология межсетевого экранирования. особенности реализации инспекторов состояния //Прикаспийский журнал: управление и высокие технологии. 2008. №. 1. С. 7-11.
4. Марков Р. Организация общего доступа в интернет и защиты от вторжений на основе Kerio Winroute Firewall 6 // Системный администратор. №. 1.
5. Яремчук С. m0n0wall – дистрибутив для создания межсетевого экрана // Системный администратор. №. 5
6. Воскресенский Г. А., Чаплыгин А. М. Способы защиты от компьютерных атак на сетевую карту // Вопросы кибербезопасности. 2013. №3.
7. Eissa M. M., Ali I. A., Abdel-Latif K. M. Wi-Fi protected access for secure power network protection scheme //International Journal of Electrical Power & Energy Systems. 2013. Т. 46. С. 414-424.
8. Mekhaznia T., Zidani A. Wi-Fi Security Analysis // Procedia Computer Science. 2015. Т. 73. С. 172-178.
9. Турский А., Панов С. Защита информации при взаимодействии корпоративных сетей в Internet //Защита информации. 1998. №. 5. С. 38-43.