ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.42

РЕАЛИЗАЦИЯ ПЕРСОНАЛЬНОГО МЕЖСЕТЕВОГО ЭКРАНА ДЛЯ ДИСТАНЦИОННОГО ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Винокуров Игорь Викторович
Кандидат технических наук, доцент кафедры «Системы обработки информации» Калужского филиала Московского Государственного Технического Университета им. Н.Э. Баумана (КФ МГТУ им. Н.Э. Баумана),
vinokurov_iv@bmstu.ru

Аннотация

При дистанционном проведении практических работ, с целью повышения уровня самостоятельности их выполнения, необходимо ограничить доступ студентов или школьников к информационным ресурсам сети Интернет. Основным назначением разработанного персонального межсетевого экрана является ограничение на сетевом уровне доступа к определённым портам, IP-адресам, DNS-именам и некоторым приложениям. Правила ограничения доступа формируются либо администратором, либо проводящим занятия преподавателем. Помимо блокирующих действий, межсетевой экран фиксирует и сохраняет информацию обо всех действиях учащегося в сети Интернет, учитываемую при оценивании его работы. Разработанный межсетевой экран реализует 4-й класс защищённости и предназначен для работы под управлением операционной системы Windows.

Ключевые слова: качество образовательного процесса, межсетевой экран, IPv4-адрес, DNS, редирект пакетов, WFP.

IMPLEMENTATION OF A PERSONAL INTERNET SCREEN FOR REMOTE PRACTICAL WORKS

Igor V. Vinokurov
Candidate of Technical Sciences, Associate Professor of Information Processing Systems Department of Kaluga Branch of Bauman Moscow State Technical University (KB BMSTU), vinokurov_iv@bmstu.ru

ABSTRACT

When conducting practical work remotely, in order to increase the level of independence of their implementation, it is necessary to restrict the access of students or schoolchildren to information resources of the Internet. The main purpose of the developed personal firewall of the 4th security class is to restrict access at the network level to certain ports, IP addresses, DNS

names and some applications. Access restriction rules are formed either by the administrator or by the teacher conducting the classes. In addition to blocking actions, the firewall captures and stores information about all student actions on the Internet, which is taken into account when assessing his work. The developed firewall is designed to operate under the Windows operating system.

Keywords: quality of education, firewall, IPv4 address, DNS, packet redirect, WFP.

Актуальность

Ограничение доступа студентов вузов или школьников к информационным ресурсам Интернет при дистанционном проведении практических или контрольных работ является в настоящее время актуальной задачей. Одним из возможных способов её решения является использование индивидуальных межсетевых экранов (МЭ), реализующих фильтрацию информации по некоторой совокупности критериев – IP-адресам, номерам портов, именам сетевых подключений и т. д.

Большинство научных работ в области безопасности в сетях ЭВМ с использованием МЭ носят чисто теоретический характер безотносительно к областям его применения [1]. Область применения МЭ может предъявить к его реализации специфичные требования. Как показала практика проведения дистанционных занятий в ряде учебных заведений, основным требованиям при организации дистанционных занятий является ограничение доступа к информационным ресурсам сети Интернет по их IP-адресам, DNS-именам и именам сетевых подключений с фиксацией всех действий и редиректа их сетевого трафика. Необходимость редиректа сетевого трафика на специализированное программное обеспечение (ПО) заключается в более детальном анализе действия студента. Редирект практически не реализован в доступных к использованию МЭ – Comodo Firewall [2], Ashampoo Firewall Free [3], AVS Firewall [4], Zone Alarm Free Firewall [5] и других. Как следствие, было принято решение о разработке персонального МЭ, реализующего редирект сетевых пакетов на указанный IP-адрес. За основу МЭ вуза был взят МЭ ЗАО “Калуга-Астрал” [6], использующийся в своё время для решения аналогичных задач в школах.

Разработанный МЭ реализует следующие основные действия:

1. регистрация администратора или пользователя;
2. доступ к МЭ по логину и паролю пользователя;
3. блокировка IPv4-адресов, портов, приложений, DNS-имён и подключений;
4. редирект сетевых пакетов;
5. включение и выключение МЭ в заданное время;
6. создание и редактирование текстового файла с описанием правил блокировок;
7. логирование операций, осуществляемых МЭ.

Все перечисленные выше действия реализованы в виде нескольких групп команд (рис. 1).

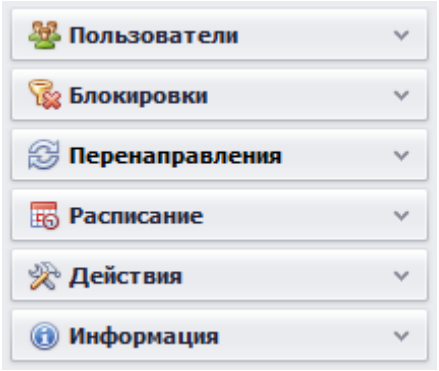

Рисунок 1. *Группы команд МЭ*

Команды группы “Пользователи” предназначены для регистрации нового пользователя, реализации входа, выхода, изменения прав и удаления зарегистрированных пользователей (рис. 2).

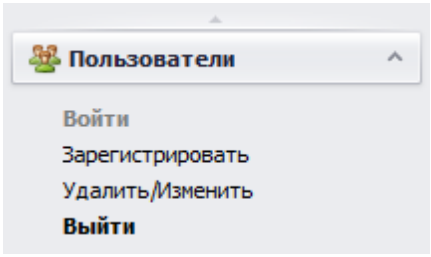

Рисунок 2. *Команды группы “Пользователи”*

При выборе команды “Войти” отображаются выпадающий список с логинаим всех зарегистрированных пользователей и однострочный текстовой редактор для ввода пароля (рис. 3). Все остальные команды этой группы, за исключением “Выйти”, возможны только для администратора. Для обычного пользователя они недоступны.

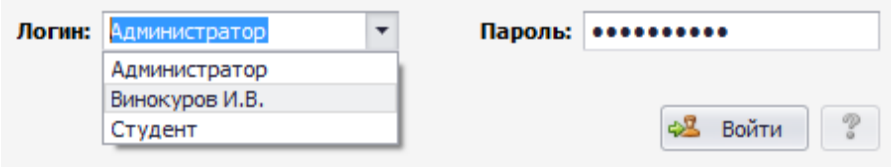

Рисунок 3. *Реализация входа пользователя*

Логин и пароль, вводимые при первом запуске МЭ, будут относиться к администратору. Каждая последующая регистрация позволяет создать или обычного пользователя, или нового администратора. Администратору доступны все операции с МЭ; для обычного пользователя их состав практически всегда является ограниченным (рис. 4).

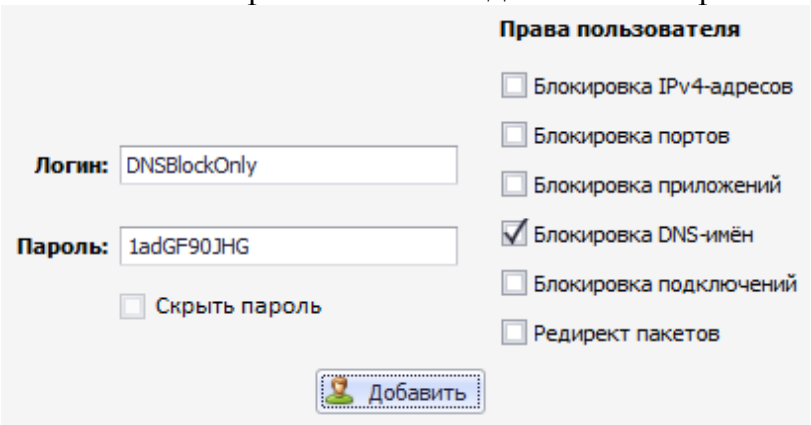

Рисунок 4. *Регистрация нового пользователя (не администратора)*

Как было отмечено выше, основными функциями, разработанного МЭ, являются реализация блокировок IPv4-адресов, номеров портов, приложений, DNS-имён и

подключений. Каждое из этих действий осуществляется в результате выбора соответствующей ей команды из группы “Блокировки” (рис. 5).

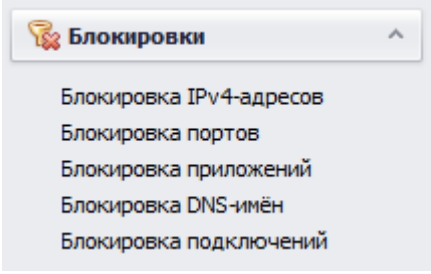

Рисунок 5. *Команды группы “Блокировки”*

При блокировке IPv4-адресов необходимо в комбинированный с текстовым редактором выпадающий список ввести соответствующий IPv4-адрес. Пример блокировки таких адресов для поисковых систем ya.ru и yandex.ru приведён на рисунке 6.

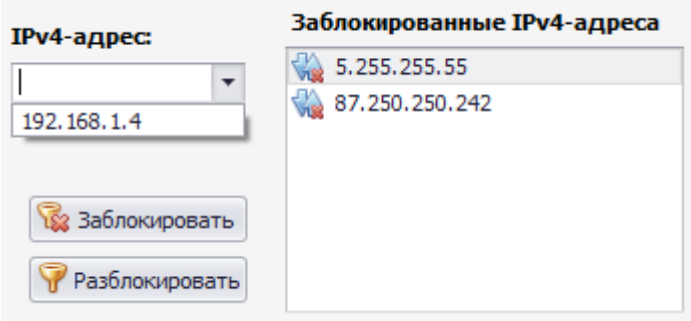

Рисунок 6. *Блокировка IPv4-адресов*

При блокировке портов можно выбрать тип блокируемых сообщений – входящие, исходящие или входящие и исходящие одновременно (рис. 7).

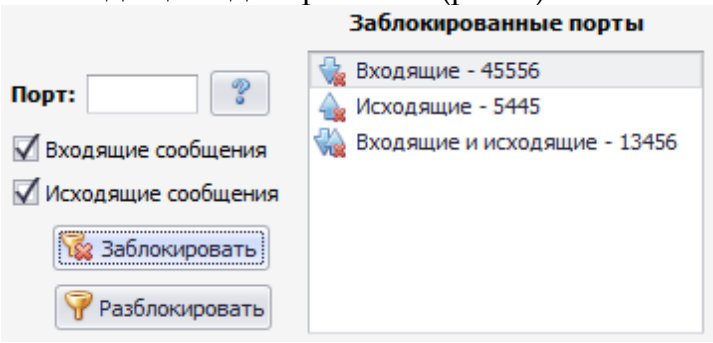

Рисунок 7. *Блокировка портов и типов сообщений*

С целью ввода номеров портов основных сетевых протоколов и служб, таких как протокол FTP (порт 21), служба Telnet (порт 23), простой протокол передачи почты SMTP (порт 25), служба доменных имён DNS (порт 53) и других, реализовано информационное окно, содержащее информацию о наименовании протокола или службы и соответствующий ей номер порта. Это информационное окно отображается по нажатию на кнопку с пиктограммой вопросительного знака (рис. 7).

Блокировка приложений предполагает их выбор из файловой системы локального компьютера (рис. 8). Выход в Интернет для заблокированных МЭ приложений становится невозможным.

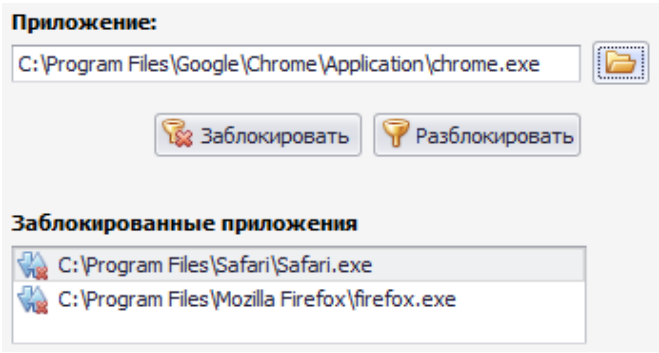

Рисунок 8. *Блокировка приложений*

При использовании блокировки DNS-имён можно заблокировать любые информационные ресурсы Интернет по их DNS-имени. Например, на рисунке 9 приведена блокировка DNS-имени известных поисковых систем *bing.com*, *google.ru*, *ya.ru* и других.

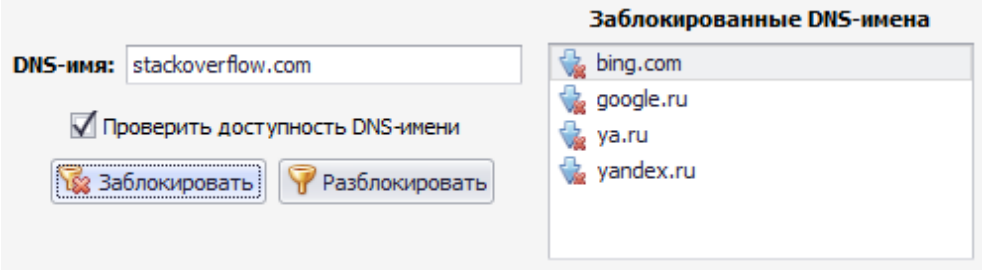

Рисунок 9. *Блокировка ресурсов Интернет по их DNS-именам*

На этом рисунке флажок "Проверить доступность DNS-имени" предназначен для проверки правильности ввода DNS-имени и доступности сетевого ресурса по введенному DNS-имени.

И, наконец, блокировка сетевых подключений позволяет заблокировать входящие или исходящие сообщения с указанными IPv4-адресами и номерами портов. Номера портов, для всех основных сетевых служб, приведены в справочнике, отображаемым по нажатии на кнопку с пиктограммой вопросительного знака (рис. 10).

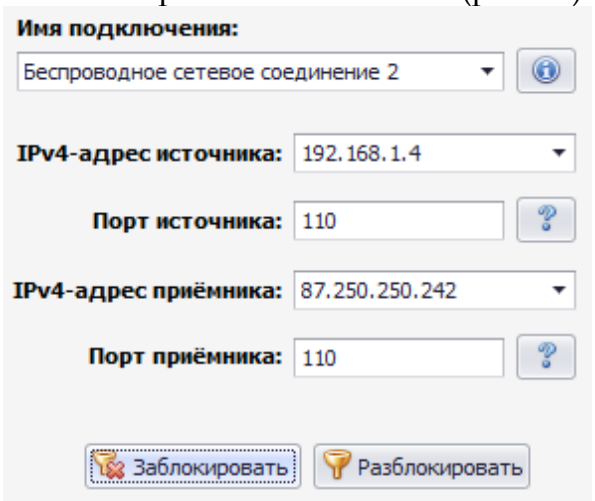

Рисунок 10. *Блокировка подключений*

Редирект сетевых пакетов (подмена получателя) предназначен для их перенаправления на указанные IPv4-адрес и порт, на которые настроено специализированное ПО для анализа сетевой активности (рис. 11).

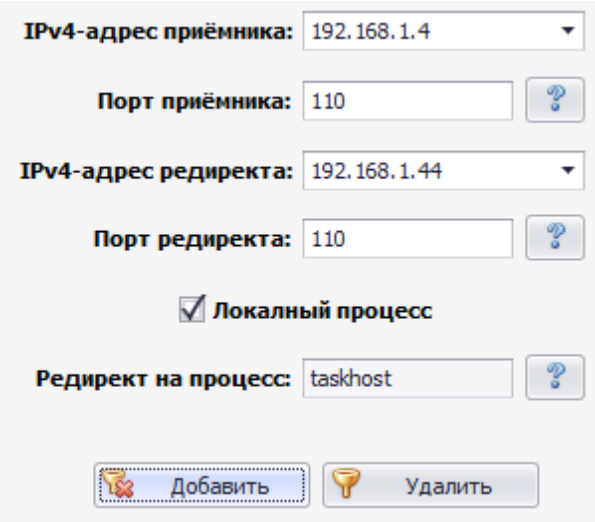

Рисунок 11. *Редирект сетевых пакетов*

Создание и последующее редактирование текстового файла с описанием правил блокировок возможно не только в результате выбора команд из их групп МЭ (рис. 1), но и вручную по команде “Редактирование файлов” из группы “Действия”. Все записи файла описания блокировок относятся к блокировке того или иного типа. Содержимое этого файла сохраняется в зашифрованном виде.

Как было отмечено выше, МЭ позволяет сохранять информацию обо всех заблокированных сетевых пакетах при запуске или останове процессов (рис. 12).

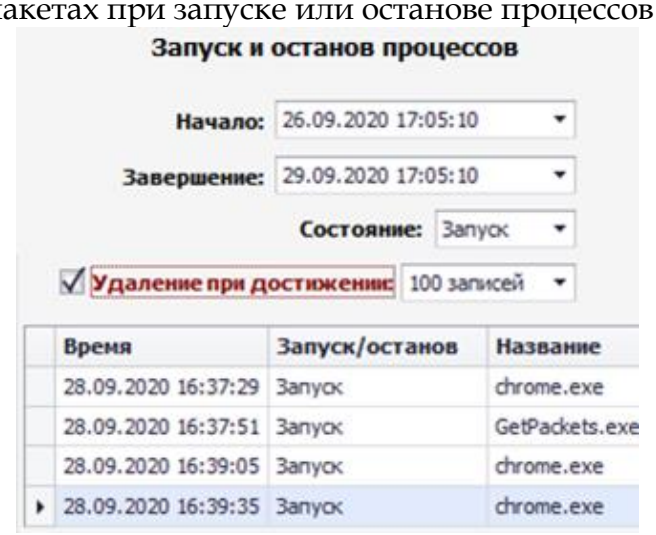

Рисунок 12. *Фиксирование запущенных процессов*

Дополнительной возможностью МЭ является его выключение и выключение по расписанию. Интервал времен, в течение которого МЭ будет работать, задаётся единственной командой группы “Расписание” (рис. 13).

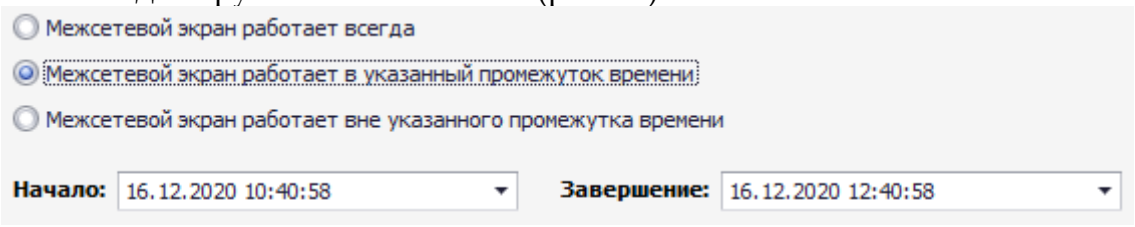

Рисунок 13. *Задание времени работы МЭ*

МЭ предназначен для работы только под управлением операционной системы Windows и представляет собой распределённое приложение, состоящее из драйвера, работающего на уровне ядра этой операционной системы и графического интерфейса, посредством которого осуществляется взаимодействие с пользователем. Драйвер

разработан с использованием пакета WDK [7] и реализует все основные действия по сетевой фильтрации и редиректу пакетов с использованием платформы WFP [8], позволяющей реализовать инспекцию, модификацию и трансляцию сетевых пакетов. Графическая оболочка МЭ написана на языке C# [9] в среде Visual Studio с использованием визуальных компонентов библиотеки DevExpress [10].

Наличие необходимых программных компонент Windows проверяет инсталлятор МЭ на этапе его установки.

На основе платформы WFP был разработан межсетевой экран 4-го класса защищенности, поскольку в нем были реализованы [11]:

1. управление доступом за счет фильтрации пакетов на сетевом уровне;
2. учет фильтруемых пакетов;
3. идентификация пользователей;
4. целостность в виде наличия средств контроля за целостностью всех программных компонент МЭ;
5. тестирование и восстановление в виде контроля целостности программных компонент МЭ, проверке правил фильтрации, процесса идентификации и аутентификации, а также возможности восстановления после сбоев и отказов оборудования.

Отличительной особенностью МЭ от существующих в настоящее время аналогов является наличие возможности перенаправления сетевых пакетов на специализированное ПО для проведения анализа реализованных действий.

Достоинством разработанного МЭ является простота его использования, недостаток, над устранением которого в настоящее время ведётся работа – отсутствие возможности блокировок IPv6-адресов.

Список литературы

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных (в 2-х томах) [Текст] / В.А. Герасименко. – М.: Энергоатомиздат, 1994. – 400 с.
2. Comodo Firewall [Электронный ресурс]. URL: https://personalfirewall.co- modo.com/ (дата обращения 23.04.2021)
3. Ashampoo Firewall [Электронный ресурс]. URL: https://ashampoo-firewall.informer.com (дата обращения 23.04.2021)
4. AVS Firewall [Электронный ресурс]. URL: https://avsfirewall.infor- mer.com/ (дата обращения 23.04.2021)
5. ZoneAlarm Free Firewall [Электронный ресурс]. URL: https://www.zone- alarm.com/ (дата обращения 23.04.2021)
6. Винокуров И.В. Реализация персонального межсетевого экрана // “Электромагнитные волны и электронные системы”. – 2015. – Т. 20. – № 7. – С. 44-49.
7. Комплект драйверов Windows – Windows Driver Kit [Электронный ресурс]. URL: https://ru.qwe.wiki/wiki/Windows_Driver_Kit (дата обращения 23.04.2021)
8. Платформа фильтрации Windows – Windows Filtering Platform [Электронный ресурс]. URL: https://ru.qwe.wiki/wiki/Windows_- Filtering_Platform (дата обращения 23.04.2021)
9. Троелсен Э. Язык программирования C# 7 и платформы .NET и .NET Core [Текст] / Э. Троелсен, Ф. Джепикс. – М: Вильямс, 2018. – 1328 с.
10. DevExpress [Электронный ресурс]. URL: https://www.devexpress.com (дата обращения 23.04.2021)
11. Классификация средств защиты информации от ФСТЭК и ФСБ России [Электронный

ресурс]. URL: https://www.anti-malware.ru/analytics/- Market_Analysis (дата обращения 23.04.2021)

References

1. Gerasimenko V.A. Information protection in automated data processing systems (in 2 volumes). M.: Energoatomizdat, 1994. – 400 p.
2. Comodo Firewall [Site]. URL: https://personalfirewall.comodo.com (access date 23.04.2021)
3. Ashampoo Firewall [Site]. URL: https://ashampoo-firewall.informer.com (access date 23.04.2021)
4. AVS Firewall [Site]. URL: https://avs-firewall.informer.com (access date 23.04.2021)
5. ZoneAlarm Free Firewall [Site]. URL: https://www.zonealarm.com (access date 23.04.2021)
6. Vinokurov I.V. "Personal firewall implementation" Electromagnetic waves and electronic systems. vol. 20. no. 7. pp. 44-49, 2015.
7. WDK [Site]. URL: https://ru.qwe.wiki/wiki/Windows_Driver_Kit (access date 23.04.2021)
8. WFP [Site]. URL: https://ru.qwe.wiki/wiki/Windows_Filtering_Platform (access date 23.04.2021)
9. Troelsen Andrew and Philip Jepiks, Programming language C # 7 and the platform .NET and .NET Core. M: Williams, 2018. – 1328 p.
10. DevExpress [Site]. URL: https://www.devexpress.com (access date 23.04.2021)
11. Classification of information security tools from the FSTEC and the FSB of Russia [Site]. URL: https://www.anti-malware.ru/analytics/Market_Analysis (access date 23.04.2021)