проблем Азербайджана													

28 августа 2010 года было подписано Соглашение №1416Р о делимитации границы между России и Азербайджана переносилась с правого берега реки Самур на середину гидроузла и стороны договорились впредь производить деление водных ресурсов в равных долях и установить размер экологического сброса равным 30,5%.

Рис.1. Река Самур в Магеррамской районе.

Таким образом 96% площади водосбора приходится на территории России, а 4%-Азербайджана[4].

Список литература:

1.Иманов Ф.А.,Асадов М.Я. Оценка водных ресурсов и экологического состояние реки Самур (Восточной Кавказ)https://ru. Wikipediya/org

2.Рустамов С.Г.,Кашкай Р.М., Водные ресурсы Азербайджана ССР. Баку:Элм, 1989, 184 с.

3.Ахмедзаде А.Дж, Гейдар Алиев и Водные хозяйство Азербайджана Баку,Азернешр,2002. 216с.

4.Водные ресурсы России и их использование/ под ред.И.А. Шикломанова СПБ: Изд.Гос.Гидрологические Института,2008.600 с.

УДК 004.81.93.29

МЕТОДИКИ НАСТРОЙКИ ПРАВИЛ БРАНДМАУЭРА МУЛЬСЕРВИСНОЙ СУПЕРКОМПЬЮТЕРНОЙ СЕТИ

Бондарчук Виктория Валерьевна
кандидат технических наук,
зав. отделом распознавания зрительных образов,
Донецкий Институт проблем искусственного интеллекта

FIREWALL RULE CONFIGURATION TECHNIQUES MULTI-SERVICE SUPERCOMPUTER NETWORK

Bondarchuk V.V.
Candidate of Technical Sciences,
Head visual recognition department,
Donetsk Institute of Artificial Intelligence Problems
DOI: 10.31618/ESU.2413-9335.2020.1.75.828

АННОТАЦИЯ

В статье описаны Правила настроек брандмауэра для обеспечения информационной безопасности при передаче данных через Интернет мультисервисной суперкомпьютерной сети. Обоснована актуальность трёхуровневой архитектуры. Описана логика информационных потоков, настройки брандмауэра. Службы сертификации

ABSTARCT

The article describes the Firewall settings rules for ensuring information security when transmitting data over the Internet of a multiservice supercomputer network. The relevance of three-level architecture is grounded. The logic of information flows, firewall settings is described, Certificate Services.

Ключевые слова: Правила настроек брандмауэра, логика информационных потоков. Службы сертификации

Key words: Firewall Settings Rules, information flow logic, Certificate Services.

Тенденции социально-экономического развития сопровождаются обеспечением устойчивости и безопасности информационных технологий, развертыванием гибких и устойчивых гибридных мультиоблачных нфраструктур, высокопроизводительных систем; улучшенных интеграционных различных решений управления ИТ-инфраструктурой; защищенных данных в облачных средах; обеспечения резервного копирования и восстановлени данных в виртуальных и контейнерных средах, предоставляющих высокую пропускную способность и надежную доступность данных.

Разработана мультисервисная суперкомпьютерная сеть (СКС) управления процессами социально-экономического развития [1, с.39]. Представлены схемы структурированной компьютерной сети, конфигурации сервера, рабочей станции центрального офиса (ЦО); функции процессов на серверах, оборудование для стыковки сервера и рабочих станций; рекомендации выбора оборудования для подключения подразделений в Интернет; Требования к основному и дополнительному серверам баз данных, расписание репликации. Проект предназначен для решения следующих подзадач: суперкомпьютерная сеть центрального офиса, 20 министерств и 40 предприятий Республики; описание активного оборудования для стыковки сервера и рабочих станций; обоснование и выбор оборудования для подключения подразделений Интернет; описание требований к основному и дополнительному серверам баз данных, расписание репликации.

Разработан комплекс профилактических мероприятий для обеспечения сохранности данных с применением технологий RAID-массивов, Executive Diskeeper v7.0, RAID-контроллера, Active Directory, NTFS-разрешения информационных ресурсов, разделов групповых политик на уровне домена, подразделений, виртуальной частной сети; гибкий инструмент определения прав пользователя в системе; централизованное управление мероприятиями по антивирусной защите рабочих станций [2, с.82].

Для осуществления информационной безопасности СКС выполним настройки брандмауэра, используя трёхуровневую модель доступа к данным. Она характеризуется тем, что деловая логика системы выносится на отдельный уровень и обособляется от пользовательского интерфейса и хранения данных. В трехуровневой модели выделяются следующие уровни: уровень представления данных (клиентский компьютер); уровень деловой логики (сервер приложений); уровень хранения данных (сервер БД).

Клиент предназначен только для представления информации пользователю, вся обработка данных осуществляется на сервере приложений. Деловая логика на этом сервере реализована в виде компонентов, и через вызовы методов этих компонентов клиентская программа получает необходимые пользователю данные. Сервер приложений обслуживает поступающие от такого клиента обращения, осуществляет запросы к серверу базы данных и обрабатывает их результаты.

Актуальность трехуровневой архитектуры обусловлена следующими причинами:

1. Поддержка распределенных архитектур и Интернет. Построение Интернет - систем невозможно без выноса деловой логики на средний уровень. Понятие "тонкого клиента" подразумевает использование серверов приложений, так как сервер БД не предназначен для обработки http-обращений, а HTML-клиент с браузером не может обсчитывать данные. В отличие от клиент-серверной модели трехуровневая модель позволяет обеспечить доступ к данным клиента самых различных типов - Windows-клиент через JBC, HTML-клиент через Интернет, смартфон (PDA) через беспроводный доступ.

2. Снижение затрат. Отделение обработки данных от пользовательского интерфейса позволяет изменять деловую логику приложения, не затрагивая клиента. При создании новой версии бизнес - логики нет необходимости обновлять все клиентские места - необходимые изменения осуществляются на одном-единственном сервере приложений. За счет этого удается снизить как финансовые, так и временные затраты на обслуживание используемых систем.

3. Масштабируемость. При повышении требований к быстродействию возможен перенос деловой логики системы на более производительную платформу, что обеспечивается кроссплатформенной совместимостью сервера приложений. При необходимости наращивания вычислительных ресурсов становится возможным приобрести только один мощный компьютер для сервера приложений, а не много быстродействующих клиентских станций.

4. Отказоустойчивость. Технологии, лежащие в основе сервера приложений, позволяют строить такие отказоустойчивые системы, которые могут работать даже в случае выхода из строя одного или нескольких компьютеров. При этом используется кластеризация - объединение в единую логическую группу нескольких серверов

приложений. Для клиентов такая группа выглядит как единый сервер, и в случае выхода из строя какого-либо из серверов кластера нагрузка динамически перераспределяется между оставшимися серверами.

Трёхуровневая модель доступа к данным информационной системы ЦО, с учётом использования брандмауэра изображена на рисунке 1.

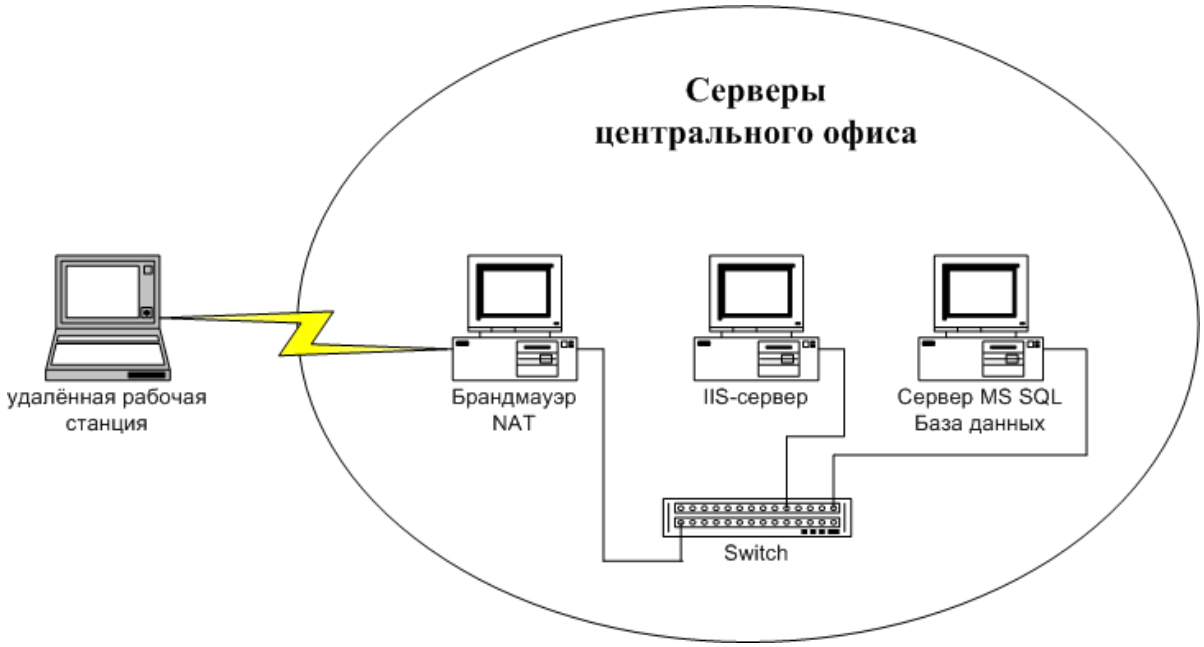


Рис. 1 Трехуровневая модель доступа к данным ЦО

Опишем логику информационных потоков в корпоративной информационной системе:

Планируется, что сервер 1 СКС центрального офиса (ЦО) будет иметь реальный статический IP-адрес, предоставленный провайдером. К тому же необходимо будет зарегистрировать DNS-имя center_office.com, указывающее на этот IP.

Итак, пользователи рабочих станций министерств и предприятий с помощью клиентской программы Internet Explorer будут отправлять запросы IIS-серверу, который расположен на сервере 3. При этом весь трафик будет фильтроваться брандмауэром WinRoute v.4.1, который предполагается установить на сервере 1.

Пользователи будут задавать в Интернет браузере хост web-узла ЦО (IP-адрес либо DNS-имя), и, следовательно, в начале будут обращаться на сервер 1. Брандмауэр сервера 1 после проверки трафика перенаправит запрос на IIS-сервер (сервер 3), на котором будет запущено приложение обработки данных. Оно осуществит запросы к серверу базы данных MS SQL v.7.0 (сервер 2) и обработает их результаты.

Далее, полученные результаты работы сервера приложений направятся через маршрутизатор сервера 1 WinRoute v 4.1 к web-браузеру рабочей станции, который отобразит их.

Рассмотрев трёхуровневую модель доступа к данным СКС центрального офиса, перейдём к описанию настроек брандмауэра WinRoute v.4.1.

Руководство ЦО планирует арендовать у провайдера 20 IP-адресов, например, диапазон от 193.200.19.1 до 193.200.19.20 с маской сети 255.255.255.0. Внешнему интерфейсу сервера 1 будет присвоен адрес 193.200.19.1, а внутренний интерфейс будет иметь IP 192.168.1.1, зарезервированный для использования в локальной сети. Оставшиеся реальные IP-адреса будут динамически присваиваться рабочим станциям министерств и предприятий после прохождения ими авторизации на сервере удалённого доступа (сервер 1). Предполагается, что рабочие станции центрального офиса будут иметь IP-адреса для локального использования: управление (192.168.1.20 – 192.168.1.22), бухгалтерия (192.168.1.4 – 192.168.1.9), менеджеры (192.168.1.10 – 192.168.1.11), специалист (192.168.1.12). Серверам центрального офиса присвоят следующие IP-адреса: сервер 1 (192.168.1.1), сервер 2 (192.168.1.2), сервер 3 (192.168.1.3). Специалисты и откомандированные сотрудники будут получать динамические IP-адреса у своих провайдеров при подключении к Интернет. Для настройки брандмауера (рис. 2) необходимо выполнить следующие шаги: произвести настройку фильтров; произвести настройку антиспама; произвести планирование портов.

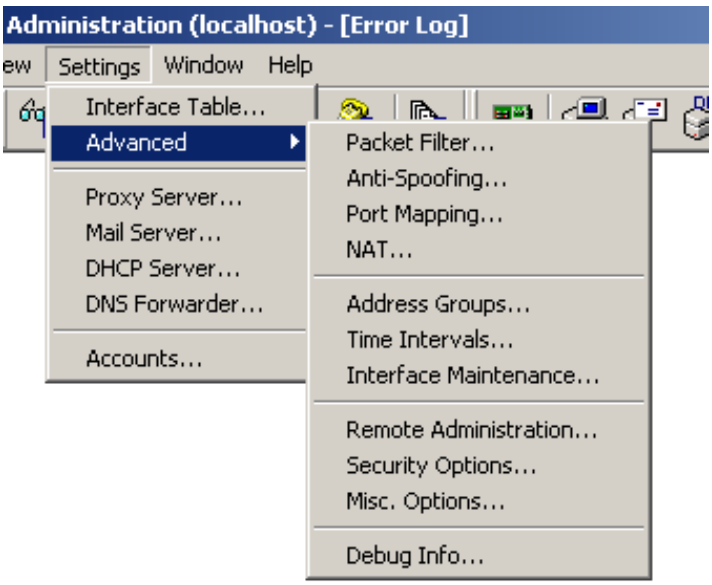


Рис. 2 Настройка брандмауэра WinRoute v.4.1

Путь к окнам настроек перечисленных компонентов брандмауэра показан на рисунке 3.

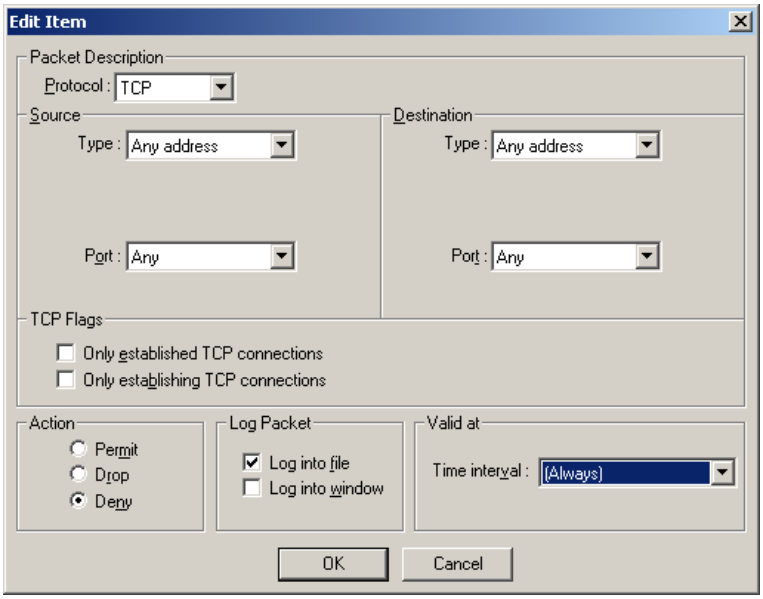


Рис. 3 Общий вид меню настройки в WinRoute v. 4.1

Шаг 1: произведём настройку фильтров.

Необходимо выбрать пункт меню Packet Filter. Появится окно с одноимённым названием (Рис.4). Будем добавлять правила фильтрации трафика для всех интерфейсов брандмауэра (~Any interface). Откроется окно для добавления правил (Рис. 5), в этом окне первым делом мы запретим доступ к нашим сетевым ресурсам с любого IP-адреса. Эта процедура необходима во благо избегания «дыр» в сетевой безопасности.

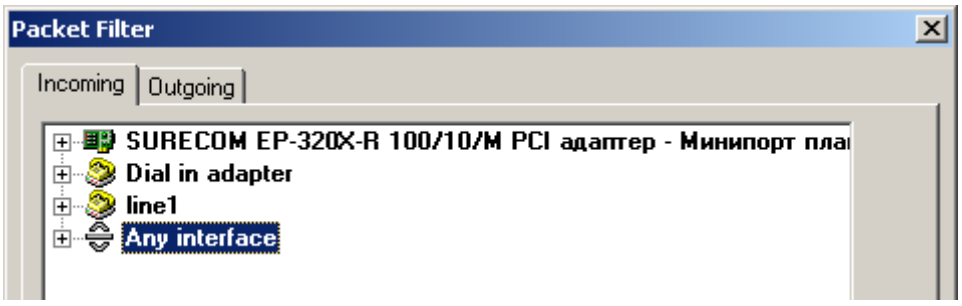


Рис.4 Окно настройки фильтра Packet Filter

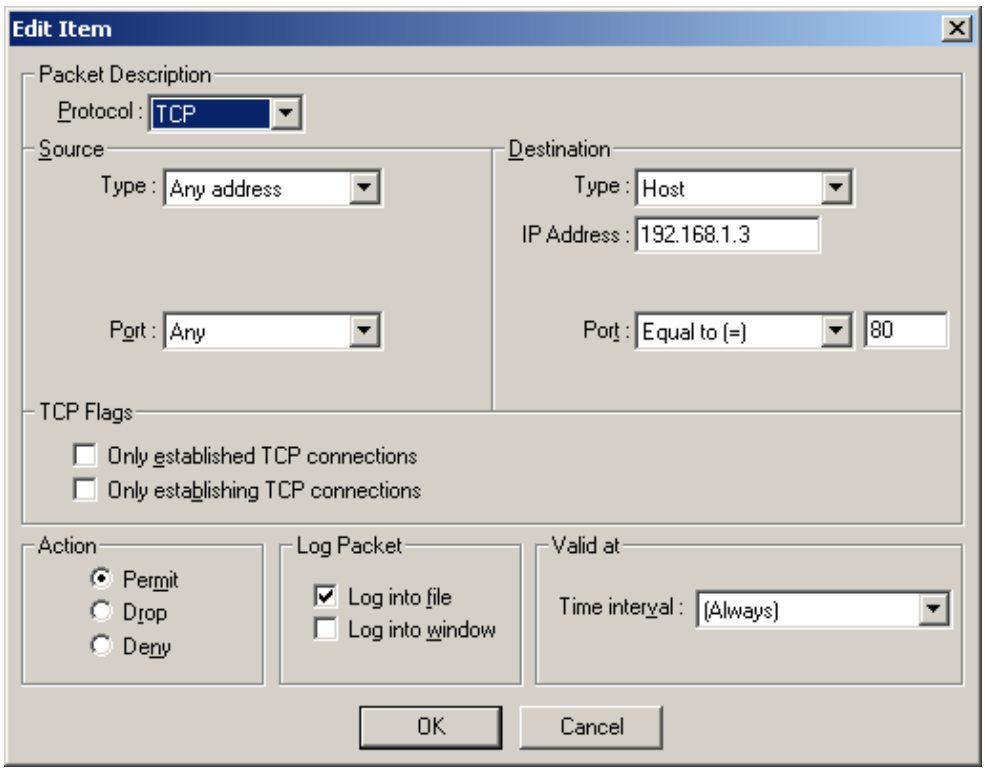


Рис. 5 Добавление правила общего запрета

На рисунке 6 представлено правило, по которому запросы с любого IP на web-узел брандмауэр переадресует Серверу 3, на котором запущены IIS-сервисы.

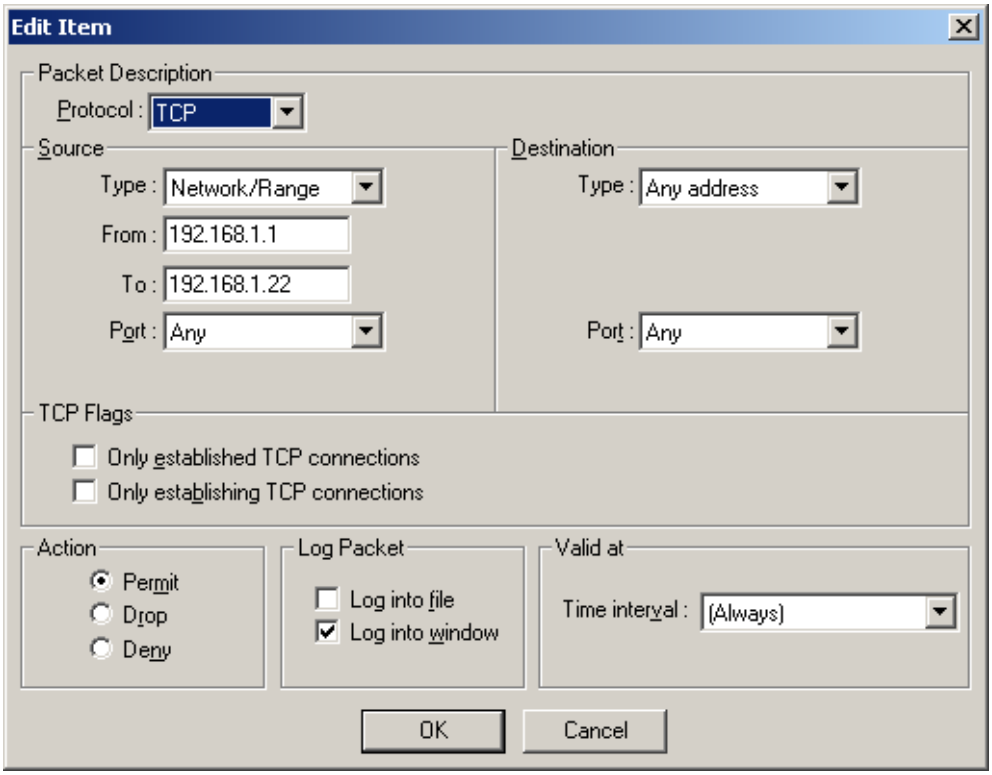


Рис. 6 Добавление правила доступа к web-серверу

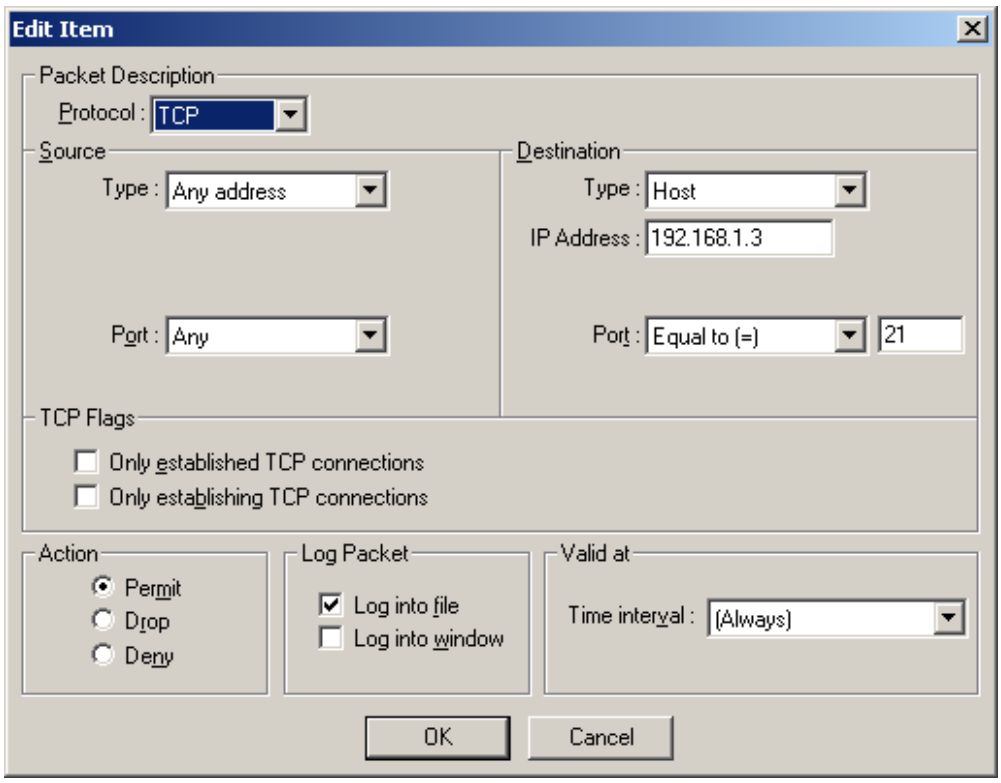


Рис. 7 Добавление правила доступа к ftp-серверу

Для удалённого администрирования web-узла администратором, а также для обмена файлами между пользователями СКС фабрики необходимо будет разрешить доступ к ftp-серверу (Рис.7).

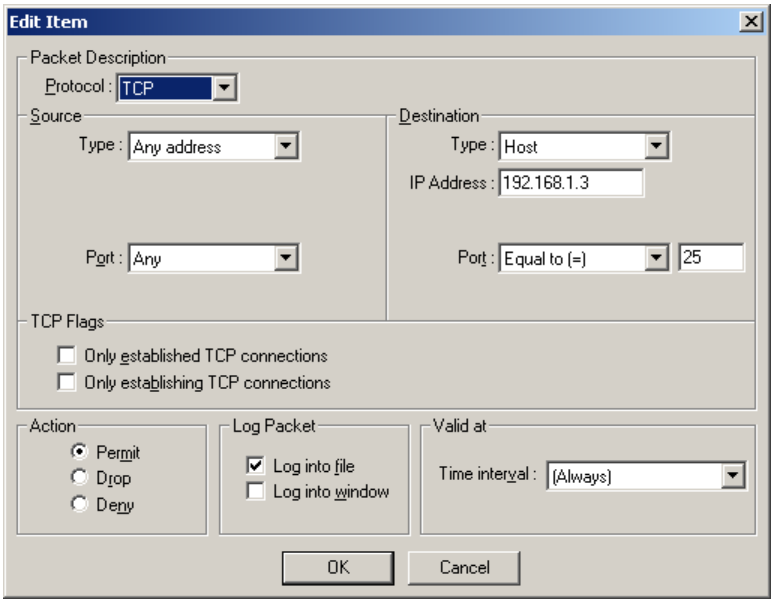


Рис. 8 Правило доступа к SMTP-сервису

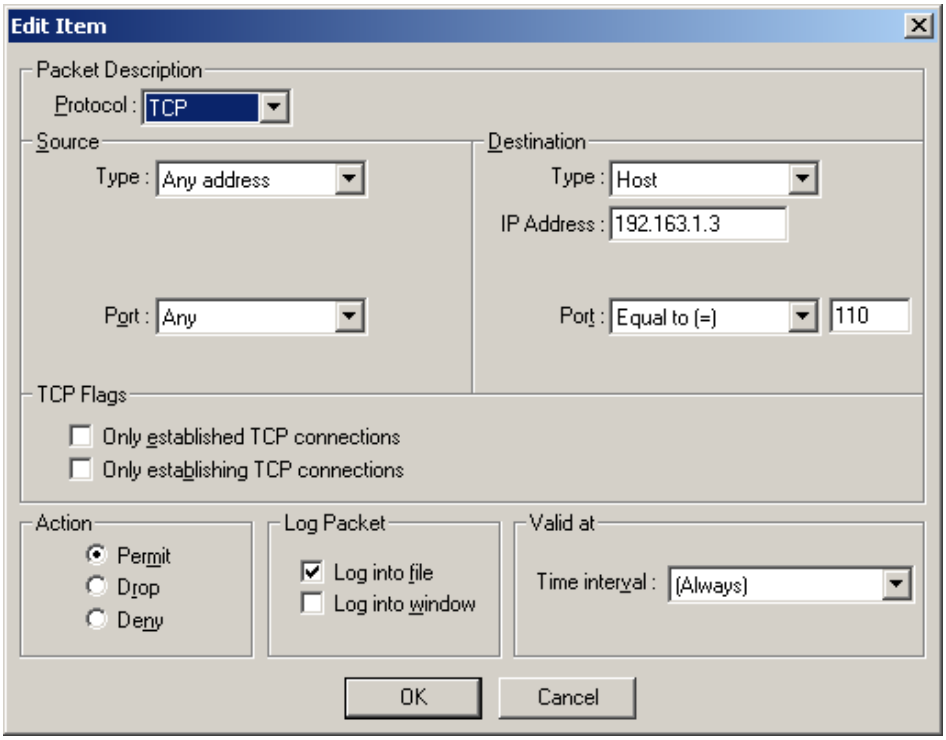


Рис. 9 Правило доступа к POP3-сервису

Планируется, что сотрудники будут пользоваться электронной почтой, поэтому необходимо обеспечить доступ к почтовым сервисам (Рис.8, 9).

На рисунке 10 изображено добавление правила, которое даёт возможность компьютерам сети ЦО посылать пакеты как любому IP-адресу СКС, так и ресурсам Интернет.

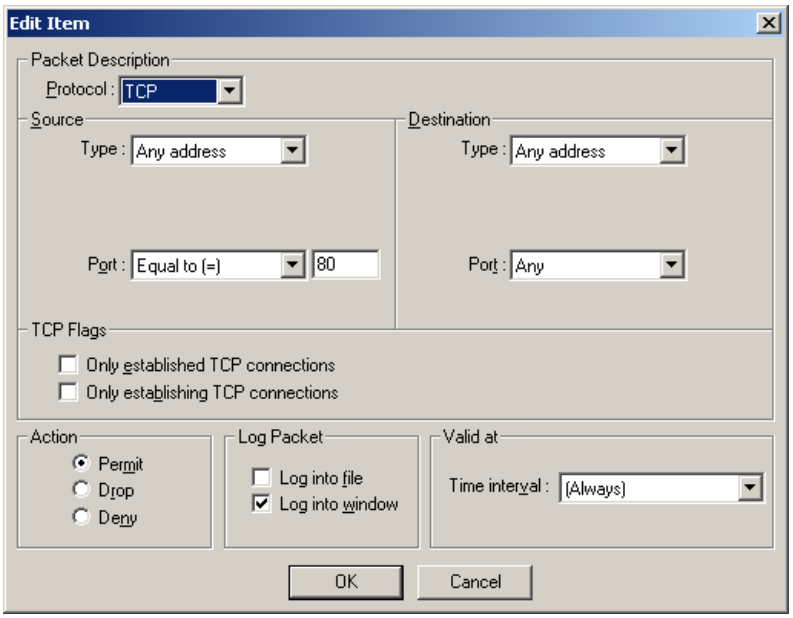


Рис. 10 Правило разрешения исходящего трафика для СКС ЦО

Необходимо разрешить доставку пакетов, отправителями которых являются рабочие станции министерств и предприятий, а получателями - компьютеры центрального офиса и другие узлы сети Интернет (Рис.11).

При всём этом, компьютерам СКС ЦО каким-то образом нужно получать входящие пакеты по http и https-запросам. Поэтому, на наш взгляд, необходимо добавить правило, разрешающее компьютерам сети принимать пакеты данных, отосланные с 80-го порта (Рис.12).

Исчерпывающий список правил, необходимых для настойки пакетного фильтра представлен на рисунке 12.

Шаг 2: произведём настройку антиспама.

Необходимо выбрать пункт меню Anti-Spoofin, вследствие чего появится окно с одноимённым названием. Можно осуществить настройку

антиспама для любого интерфейса, отображённого в окне.

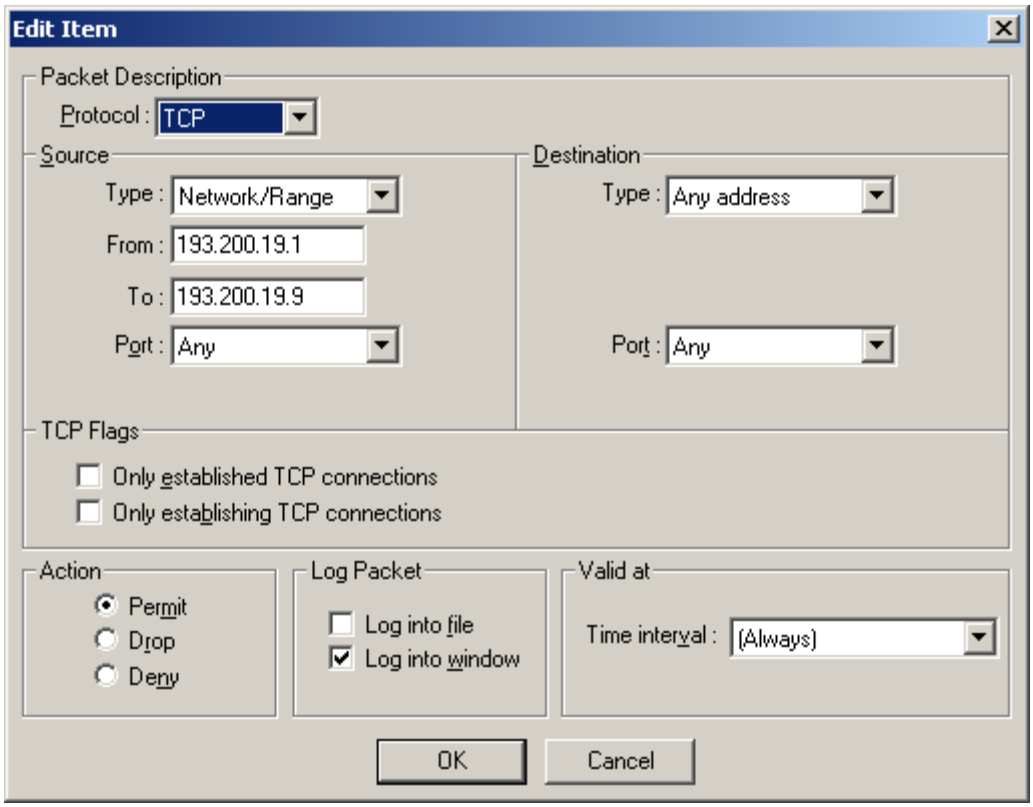


Рис.11 Доступ рабочих станций министерств и предприятий к ресурсам СКС центрального офиса

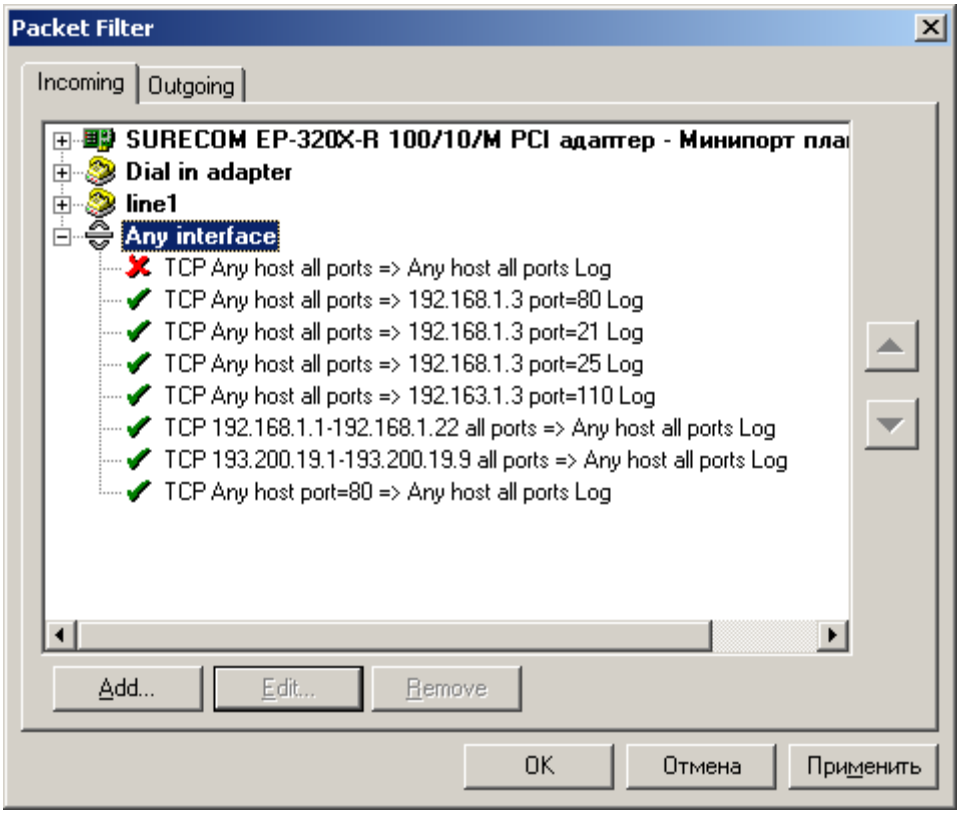
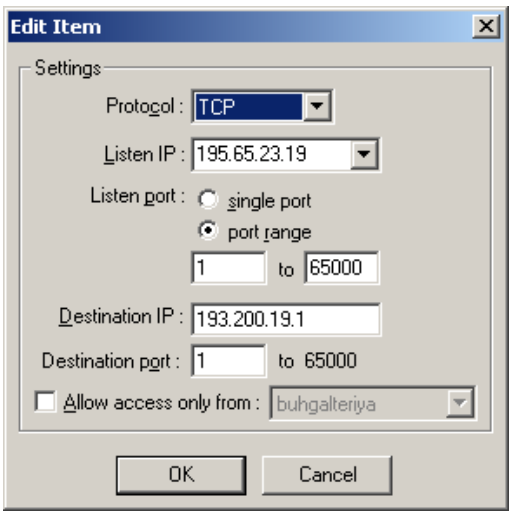


Рис. 12 Список заданных правил для пакетного фильтра

Шаг 3: осуществим планирование портов.



Планирование портов обеспечивает повышенную безопасность для серверов. Использование планирования портов позволит сохранить конфиденциальность хоста маршрутизатора. Реализация такой возможности снижает риск атаки хакеров. Необходимо выбрать пункт меню Port-Mapping, в результате чего должно появиться окно с одноимённым названием. Для добавления новой записи нажмите на кнопку Add. Появится окно для добавления новой записи Edit Item (Рис. 13).

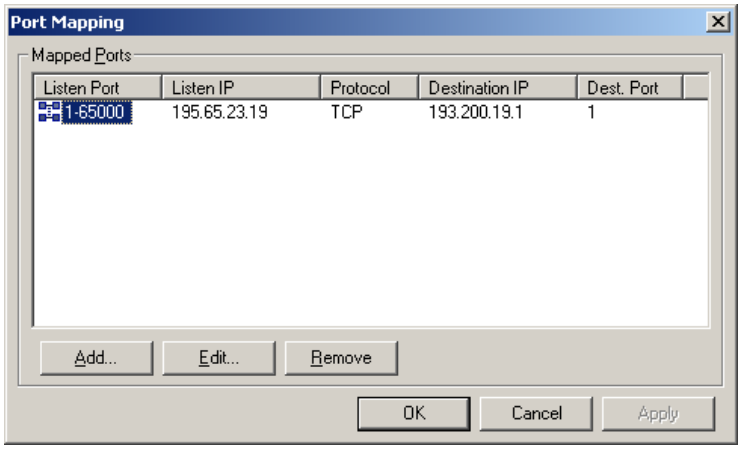


Рис. 13 Осуществление планирования портов

Использование служб сертификации, станет наиболее приемлемым и оправданным методом обеспечения безопасности при передаче данных через Интернет.

Службы сертификации предоставляют собой настраиваемые службы для выдачи сертификатов и управления ими. Последние используются в системах защиты данных, построенных на технологии открытого ключа (PKI). Установку центра сертификации планируется осуществить в центральном офисе на сервере 2.

Есть несколько причин, по которым в организации следует внедрять PKI с помощью Windows:

1) Надежная защита. С помощью смарт-карт обеспечивается надежная проверка подлинности. Также обеспечивается конфиденциальность и целостность передаваемых данных в сетях общего доступа с помощью безопасности протокола IP, а также конфиденциальность сохраненных данных с помощью шифрованной файловой системы.

2) Более простое администрирование. Организация может выдавать сертификаты и при помощи других технологий исключать использование паролей. Сертификаты могут быть отозваны при необходимости и опубликованы в списках отзыва сертификатов (CRL). Это позволяет использовать сертификаты для масштабирования доверительных отношений на предприятии. Кроме того, можно воспользоваться преимуществами интеграции служб сертификации со службой каталогов Active Directory и политикой. Также доступна возможность сопоставления сертификатов с пользовательскими учетными записями.

3) Дополнительные возможности. Имеется возможность безопасного обмена данными и файлами с помощью сетей общего доступа, таких

как Интернет. Можно использовать безопасную электронную почту с помощью протокола S/MIME и безопасные веб-подключения с помощью протоколов SSL и TLS. Кроме того, можно повысить уровень безопасности беспроводных сетей.

В семействе Windows Server 2019 Standard предоставляются следующие возможности внедрения в организации инфраструктуры открытого ключа:

- Сертификаты. Сертификат представляет из себя цифровое выражение, выданное центром сертификации, подтверждающее личность его владельца. Сертификат связывает открытый ключ с пользователем, компьютером или службой, имеющими соответствующий закрытый ключ. Сертификаты используются различными службами безопасности открытого ключа и приложениями, обеспечивающими проверку подлинности, целостность данных и безопасность коммуникаций в таких сетях, как Интернет.

В процессах, связанных с сертификатами, в Windows используется стандартный формат сертификатов X.509v3. Сертификат X.509 содержит сведения о лице или объекте, которому выдан сертификат, сведения о самом сертификате, а также дополнительные сведения о выдавшем его центре сертификации. Сведения об объекте могут включать имя объекта, открытый ключ и алгоритм открытого ключа. Пользователи могут управлять сертификатами с помощью консоли MMC «Сертификаты». Кроме того, для автоматического управления сертификатами пользователи могут воспользоваться автоматическим получением сертификатов.

- Службы сертификации. В системах Windows Server 2019 Standard Datacenter Edition службы сертификации являются компонентом, который используется для создания и управления центрами сертификации (ЦС). ЦС отвечает за установление и подтверждение подлинности владельцев сертификатов. ЦС также отзывает сертификаты, ставшие недействительными, и публикует лист отзыва для проверки сертификатов. Самая простая инфраструктура открытого ключа имеет только один корневой центр сертификации. Тем не менее, на практике большинство организаций, внедряющих инфраструктуру открытого ключа, используют несколько центров сертификации, организованных в иерархии сертификации.

Администраторы могут управлять службами сертификации с помощью консоли MMC «Центр сертификации».

- Шаблоны сертификатов. Сертификаты выдаются ЦС на основе представленных в запросе сертификата сведений и настроек, содержащихся в шаблоне сертификата. Шаблон сертификата — это набор правил и настроек, которые применяются ко всем приходящим запросам сертификатов. Такой шаблон должен быть настроен для каждого типа выдаваемых ЦС сертификатов.

Шаблоны сертификатов настраиваются в корпоративных ЦС систем Windows Server 2019 Standard и хранятся в Active Directory для использования всеми ЦС. Это позволяет администраторам выбирать один или несколько шаблонов по умолчанию, устанавливаемых со службами сертификации, или создавать новые, для конкретных задач или ролей.

Администраторы могут управлять шаблонами сертификатов с помощью консоли MMC «Шаблоны сертификатов».

- Автоматическое получение сертификатов. Автоматическая подача заявок позволяет администратору настроить субъект для выполнения автоматической подачи заявок, получения выданного сертификата, обновления сертификата с истекающим сроком годности без участия субъекта. Для этого субъекту не нужно обладать знаниями о каких-либо операциях с сертификатами, если шаблон сертификата не настроен на взаимодействие с субъектом или для CSP не нужно взаимодействие. Это намного упрощает использование клиентом сертификатов и минимизирует задачи администрирования.

Администраторы могут настраивать автоматическое получение сертификатов через настройку шаблонов сертификатов и ЦС.

- Веб-страницы, используемые для подачи заявок**.** Это отдельный компонент служб сертификации. Эти веб-страницы устанавливаются по умолчанию при настройке центра сертификации и позволяют запросившим сертификат отправлять запросы сертификатов с помощью веб-обозревателя. Веб-страницы ЦС могут быть установлены на серверы Windows, на которых не установлены центры сертификации. В этом случае веб-страницы используются для прямых запросов сертификатов в ЦС, по какой-либо причине не разрешающих прямые запросы. При создании пользовательских веб-страниц для доступа организации к ЦС можно использовать уже имеющиеся в операционной системе веб-страницы в качестве образца. Соответствующие инструкции по настройке служб сертификатов и веб-страниц центров сертификации содержатся в пакете Microsoft Platform Software Development Kit.

Поддержка смарт-карт**.** В Windows поддерживается вход в систему с помощью сертификатов на смарт-картах, а также использование смарт-карт для хранения сертификатов и закрытых ключей. Они могут быть использованы для проверки подлинности в Интернете, безопасной электронной почты, беспроводной связи и других действий, связанных с криптографией открытого ключа.

- Политики открытого ключа. Для автоматического распространения сертификатов на субъекты, установки общих доверенных центров сертификации, а также для управления политиками восстановления шифрованной файловой системы в Windows можно использовать групповую политику.

Заключение

Изложены методики настройки брандмауэра, учитывая трёхуровневую модель доступа к

данным, Правила настроек брандмауэра политики безопасности проекта суперкомпьютерной сети управления процессами социально-экономического развития. Удалось решить комплекс задач, обеспечивающих реализацию цели данной работы. Создание суперкомпьютерной сети управления процессами социально-экономического развития позволит руководству эффективно управлять, защищать и масштабировать ресурсы.

СПИСОК ЛИТЕРАТУРЫ

1.Бондарчук, В. В. Мультисервисная суперкомпьютерная сеть управления процессами социально-экономического развития [Текст] / Отв. ред. к.э.н. Герман Юрьевич Гуляев // EUROPEAN RESEARCH: сборник статей XXVI Международной научно-практической конференции – Пенза: МЦНС «Наука и Просвещение», 2020. – 218 с. – С. 39–43

2. Бондарчук, В. В. Профилактические мероприятия для обеспечения сохранности данных в суперкомпьютерной сети [Текст] / Отв. ред. к.э.н. Герман Юрьевич Гуляев // EUROPEAN SCIENTIFIC CONFERENCE. Сборник статей XX Международной научно-практической конференции – Пенза: МЦНС «Наука и Просвещение», 2020. – 386 с. – С. 82–87

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ ТЕСТИРОВАНИЯ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Воробьев Н. А.,
студент КемГУ, каф. ЮНЕСКО по ИВТ
Бурмин Л.Н.,
канд.техн.наук, доцент каф. ЮНЕСКО по ИВТ, КемГУ
Степанов Ю.А.,
д-р.техн.наук, профессор каф. ЮНЕСКО по ИВТ, КемГУ

Аннотация. Рассмотрены популярные фреймворки и библиотеки для тестирования мобильных приложений (React-Native, Android). Выявлены позитивные и негативные стороны инструментов. Проведен сравнительный анализ рассмотренных фреймворков по выбранным характеристикам.

Ключевые слова: Тестирование, фреймворки, мобильные приложения, Android, кроссплатформенная разработка

Введение

В связи с большой популяризацией мобильных приложений мы все чаще и чаще начинаем пользоваться мобильными устройствами. Такси, погода, новости, заказ еды и прочее, практически для всего уже существуют свои мобильные сервисы. А раз количество приложений растет, то растет и потребность в качестве выпускаемых приложений. Все больше компаний разработчиков более осознано подходят к тестированию своих мобильных приложений. Разработчики осознают что, если приложение имеет большую аудиторию, то цена дефекта растет, а значит необходимо использовать современные технологии для эффективного нахождения дефектов. Тесты - это тоже код, который требует подержки. Более того, код тестов должен быть прост для понимания, чтобы его можно было верифицировать визуально.В связи с этим, целесообразно инвестирование в упрощение кода тестов, избавление от дублирования и повышение читабельности. Рассмотрим наиболее популярные библиотеки, которые используются в современных IT-компаниях.

Проблема повышения качества продукта на данный момент имеет острый характер, так как ручное тестирование занимает много времени, а использование различных инструментов поможет упростить данную проблему. Рассмотрим перечень широко используемых фреймворков (программных каркасов). Для автоматизации тестирования существует две основные группы: нативные (которые были разработаны для использования на определённой платформе) и кроссплатформенные. Для первого случая мы возьмем платформу Android, а для второго рассмотрим React-Native.

1.Тестирование приложений под Android

1.1.**Unit-тестирование.** Существует два популярных фреймворка для модульного тестирования.

1.1.1.JUnit. Сам фреймворк состоит из нескольких проектов: Jupiter, Vintage, Platform. В данное статье будет рассмотрен Junit Jupiter, который является основным проектом JUnit. Он позволяет создавать тесты и свои расширения. В проекте есть свой TestEngine, который запускает тесты на JUnit платформе. Инструмент позволяет запускать тесты автоматически при каждой сборке проекта. Тем самым можно повысить качество продукта и выпускаемого функционала. Порог вхождения минимален, никаких сторонних зависимостей ставить не требуется, JUnit встраивается непосредственно в проект. В официальной документации можно найти примеры использования с лучшими практиками. Довольно просто интегрируется с другими библиотеками и фреймворками для тестирования, такими как Mockito или Espresso. У данного инструмента есть некоторые недостатки, например, нельзя тестировать зависимости и он не подходит для тестирования больших наборов тестов. К недостаткам можно отнести и малое число аннотаций, однако для небольшого проекта их хватает.