УТВЕРЖДЕНО
501540.002.58169198-02-01 31 01-ЛУ

Программно-аппаратный комплекс “Shield Multi Service - FW”

Описание применения

501540.002.58169198-02-01 31 01

Москва
2012

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

Программно-аппаратный комплекс «Shield Multi Service-FW» (ПАК «SMS-FW») разработан во исполнение Решения №61 Гостехкомиссии России от 21 октября 1997 г. «О защите информации при вхождении России в международную информационную систему «Интернет» и предназначен для построения комплексов, обеспечивающих доступ по протоколам TCP/IP пользователей защищенных вычислительных сетей к различным услугам публичных сетей (включая сеть Интернет), при отсутствии сетевого взаимодействия между защищенной и публичной сетями, в том числе:

- для автоматизированных систем (АС) органов государственного управления и организаций Российской Федерации, обрабатывающих сведения, составляющие государственную тайну, и конфиденциальную информацию;
- для систем управления транспортом, связью, энергетикой и др.

Программно-аппаратный комплекс «SMS-FW» состоит из двух серверов (внутреннего и внешнего), сопряженных между собой по шине IEEE1394, драйвера для обмена сообщениями (данными) между этими серверами и двух программных модулей (***client_sms*** и ***server_sms***), которые функционируют соответственно на внутреннем и внешнем серверах комплекса. Внутренний и внешний серверы ПАК «SMS-FW» взаимодействуют между собой через драйвер shieldhpsb.o. Драйвер shieldhpsb.o функционирует на уровне ядра операционной системы и производит обмен данными между внутренним и внешним серверами ПАК «SMS-FW» через интерфейс IEEE1394 без использования сетевых протоколов и передачи адресной информации сетевого уровня.

Программно-аппаратный комплекс «SMS-FW» функционирует под управлением операционной системы Linux с версией ядра не ниже 2.4.18.

Для ограничения доступа пользователей защищенной вычислительной сети к программно-аппаратному комплексу «SMS-FW» можно использовать как встроенные средства ПАК «SMS-FW», так и любой межсетевой экран, устанавливаемый на внутреннем сервере.

Для обеспечения максимальной безопасности внешнего сервера ПАК «SMS-FW» целесообразно установить и настроить на нем межсетевой экран.

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

ПАК «SMS-FW» позволяет строить комплексы, использующие технологию «клиент-сервер» и обеспечивающие взаимодействие компонент автоматизированных систем как по стандартным, так и по собственным протоколам.

Примерами поддерживаемых стандартных протоколов являются:

- HTTP (HTTPS) для доступа к серверам World Wide Web (WWW), создания электронных торговых площадок и т.п.;
- FTP для доступа к FTP-серверам;
- SMTP, POP3 для обмена сообщениями электронной почты между пользователями защищенных и публичных сетей;
- SSH, Telnet для удаленного администрирования и т.п.;
- использование собственных протоколов для решения различных задач, в частности, для передачи данных через публичные сети, в том числе сеть Интернет, между 2-мя защищенными сетями.

Применение ПАК «SMS-FW» позволяет также строить комплексы, обеспечивающие:

- интерактивный доступ пользователей защищенных вычислительных сетей к удаленным компьютерам публичных сетей, в том числе сети Интернет и др.;
- защиту корпоративных Web-порталов и Удостоверяющих центров;
- создание распределенных автоматизированных систем различного назначения (например, системы электронной коммерции);
- и т.п.

Для доступа к различным услугам публичных сетей с помощью ПАК «SMS-FW» не требуется изменения прикладного или системного программного обеспечения автоматизированных систем, достаточно лишь правильно настроить файл конфигурации ПАК «SMS-FW» и внести, при необходимости, изменения в сетевые настройки автоматизированной системы.

ПАК «SMS-FW» позволяет одновременно поддерживать несколько сервисов, например, обслуживать безопасный доступ к WWW-ресурсам сети Интернет и поддерживать услуги электронной почты сети Интернет.

Применение ПАК «SMS-FW» не приводит к снижению класса защищенности локальной вычислительной сети и автоматизированной системы в целом.

3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

Для построения комплексов, обеспечивающих обмен сообщениями (данными) между защищенной и публичной сетями, используется многоуровневая схема. Типовая схема комплекса для обмена сообщениями (данными) между защищенной и публичной сетями приведена на рис. 1.

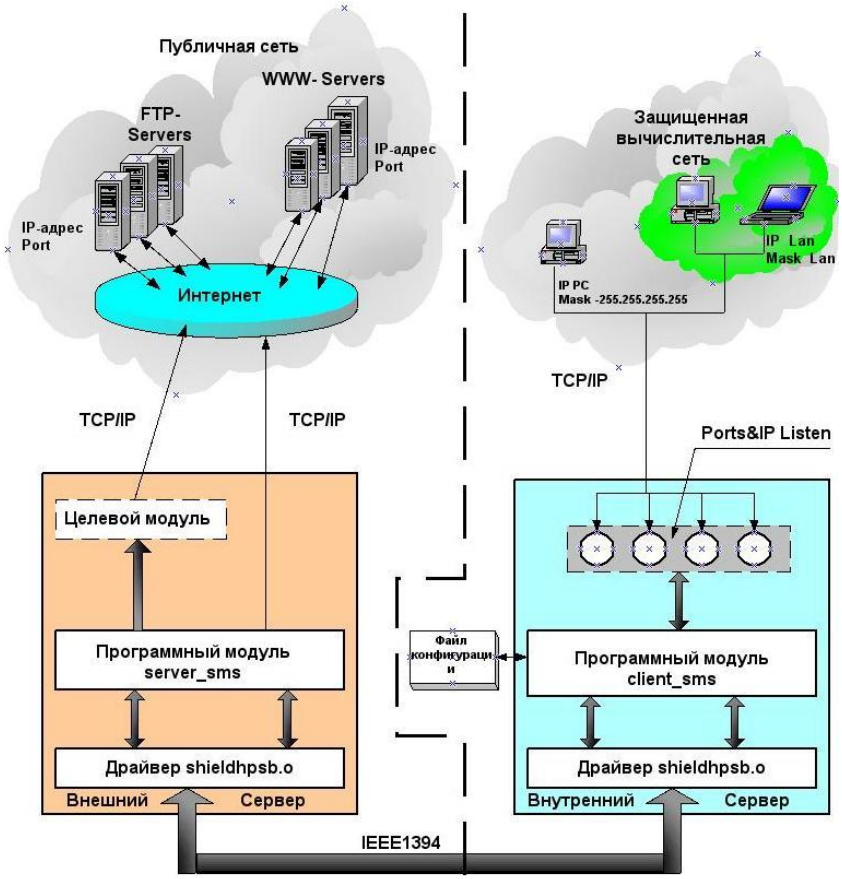

Рис. 1. Схема обмена данными в ПАК «SMS-FW»

На представленной схеме показан процесс доступа из защищенной сети к тем или иным сервисам (серверам), находящимся за пределами данной сети, например, в сети Интернет. Каждый из этих сервисов имеет свой IP-адрес (**IP remote service**) и порт (**Port remote service**), через которые он обслуживает запросы клиентов. Для доступа к тому или иному сервису на внутреннем шлюзе ПАК «SMS-FW» открываются слушающие порты (**Port client_sms Listen for remote service**). При этом каждый порт может быть закреплен за определенным IP-интерфейсом внутреннего шлюза (**IP client_sms Listen for remote service**). Когда от пользователя защищенной ЛВС приходит запрос на соответствующий порт внутреннего шлюза, то модуль **client_sms** через драйвер **shieldhpsb.o** передает модулю **server_sms**, находящемуся на внешнем сервере ПАК «SMS-FW», информацию о внешнем сервисе (**IP remote service** и **Port remote service**) и сам запрос. При этом **никакая информация о клиентском рабочем месте на внешний сервер не передается**. Модуль **server_sms**, получив данные от внутреннего сервера, от своего «имени» (от своего IP-адреса и порта) устанавливает сессию с запрошенным сервисом (**remote service**). Отметим также, что модуль **server_sms** не имеет никаких слушающих портов, поэтому доступ извне к нему невозможен. По аналогичной схеме осуществляется прием данных от сервиса и передача их клиенту: модуль **server_sms** получает данные от сервиса и через драйвер **shieldhpsb.o** передает их модулю **client_sms** без передачи какой-либо сетевой информации, а уже модуль **client_sms** от своего «имени» передает их клиенту. В отдельных случаях в качестве удаленных сервисов могут указываться так называемые целевые модули, которые могут устанавливаться непосредственно на внешнем сервере ПАК «SMS-FW». В качестве целевых модулей могут быть использованы различные системные сервисы (**squid**, **postfix** и другие). Выбор конкретного модуля зависит от функций, которые должен выполнять построенный комплекс. Например, для доступа к WEB-порталам публичных сетей на внешнем сервере может использоваться прокси-сервер **squid**, в задачу которого будет входить взаимодействие со службой **DNS** с целью разрешения имен, а для получения почты из публичных сетей на внешнем сервере может использоваться один из почтовых серверов, например, **sendmail**, **postfix** и т.д. Вся информация, необходимая для функционирования ПАК «SMS-FW», содержится в файле конфигурации **/usr/local/etc/sms.conf**.

4. ФАЙЛ КОНФИГУРАЦИИ

Файл конфигурации ***/usr/local/etc/sms.conf*** предназначен для задания правил, следуя которым можно получить доступ из защищенной ЛВС к тем или иным информационным ресурсам другой сети, включая сеть Интернет. Этот файл создается на внутреннем сервере ПАК «SMS-FW», где исполняется программный модуль ***client_sms***. Файл конфигурации представляет собой текстовый файл. Каждая строка файла конфигурации состоит из одиннадцати полей, из которых обязательными являются первые шесть полей. Поля разделяются пробелами или символами табуляции. В файле конфигурации допускаются комментарии. Строка комментария всегда начинается с символа **#**.

Первые два поля файла конфигурации определяют IP-адрес сетевого интерфейса (**IP client_sms Listen for remote service**) и порт внутреннего сервера ПАК «SMS-FW» (**Port client_sms Listen for remote service**), на котором модулем **client_sms** будут приниматься запросы от клиентов, инициирующих соединение.

Третье (IP-адрес подсети или отдельного компьютера - **IP Client**) и четвертое (маска подсети - **Mask for IP Client**) поля определяют подсеть (или отдельный компьютер), с которой могут приходить запросы на вышеуказанный IP-адрес (**IP client_sms Listen for remote service**) и порт (**Port client_sms Listen for remote service**).

Следующая пара полей определяет IP-адрес (**IP remote service**) и порт сервиса (**Port remote service**), к которому будут получать доступ клиенты и куда будут отправляться запросы с серверного шлюза ПАК «SMS-FW», поступающие на клиентский шлюз ПАК «SMS-FW» по адресу и порту, определяемым первыми двумя полями текущей строки файла конфигурации.

Седьмое поле определяет IP-адрес интерфейса внешнего сервера ПАК «SMS-FW» (**IP server_sms for connect remote service**), с адресом которого будут исходить запросы к заданному сервису.

Восьмое поле задает минимальное количество сессий (**Number sessions**), гарантированно поддерживаемых для данного сервиса.

Девятое, поле задает максимально допустимый трафик (**Volume traffik for one session**) для каждой сессии, устанавливаемой с данным сервисом.

Десятое (**Session time start**) и одиннадцатое (**Session time end**) поля определяют период времени суток, во время которого пользователи имеют возможность устанавливать сессии с удаленным сервисом, задаваемым в четвертом (**IP remote service**) и пятом (**Port remote service**) полях.

Рассмотрим более подробно описание полей файла конфигурации:

Поле1 (**IP client_sms Listen for remote service**) - IP-адрес внутреннего сервера ПАК «SMS-FW» в стандартной точечно-цифровой форме - определяет сетевой адрес интерфейса внутреннего сервера ПАК «SMS-FW», на котором программный модуль ***client_sms*** будет ожидать поступления запросов на соединение из защищенной ЛВС. Указание символа **«*»** (звездочка) в этом поле говорит о том, что будут приниматься запросы, поступающие на любой из сетевых интерфейсов внутреннего шлюза.

Поле2 (**Port client_sms Listen for remote service**) - Порт – определяет порт по заданному сетевому адресу, на котором программный модуль ***client_sms*** будет ожидать поступления запросов на соединение из защищенной вычислительной сети. Представляет собой целое положительное число от 1 до 65535. Порты с номерами меньше 1024 являются привилегированными, и их использование не рекомендуется.

Поле3 (IP Client) - IP-адрес подсети (отдельного компьютера) в стандартной точечно-цифровой форме - определяет адрес подсети (отдельного компьютера), от которой следует принимать запросы на соединение. В случае если поле содержит символ **«*»** (звездочка), будут обрабатываться все поступающие запросы. В том случае, если мы хотим для отдельных подсетей (компьютеров) определить свои правила, а для всех остальных - другое правило, то в файле конфигурации сначала прописываются конкретные правила для подсетей (отдельных компьютеров) с указанием их IP-адреса (**IP Client**), а затем - общее правило для всех остальных с указанием в качестве IP-адреса символа **«*»** (звездочка).

Поле4 (Mask for IP Client) - IP-маска подсети в стандартной точечно-цифровой форме, IP-адрес которой задан в «**Поле3**». Если в «**Поле3**» указывается IP-адрес отдельного компьютера, то в этом случае «**Поле4**» должно содержать маску следующего вида: **255.255.255.255**.

Четверка полей «**Поле1 x Поле2 x Поле3 x Поле4»** должна быть уникальна в пределах одного файла конфигурации.

Поле5 (**IP remote service**) - IP-адрес удаленного сервиса или целевого модуля в стандартной точечно-цифровой форме. Определяет IP-адрес целевого модуля или сервиса в публичной сети, по которому будут направляться запросы, поступающие на внутренний сервер ПАК «SMS-FW» на IP-адрес и порт, определяемые первой парой полей файла конфигурации.

Поле6 (**Port remote service**) - Порт – определяет порт, на котором принимает запросы удаленный сервис в публичной сети (или целевой модуль) по IP-адресу, указанному в предыдущем поле. По сути **Поле6** определяет тип сервиса, к которому будет осуществляться доступ (**80 – http**, **22 – ssh** и т.д.). Отметим особенности доступа к **ftp**-серверам (порт 21). Первая особенность состоит в том, что при доступе к **ftp**-серверам **Поле1** (**IP client_sms Listen for remote service**) всегда должно быть указано явно. Вторая и основная особенность состоит в том, что **ftp**-клиент должен всегда выступать

инициатором связи с **ftp**-сервером (**passive mode on**) для передачи/приема данных. В противном случае соединение будет отвергаться, и в системный журнал syslog будет записываться следующее сообщение: **client_sms[5775]: FTP-client: passive mode off, refused 192.168.0.155:1776**

Это связано с тем, что модуль **server_sms**, функционирующий на внешнем сервере ПАК «SMS-FW», никогда не имеет открытых слушающих (**listen**) портов.

Если в данном поле задать **0** (нуль), то все запросы, приходящие из подсети (конкретного компьютера), заданной в полях **Поле3** (**IP Client**) и **Поле4** (**Mask for IP Client**), на интерфейс, заданный в полях **Поле1** (**IP client_sms Listen for remote service**) и **Поле2** (**Port client_sms Listen for remote service**), будут отвергаться с соответствующей записью в системный журнал **syslog**.

Поле7 (**IP server_sms for connect remote service**) - IP-адрес локального интерфейса внешнего сервера ПАК «SMS-FW» в стандартной точечно-цифровой форме. Определяет локальный адрес интерфейса внешнего сервера ПАК «SMS-FW», который будет обозначен в качестве источника запроса на соединение с удаленным сервисом в публичной сети. Если поле содержит символ **«*»** (звездочка), то запрос будет отправлен с основного интерфейса внешнего сервера ПАК «SMS-FW». По умолчанию это поле содержит символ **«*»** (звездочка).

Поле8 (**Number sessions**) - минимальное количество сессий, гарантированно поддерживаемых для данного сервиса. По умолчанию это значение равно 10.

Поле9 (**Volume traffik for one session**) – максимальный трафик для данного сервиса на каждый сеанс. Трафик задается в килобайт/сек. Например, значение 100 указывает, что в рамках одного сеанса с данным сервисом может быть принято не более 100 Кбайт данных в секунду. Максимальная пропускная способность равна 10 Мбайт/сек и определяется пропускной способностью контроллера IEEE1394. Если это поле содержит символ **«*»** (звездочка) или нуль, то реальный трафик для каждой сессии определяется общей загруженностью канала IEEE1394. **Значение этого поля не может превышать величины пропускной способности канала доступа в публичную сеть, в частности, в сеть Интернет**. По умолчанию это поле содержит символ **«*»** (звездочка).

Для задания временного интервала, в течение которого будет разрешен доступ к сервису, используются 10-е и 11-ое поля. Время может задаваться в одном из следующих форматов: **[[ММ]ДД]ЧЧММ** или **[Д]ЧЧММ**.

В первом случае задается календарное время, например, **02040830** – февраль 4-ое восемь часов тридцать минут.

Во втором случае дается день недели (число от 1-го до 7-и) и время суток, например **51655** – пятница (пятый день недели) 16-ть часов 55 минут.

Поле10 (**Session time start**) – время суток, начиная с которого возможно установление сессии с удаленным сервисом. Время задается в одном из выше указанных форматов. Если в данном поле стоит символ «*» (звездочка), то пользователь может устанавливать сессию в любое время суток.

Поле11 (**Session time end**) – время, до которого пользователь вправе устанавливать сессии. По наступлению этого времени система принудительно закроет все ранее установленные сессии с удаленным сервисом, заданным в данной строке файла конфигурации (**Поле5** - **IP remote service** и **Поле6** - **Port remote service**).

Заметим, что если время задается в формате ЧЧММ, то период, в течение которого возможно установление сессии, может начинаться в одних сутках, а заканчиваться в других, например, с **2200** (**Поле10**) до **0600** (**Поле11**), т.е. с 22.00 предыдущих суток до 6.00 следующих суток.

В системе по умолчанию принято максимальное значение одновременно поддерживаемых сеансов, равное 512. Пользователь может изменить это число, задав внешнюю переменную ***SMS_MAX_CONN*** из командной строки на внутреннем сервере ПАК «SMS-FW», например:

#export SMS_MAX_CONN=1000

Максимальное значение, которое может принимать переменная ***SMS_MAX_CONN***, равно 1000.

Система резервирует из этого числа для каждого сервиса (см. **Поле8**) минимально гарантированное число сеансов. Оставшееся число сеансов динамически распределяется между всеми по принципу «первым пришел - первым обслужен». При достижении максимального числа сеансов с учетом гарантированного минимума сеансов для всех сервисов в системном журнале **syslog** будет писаться одно из следующих сообщений:

Oct 22 12:33:22 gate02int client_sms[19665]: TOO many connect=73 for service=0. Min Connect for service=5. Connect from 127.0.0.1:36606 to 192.168.0.93:80 refused

Oct 22 12:33:20 gate02int client_sms[19665]: Too many connect=512. Max Connect=512

Первое сообщение говорит о том, что нулевой сервис (первый в файле ***/usr/localetc/sms.conf***) исчерпал (установлено 73 сессии) свой гарантированный минимум (5 сессий) и система не в состоянии в данный момент открыть новую сессию, так как общее число установленных сессий достигло максимального значения.

Второе сообщение говорит о том, что установлено максимальное количество сессий (512) и открыть в данный момент новую сессию не представляется возможным.

При запуске программного комплекса «SMS-FW» программный модуль ***client_sms*** считывает файл конфигурации, и дальнейшая работа будет происходить с учетом содержимого этого файла. В системный журнал внутреннего сервера будет сделана запись о старте комплекса «SMS-FW» и будут выведены все строки файла конфигурации, например:

plusb_open okey=/proc/shieldhpsb1
plusb_open okey=/proc/shieldhpsb0
Identification started
Identification succeeded!
Shield Multi Service - FW started, copyright 2002 LISSI, http://www.lissi.ru
SMS Serial Number =0101010100010000
Using config file /usr/local/etc/sms.conf, Number services=2
Configuration table:
Listen=192.168.0.71:10021 Wait_connect from=* (mask=255.255.255.255) Connect to=127.0.0.1:21 Wait answer:* socket=1, num_connect=10, vol_traffik=100, time_start=12:01, time_end=18:03
Listen=192.168.0.71:10121 Wait_connect from=* (mask=255.255.255.255) Connect to=192.168.0.70:21 Wait answer:* socket=21, num_connect=10, vol_traffik=2000, time_start=20:00, time_end=19:00
End of configuration table. Max Connect=512, Min garanty connect=20

При поступлении запроса из защищенной сети модуль **client_sms** определяет, на какой сетевой интерфейс и порт поступил запрос (первая пара полей записи файла конфигурации) и от кого (вторая пара полей записи файла конфигурации). По этим данным из файла конфигурации будет извлечен IP-адрес удаленного сервиса (поле 5 **- IP remote service**) в публичной сети и его порт (поле 6 **- Port remote service**). Таким образом, четверка полей «**Поле1 x Поле2 x Поле3 x Поле4**» предоставляет возможность установления множественных соединений, и даже через один и тот же порт (см. **Поле2**) разные клиенты могут получать доступ к разным удаленным сервисам.

Для примера рассмотрим файл конфигурации, в котором разные клиенты получают доступ к разным удаленным сервисам (рис. 2). В соответствии с данным файлом конфигурации можно:

1) Получать и отправлять почту с почтового сервера **mail.lissi.ru**.

#e-mail
192.168.0.90 10025 * 255.255.255.0 194.135.62.117 25 * 10 10
192.168.0.90 10110 * 255.255.255.0 194.135.62.117 110 * 10 10

2) Получить доступ с IP-адреса 10.0.0.1 к удаленной системе с IP-адресом 192.168.0.60 по протоколу **ssh** .

#ssh
192.168.0.90 22 10.0.0.1 255.255.255.0 194.135.62.60 22 * 10 10

3) Получить доступ с IP-адреса 10.0.0.3 к удаленной системе с IP-адресом 192.168.0.60 по протоколу **ftp** .

#ftp
192.168.0.90 10021 10.0.03 255.255.255.0 194.135.62.60 21 * 10 10

4) Разрешить доступ всем к удаленной системе с IP-адресом 192.168.0.252 по протоколу **ftp** .

#ftp
192.168.0.90 10021 * 255.255.255.0 194.135.62.252 21 * 10 10

5) Разрешить доступ всем к удаленной системе с IP-адресом 192.168.0.252 по протоколу **telnet** .

#telnet
192.168.0.90 10023 * 255.255.255.0 194.135.62.60 23 * 10 10

6) Разрешить доступ всем к www – серверам публичной сети в период с 10.00 до 18.00.

#www
*** 3128 * 255.255.255.0 127.0.0.1 3128 * 10 10 10:00 18:00**

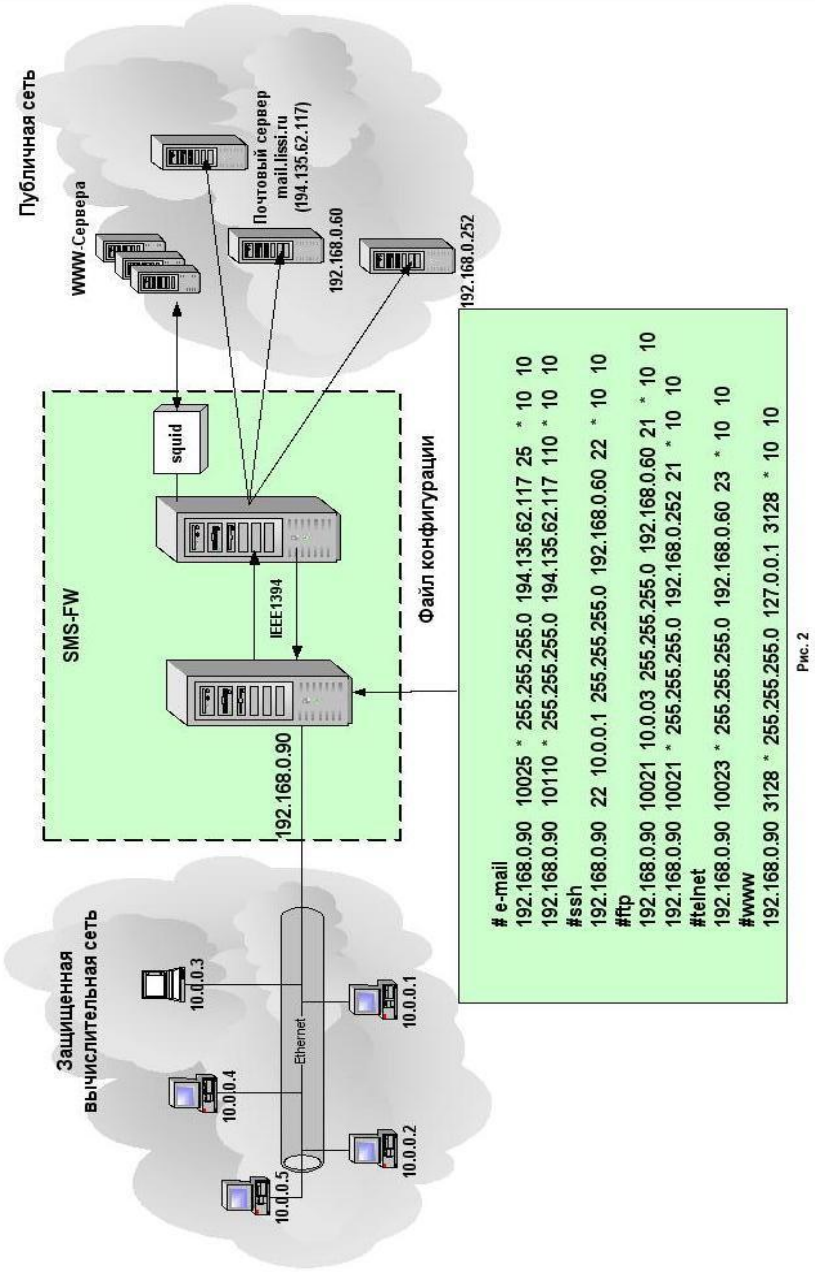

Рис. 2

Для создания и редактирования файла конфигурации можно использовать любой текстовый редактор, например, **vi**.

5. УПРАВЛЕНИЕ ПАК «SMS-FW»

5.1 Установка ПО ПАК «SMS-FW»

Программное обеспечение ПАК “SMS-FW” поставляется в виде RPM-пакетов:

- ***shield-base-1.0-1.i686.rpm*** – драйвер интерфейса IEEE1394;
- ***shield-multiservice-client-1.0-1.i686.rpm*** – ПО внутреннего сервера;
- ***shield-multiservice-server-1.0-1.i686.rpm*** – ПО внешнего сервера.

Для установки ПО необходимо:

- смонтировать компакт-диск с дистрибутивом ПО ПАК “SMS-FW” с помощью команды:
  # mount /mnt/cdrom
- На внутреннем и внешнем серверах выполнить команду:
  # rpm -ihv /mnt/cdrom/shield-base-1.0-1.i686.rpm
- На внутреннем сервере выполнить команду:
  # rpm -ihv shield-multiservice-client-1.0-1.i686.rpm
- На внешнем сервере выполнить команду:
  # rpm -ihv shield-multiservice-server-1.0-1.i686.rpm.

Все вышеприведенные команды должны выполняться от имени пользователя root.

После установки ПО следует выполнить перезагрузку серверов ПАК «SMS-FW» (команда ***reboot***) и, после того как оба сервера успешно перезагрузились, система готова к работе.

5.2. Запуск и останов ПО ПАК «SMS-FW»

Запуск программного обеспечения ПАК «SMS-FW» выполняется на внутреннем сервере путем выполнения команды:

 # service client_sms start

При старте ПАК «SMS-FW» проводится взаимная идентификация модулей ***client_sms*** и ***servert_sms*** и контроль целостности программного обеспечения с записью соответствующих данных в системный журнал **syslog**.

При успешном запуске выводится сообщение:

Starting client_sms service: [OK]

При неудачном запуске выводится сообщение:

Starting client_sms service: [FAILED]

Для остановки работы программного обеспечения ПАК «SMS-FW» необходимо выполнить на внутреннем сервере команду следующего вида:

 # service client_sms stop

При успешном останове выводится сообщение:

Shutting down client_sms service: [OK]

5.3. Перезагрузка файла конфигурации ПАК «SMS-FW»

В процессе функционирования ПАК «SMS-FW» может потребоваться перезагрузить файл конфигурации. Этого можно достичь путем последовательного выполнения команд останова и старта программного обеспечения ПАК «SMS-FW» на внутреннем сервере:

 # service client_sms stop
Shutting down client_sms service: [OK]
 # service client_sms start
Starting client_sms service: [OK]

или воспользоваться командой вида:

 # service client_sms restart

Следует иметь в виду, что такая перезагрузка файла конфигурации приводит к кратковременной остановке ПАК «SMS-FW» (в течение нескольких секунд).

ПАК «SMS-FW» позволяет осуществлять загрузку измененного файла конфигурации в реальном масштабе времени без прекращения функционирования. Для этого достаточно внести изменения в файл конфигурации ***/usr/local/etc/sms.conf*** и выполнить на внутреннем сервере, на котором функционирует программный модуль ***client_sms***, команду вида:

 # service client_sms reload

Содержимое нового файла конфигурации будет записано в системном журнале **syslog** внутреннего сервера.

5.4. Проверка состояния ПАК «SMS-FW»

Для проверки состояния программного модуля ***client_sms*** выполнить команду:

 # service client_sms status

В случае если программный модуль ***client_sms*** загружен, будет выдано сообщение:

Client_sms (pid <PID>) is running

где <PID> - идентификатор процесса ***client_sms*** в операционной системе.
В случае если программный модуль ***client_sms*** выгружен, появится сообщение:

Client_sms is stopped
Для проверки состояния программного модуля ***client_sms*** выполнить команду:

 # service server status

В случае если программный модуль ***server_sms*** загружен, будет выдано сообщение:

Server_sms (pid <PID>) is running
где <PID> - идентификатор процесса ***server_sms*** в операционной системе.
В случае если программный модуль ***server_sms*** выгружен, появится сообщение:

Server_sms is stopped

5.5. Серийный номер ПАК «SMS-FW»

Каждый ПАК «SMS-FW» обладает уникальным серийным номером, который используется самим комплексом для контроля целостности ПО и администратором при обращении в службу технической поддержки, а также для получения обновлений ПО ПАК «SMS-FW».

Серийный номер записывается в системный журнал внутреннего шлюза при успешном запуске ПАК «SMS-FW»:

```
Feb  7 11:09:49 gate02int client_sms: [18916]: SMS Serial Number: [010100010001]
```

Получить серийный номер можно также, выполнив на внутреннем сервере, в независимости от того, функционирует программное обеспечение ПАК «SMS-FW» или нет, следующую команду:

#client_sms –v

```
Shield Multi Service - FW, copyright 2002 LISSI, http://www.lissi.ru, email:
info@lissi.ru
SMS Serial Number =0101010100010000
Usage: client_sms –v | [0]|<1> [<PORT>]
#
```

6. СИСТЕМНЫЙ ЖУРНАЛ ПАК «SMS-FW»

Протоколирование работы ПАК «SMS-FW» по умолчанию ведется в системном журнале */var/log/syslog*.

При запуске ПАК «SMS-FW» в системный журнал внешнего сервера, на котором функционирует программный модуль ***server_sms***, будет выведено:

```
Feb 7 11:09:05 gate02ext server_sms[5998]: Shield Multi Service - FW started,
copyright 2002 LISSI, http://www.lissi.ru, email: info@lissi.ru
Feb  7 11:09:05 gate02ext server_sms[6002]: plusb_open okey=/proc/shieldhpsb0
Feb  7 11:09:05 gate02ext server_sms[5998]: plusb_open okey=/proc/shieldhpsb1
Feb  7 11:09:05 gate02ext server_sms: server_sms startup succeeded
```

После успешного старта ПАК «SMS-FW» в системный журнал на внутреннем сервере, на котором функционирует программный модуль ***client_sms***, будет выведено:

```
Feb   7 11:09:48 gate02int client_sms: client_sms startup succeeded
Feb  7 11:09:49 gate02int client_sms: [18911]: plusb_open okey=/proc/shieldhpsb1
Feb  7 11:09:49 gate02int client_sms: [18916]: plusb_open okey=/proc/shieldhpsb0
Feb  7 11:09:49 gate02int client_sms: [18911]: Identification started
Feb  7 11:09:49 gate02int client_sms: [18916]: identification succeeded!
Feb  7 11:09:49 gate02int client_sms: [18916]: Shield Multi Service - FW started,
copyright 2002 LISSI, http://www.lissi.ru, email: info@lissi.ru
Feb  7 11:09:49 gate02int client_sms: [18916]: SMS Serial Number: [010100010001]
```

В системный журнал на внешнем сервере при успешной идентификации программного обеспечения ПАК «SMS-FW» будет выведено:

```
Feb 7 11:09:21 gate02ext server_sms[5998]: server_sms:Start identification
Feb 7 11:09:21 gate02ext server_sms[6002]: server_sms:End identification
```

В системный журнал на внутреннем сервере при успешной идентификации программного обеспечения ПАК «SMS-FW» будет выведено:

```
Nov 3 18:52:37 host1-90 client_sms[2038]: Identification succeeded!
```

В случае неудачной идентификации программного обеспечения ПАК «SMS-FW» в системный журнал на внутреннем сервере будет сделана запись следующего вида:

```
Feb  7 11:09:49 gate02int client_sms: [18911]: Bad identification
```

и программное обеспечение на обоих компьютерах будет остановлено. Это говорит о том, что нарушена лицензия на использование ПАК «SMS-FW» либо был сбой при установке программного обеспечения.

После успешного старта ПАК «SMS-FW» или перезагрузки файла конфигурации (см. п. 5.3) в системный журнал на внутреннем сервере будет выведена информация о файле конфигурации:

```
Nov  5 21:01:44 host1-90 client_sms[3874]: Using config file
/usr/local/etc/sms.conf, Number services=5
Nov  5 21:01:44 host1-90 client_sms[3874]: Configuration table:
Nov  5 21:01:44 host1-90 client_sms[3874]: Listen=*:10080 Wait_connect from=*
(mask=255.255.255.255) Connect to=127.0.0.1:80 Wait answer:* f_d_sockfd=1,
num_connect=5, vol_traffik=10, time_start=12:01, time_end=18:03
Nov  5 21:01:44 host1-90 client_sms[3874]: Listen=*:10022 Wait_connect from=*
(mask=255.255.255.255) Connect to=192.168.0.60:22 Wait answer:0 f_d_sockfd=19,
num_connect=3, vol_traffik=100, time_start=20:01, time_end=06:03
Nov  5 21:01:44 host1-90 client_sms[3874]: Listen=*:10022 Wait_connect
from=192.168.0.252 (mask=255.255.255.255) Connect to=192.168.0.60:22 Wait answer:0
f_d_sockfd=20, num_connect=3, vol_traffik=100, time_start=-1:-1, time_end=-1:-1
Nov  5 21:01:44 host1-90 client_sms[3874]: Listen=192.168.0.90:10021 Wait_connect
from=* (mask=255.255.255.255) Connect to=192.168.0.252:21 Wait answer:*
f_d_sockfd=21, num_connect=3, vol_traffik=100, time_start=-1:-1, time_end=-1:-1
Nov  5 21:01:44 host1-90 client_sms[3874]: End of configuration table. Max Connect=500, Min garanty
connect=14
```

Заметим, если **time_start=-1:-1**, то это обозначает только то, что доступ к этому сервису разрешен в любое время суток (в **поле10 – Session time start** задан символ *).

При останове программного обеспечения ПАК «SMS-FW» в системные журналы будут выведены следующие сообщения:

```
Feb  7 13:26:14 gate02ext server_sms[6002]: plusb_close okey
Feb  7 13:26:16 gate02ext server_sms[5998]: plusb_close okey
Feb  7 13:26:16 gate02ext server_sms[5998]: Server_sms: Stopped
и
Feb  7 13:26:39 gate02int client_sms: [18916]: plusb_close okey
Feb  7 13:26:41 gate02int client_sms: [18911]: plusb_close okey
Feb  7 13:26:39 gate02int client_sms: [18911]: client_sms: Stopped
```

В процессе функционирования ПАК «SMS-FW» в системный журнал на внутреннем сервере выводится следующая информация:

- при успешном подключении пользовательской программы

```
Feb  7 13:26:00 gate02int client_sms: [20049]: New connection from 127.0.0.1 to
gate02int.lissi:10000, socket=18
```

- при закрытии сеанса

```
Feb  7 13:26:00 gate02int client_sms: [20049]: Connection closed for socket=18.
```

- общее число активных сеансов

```
Feb  7 13:26:00 gate02int client_sms: [18916]: Total 83 active connections now.
```

- превышение числа максимально допустимых сессий

```
Oct 22 12:33:22 gate02int client_sms[19665]: TOO many connect=73 for service=0.
Min Connect for service=5. Connect from 127.0.0.1:36606 to 192.168.0.93:80 refused

Oct 22 12:33:20 gate02int client_sms[19665]: Too many connect=512. Max Connect=512
```

- при попытке несанкционированного доступа к ПАК «SMS-FW»

```
Feb  7 11:10:34 gate02int client_sms: [18908]: access from 127.0.0.1 to port 60100
denied
```

- при попытке доступа к ПАК «SMS-FW» в неразрешенный период суток

```
Jan 17 13:32:26 CLIENT_SMS client_sms[10872]: Cannot access from 192.168.0.71 to
port 10022 for current time 13:32
```

- если установлена ftp-сессия и клиент переходит в режим **passive off**

```
Nov  2 13:51:59 host1-90 client_sms[5775]: FTP-client: passive mode off, refused
192.168.0.155:1776
```

- если установлена сессия и истек период времени доступа к данному сервису

```
Jan 17 13:43:00 CLIENT_SMS client_sms[10946]: Connection close for socket=29, time
end
```

В системный журнал ***syslog*** внешнего сервера, на котором функционирует программный модуль ***server_sms***, в процессе функционирования выводится информация о том, к какому внешнему сервису идет обращение:

```
Feb  7 13:25:31 gate02ext server_sms[5998]: connect to 127.0.0.1:80 from  socket 6
(Client socket=18) , traffik=100K.
```

а при завершении сеанса - сообщение о закрытии сессии:

```
Feb  7 13:25:39 gate02ext server_sms[5998]: Connection to 127.0.0.1:80 from
socket 6 closed
```

7. ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ ПАК «SMS-FW»

7.1. Организация доступа к Web-сайтам публичной сети через Web-броузер

7.1.1. Схема организации доступа к Web-сайтам

Для доступа к любым WWW-ресурсам публичных сетей из защищенной вычислительной сети на внешнем сервере ПАК «SMS-FW» целесообразно установить в качестве целевого модуля прокси-сервер. В качестве прокси-сервера используется программный комплекс **squid**. Прокси-сервер **squid** устанавливается на внешнем сервере ПАК «SMS-FW» (**IP remote service = 127.0.0.1**), прежде всего, для взаимодействия со службой **DNS** в публичной сети с целью разрешения имен (см. п. 3).

Схема работы ПАК «SMS-FW» при организации доступа из защищенной сети к WWW-ресурсам сети Интернет (рис. 3) выглядит следующим образом.

На внутреннем сервере ПАК «SMS-FW» с IP-адресом 192.168.0.88 (**IP client_sms Listen for remote service=192.168.0.88**) работает программный модуль ***client_sms***, принимающий запросы от пользователей защищенной ЛВС, например, на tcp порт 3128 (**Port client_sms Listen for remote service=3128**). Ограничений на входящие запросы не накладывается (**IP Client = ***). Таким образом, строка файла конфигурации будет выглядеть следующим образом:

#Строка файла конфигурации для доступа к squid
192.168.0.90 3128 * 255.255.255.255 127.0.0.1 3128 * 100 32

На внешнем сервере работает программный модуль ПАК «SMS-FW» ***server_sms***, который обращается к прокси-серверу **squid**, установленному также на внешнем сервере и принимающему соединения по умолчанию на tcp порт **3128** (**Port remote service = 3128**). Прокси-сервер **squid** уже в свою очередь перенаправляет запрос на удаленный сервис в публичной сети (сети Интернет). Отметим, что для корректной работы прокси-сервера **squid** на внешнем сервере, естественно, должен быть прописан **DNS**-сервер.

При получении ответа из публичной сети прокси-сервер на внешнем сервере отправляет полученные данные модулю ***server_sms***, который передает их на внутренний сервер через драйвер шины IEEE1394. На внутреннем сервере данные (ответ на запрос) принимаются модулем ***client_sms*** и передаются клиенту в защищенной сети.

Отметим, что прокси-сервер **squid** позволяет применять различные правила по доступу (**access control list** – списки контроля доступа) к тем или иным ресурсам сети, в частности, например, запрещать доступ к тем или иным серверам, ограничивать доступ по времени и т.д. Списки контроля доступа хранятся в файле конфигурации **/etc/squid/squid.conf**. В нем же можно найти подробную информацию по работе со списками контроля. Официальная документация на прокси-сервер squid доступна по адресу **http://www.squid-cache.org**.

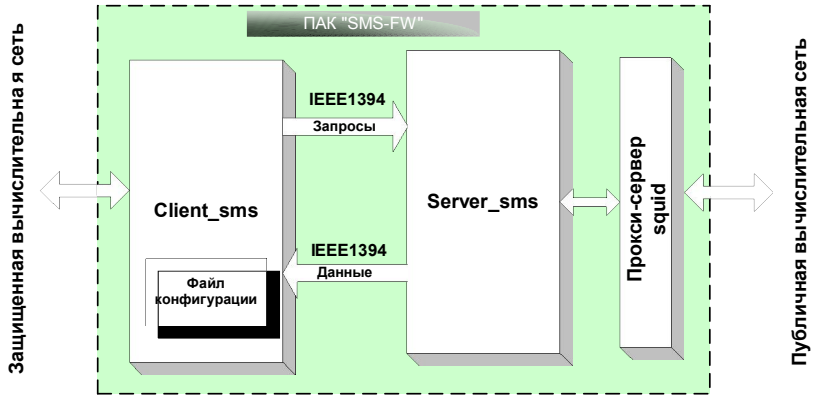

Рис. 3. Схема организации доступа к Web-ресурсам сети Интернет

7.1.2. Настройка клиентских программ в защищенной вычислительной сети

В качестве примера рассмотрим настройку WEB-броузера Internet Explorer операционной системы Windows (см. рис. 4). Настройка осуществляется в следующей последовательности:

- запустить WEB-броузер Internet Explorer;
- последовательно выбрать пункты меню Internet Explorer: Tools > Internet Option > Connection > LAN settings;
- в поле <адрес прокси-сервера> указать IP-адрес внутреннего сервера ПАК «SMS-FW» (**IP client_sms Listen for remote service**), на котором установлен программный модуль ***client_sms*** (например, 192.168.0. 90), а в поле <порт> – номер порта (**Port client_sms Listen for remote service**), на котором ***client_sms*** ожидает запросы (например, 3128).

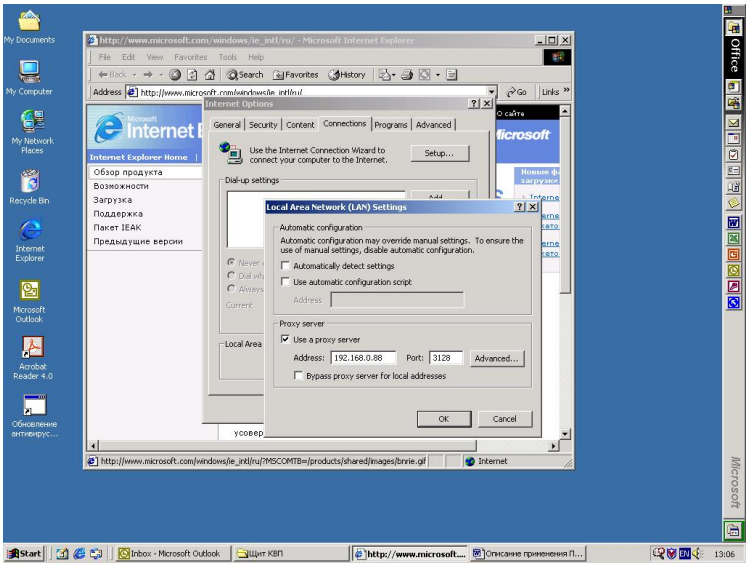

Рис. 4. Настройка WEB-броузера Internet Explorer

7.1.3. Пример использования

7.1.3.1. Запуск программного обеспечения ПАК «SMS-FW»

1. Запустить на внешнем сервере прокси-сервер **squid**. Для этого выполнить команду:

   # service squid start

   Напомним, что **squid** по умолчанию принимает запросы на порт 3128.

2. Стартовать ПАК «SMS-FW». Для этого на внутреннем сервере выполнить команду:

   # service client_sms start

7.1.3.2. Получение доступа к Web-ресурсам

Настроить WEB-броузер персонального компьютера (Internet Explorer, Konqueror и т.п.) защищенной вычислительной сети для работы с ПАК «SMS-FW» (см. п. 7.1.2).

В поле Address WEB-броузера Internet Explorer персонального компьютера защищенной вычислительной сети ввести адрес некоторого WWW-сервера публичной сети (например, **www.lissi.ru**). Результатом выполнения команды является появление в окне **WEB**-броузера запрошенной HTML-страницы (рис. 5).

Рис. 5. Доступ к WWW-серверу

7.1.3.3. Получение доступа к FTP-ресурсам публичной сети

1. Настроить WEB-броузер персонального компьютера (Internet Explorer, Konqueror и т.п.) защищенной вычислительной сети для работы с ПАК «SMS-FW», если он не был настроен ранее.

2. В поле Address WEB-броузера Internet Explorer персонального компьютера защищенной ВС ввести адрес некоторого FTP-сервера публичной сети (например, ftp://ftp.kde.org).

Переместить файл с FTP-сервера публичной сети на персональный компьютер защищенной вычислительной сети.

7.2. Организация обмена сообщениями электронной почты между защищенной сетью и сетью Интернет

7.2.1. Схема организации обмена сообщениями электронной почты

Можно предложить несколько схем организации использования внешней электронной почты клиентами защищенной ЛВС. Простейшая из них (см. рис. 6), когда почтовый сервер организации находится в публичной сети и нужно обеспечить отправку и получение почты клиентам защищенной ЛВС. При этом отдельным сотрудникам может быть разрешена только отправка почты, другим - только прием, а третьи могут пользоваться почтой без ограничений.

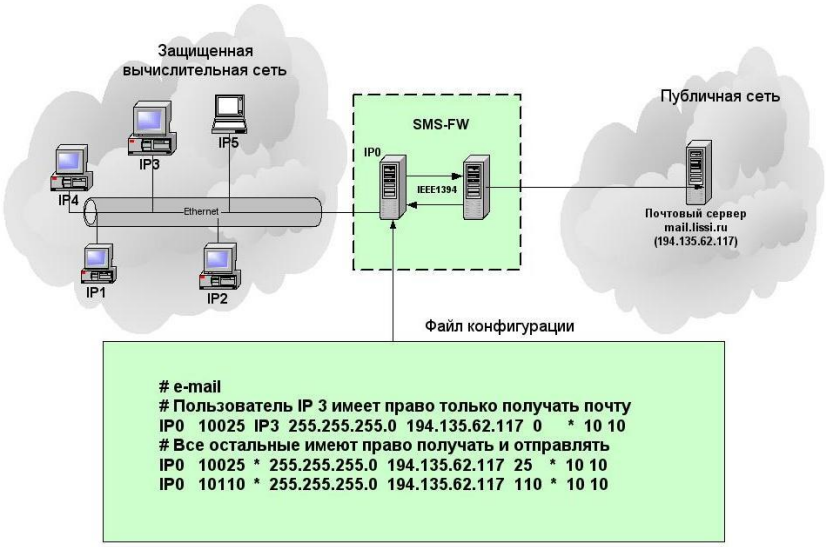

Рис. 6. Схема организации доступа к услугам электронной почты сети Интернет

Файл конфигурации для использования публичной электронной почты состоит, по крайней мере, из двух строк: одна предназначена для передачи электронных писем внешнему почтовому серверу, а вторая - для получения писем от почтового сервера. Подчеркнем, что адрес публичного почтового сервера в файле конфигурации должен указываться явно в стандартной точечно-цифровой форме. Если для отправки писем используется протокол **smtp**, то необходимо обеспечить доступ к **25-му** порту почтового сервера (вторая строка файла конфигурации), а для получения писем по протоколу **pop3** требуется обеспечить доступ к **110-ому** порту внешнего почтового сервера (третья строка файла конфигурации). В данном примере первая строка в файле конфигурации запрещает отправлять почту с компьютера с IP-адресом **IP3**.

Следует иметь в виду, что в функции ПАК «SMS-FW» не входит поиск вирусов в письмах или их контекстный анализ. Для этого должны применяться специализированные средства.

7.3. Совместное использование услуг сети Интернет

Одновременное использование нескольких услуг внешней сети по отношению к защищенной, в частности, доступа к WWW-серверам, электронной почты, доступа по протоколу ssh к внешнему серверу ПАК «SMS-FW» достигается записью в файл конфигурации ПАК «SMS-FW» соответствующих строк.

Ниже приведен пример файла конфигурации, объединяющий все выше рассмотренные примеры:

```
# e-mail
192.168.0.90  10025 * 255.255.255.0 194.135.62.117 25  * 10  10
192.168.0.90  10110 * 255.255.255.0 194.135.62.117 110 * 10  10
#ssh
192.168.0.90  22 10.0.0.1 255.255.255.0 192.168.0.60 22  * 10  10
#ftp
192.168.0.90 10021 10.0.03 255.255.255.0 192.168.0.60 21  * 10  10
192.168.0.90 10021 * 255.255.255.0 192.168.0.252 21  * 10  10
#telnet
192.168.0.90 10023 * 255.255.255.0 192.168.0.60 23  * 10  10
#www
192.168.0.90 3128 * 255.255.255.0 127.0.0.1 3128  * 10  10
```

Рис. 7. Файл конфигурации для ПАК «SMS-FW»