Министерство связи и массовых коммуникаций Российской Федерации

Государственное образовательное учреждение высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара

Федеральное агентство связи

Государственное образовательное учреждение высшего профессионального образования

Поволжская государственная академия телекоммуникаций и информатики

Кафедра передачи дискретных сообщений

КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ “ИЗУЧЕНИЕ VPN НА ОСНОВЕ КОМПЛЕКСА VIPNET”

(часть 3)

для студентов, обучающихся по специальностям 210403,210404,210406

Составители: к.т.н., доцент Крыжановский А.В.

. к.т.н., доцент Киреева Н.В.

к.т.н., доцент Пугин В.В.

Редактор: д.т.н., профессор Лихтциндер Б.Я.

Рецензент: д.т.н., профессор Карташевский В.Г

Самара 2008

Содержание

Лабораторная работа №5
«Установка и настройка Защищённого Рабочего Места ViPNet [Клиент]»

1 Цель работы

Основной целью данного занятия является получение опыта работы и администрирования АП с установленным ПО ViPNet [Клиент].

2 Состав ПО Защищённого Рабочего Места ViPNet [Клиент]

ViPNet [Клиент] обеспечивает защиту информации при ее передаче в сеть, а также защиту от доступа к ресурсам компьютера и атак на него из локальных и глобальных сетей. При этом ViPNet [Клиент] может быть установлен как на рабочую станцию (мобильную, удаленную, локальную), так и на всевозможные типы серверов (баз данных, файл-серверов, WWW, FTP, SMTP, SQL и пр.) с целью обеспечения безопасных режимов их использования.

ViPNet [Клиент] - модуль, реализующий на рабочем месте следующие функции:

1) Персональный сетевой экран - позволяет защитить компьютер от попыток несанкционированного доступа, как из глобальной, так и из локальной сети.

Персональный сетевой экран позволяет системному администратору или пользователю (при наличии присвоенных ему полномочий):

- управлять доступом к данным компьютера из локальной или глобальной сети;
- определять адреса злоумышленников, пытающихся получить доступ к информации на Вашем компьютере;
- обеспечивать режим установления соединений с другими открытыми узлами локальной или глобальной сети только по инициативе пользователя, при этом компьютер пользователя остается «невидимым» для открытых узлов локальной и глобальной сетей (технология Stealth), что исключает

возможность запуска по инициативе извне всевозможных программ «шпионов»;

- формировать «черные» и «белые» списки узлов открытой сети, соединение с которыми соответственно «запрещено» или «разрешено»;
- осуществлять фильтрацию трафика по типам сервисов и протоколов для данного адреса открытой сети или диапазона адресов, что позволяет, в случае необходимости, ограничить использование «опасных» сервисов на «сомнительных» узлах открытой сети;
- осуществлять фильтрацию трафика по типам сервисов и протоколов для связанных с данным узлом других защищенных узлов;

- контролировать активность сетевых приложений на данном компьютере, где установлен ViPNet [Клиент], что позволяет вовремя обнаружить и заблокировать активность несанкционированно установленных и запущенных программ «шпионов», которые могут передавать злоумышленникам сведения об информации, обрабатываемой на данном компьютере (пароли доступа, данные о кредитных картах, идентификаторы для доступа в корпоративные базы данных и др.);

2) Установление защищенных соединений между компьютерами, оснащенными ViPNet [Клиент], для любых стандартных сетевых приложений.

Для любых сетевых приложений обеспечиваются следующие основные функции: - шифрование IP-пакетов с добавлением в них информации для обеспечения целостности, контроля времени, идентификации (авторизации) и скрытия первоначальной структуры пакета;

- блокировка шифрованных пакетов при нарушении их целостности, превышении допустимой разницы между временем отправки и текущим временем (защита от переповторов) или при невозможности аутентифицировать пакет;

- предоставление COM интерфейса для вызова криптографических функций и их использования Web приложениями.

Возможность установления защищенных соединений между компьютерами, оснащенными ViPNet [Клиент] позволяет:

- организовать схему защищенного использования всевозможных Web-приложений, в том числе Web-trading, Web-ordering, Web-хостинга, Web-вещания и т.д., с доступом к Web-платформе, на которой

установлен ViPNet [Клиент], только определенному списку участников VPN. Данная схема обеспечивает пользователям и корпорации гибкое и безопасное использование всевозможных Web-приложений как наиболее простого и доступного средства коллективной работы корпорации и ее партнеров;

- защитить и дополнительно авторизовать все соединения между локальными, мобильными и удаленными пользователями, оснащенными ViPNet [Клиентом], и корпоративными серверами приложений, баз данных, SQL-серверами, также оснащенными ViPNet [Клиентом]. Это открывает широкие возможности по безопасному внедрению всевозможных ERP-систем, финансово-учетных систем, работающих в реальном времени, систем типа «Клиент-Банк», «Интернет-Банкинг», CRM

(Customer Relationship Management) систем и прочих систем, где с одной стороны накапливается конфиденциальная информация, требующая соблюдения правил информационной безопасности и

управления доступом, а с другой стороны необходима коллективная работа с приложениями на сети разных категорий пользователей;

- использовать недорогие и общедоступные сетевые ресурсы открытой сети для передачи конфиденциальной информации;

3) Услуги защищенных служб реального времени для организации обмена сообщениями, проведения конференций, защищенных аудио- и видео-переговоров позволяют:

- обмениваться сообщениями или организовывать циркулярный обмен сообщениями, в процессе которого организатор такого обмена видит все сообщения, в то же время участники обмена сообщений друг друга не видят. При этом ведутся и могут быть сохранены протоколы всех сообщений;
- проводить защищенные конференции;
- оперативно видеть подтверждения доставки и прочтения сообщений;
- проводить защищенные аудио- (Voice over IP) и видео-переговоры (конференции).

При этом, технология ViPNet поддерживает любые стандартные программные и аппаратные средства для проведения аудио- и видео-конференций, основанные на IP-технологиях;

4) Сервис защищенных почтовых услуг - защищенный почтовый клиент с возможностями аутентификации отправителя и получателя, а также обеспечивающий контроль за прохождением и использованием документов.

Деловая почта - модуль, входящий в состав ViPNet [Клиент], позволяет:

- передавать электронные сообщения по открытым каналам связи с защитой на всем маршруте следования от отправителя до получателя, при этом в качестве

-открытого канала могут быть использованы стандартные сервера SMTP/POP3;

- одновременно с самим сообщением защитить прикрепленные к нему файлы;
- организовать по установленным правилам защищенный автопроцессинг стандартных документов, «рождаемых» другими приложениями и системами управления бизнесом (бухгалтерскими, банковскими, управленческими и пр.);
- осуществлять поиск документа в почтовой базе документов по множеству параметров (отправитель, получатель, тема, дата, период, контекст и т.п.);
- подтверждать личность отправителя, используя электронную цифровую подпись, встроенную в общую систему безопасности;
- передать сообщение только тем получателям, для которых оно предназначалось, а также при необходимости автоматически отправить копии сообщений на заданные в ЦУС узлы;
- подтвердить получение и использование сообщений, а также дату, время получения и личности получателей;
- вести учетную нумерацию сообщений.

Кроме вышеперечисленных функций ViPNet [Клиент] предоставляет COM интерфейс для вызова криптофункций и их совместного использования с Web приложениями.

3 Межсетевые экраны (МЭ)

Существуют следующие основные классы межсетевых экранов:

- МЭ-фильтры;
- МЭ сеансового уровня;
- Прокси-МЭ.

Однако, очень немногие существующие межсетевые экраны могут быть однозначно отнесены к одному из названных типов. Как правило, МЭ совмещает в себе функции двух или трех типов. Кроме того, недавно появилась новая технология построения межсетевых экранов, объединяющая в себе положительные свойства всех трех вышеназванных типов. Эта технология была названа Statefiil inspection. И в настоящий момент практически все предлагаемые на рынке межсетевые экраны анонсируются, как относящиеся к этой категории (Stateful Inspection Firewall). При этом следует иметь ввиду, что Stateful inspection - запатентована компанией Check Point. Рассмотрим каждый из перечисленных классов отдельно:

1) МЭ-фильтр. Функциональность данного типа МСЭ заключается в применении заданного набора правил в отношении IP - адресов входящих и исходящих пакетов, в соответствии с которым анализируется трафик.

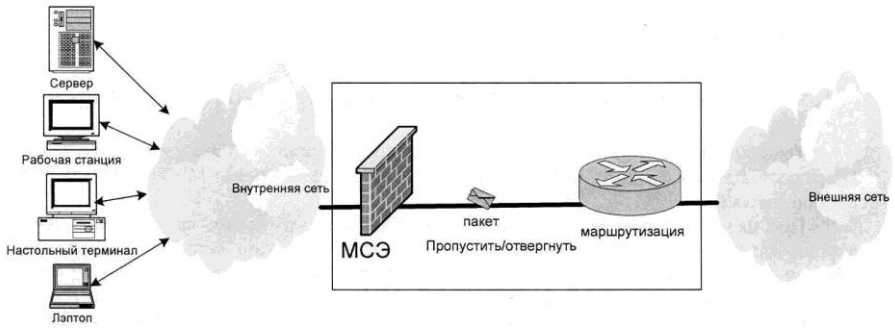

Рисунок 3.1 – Межсетевой экран

Весь анализ данных сосредоточен на транспортном уровне, т.е. для принятия решения необходима и достаточна информация сетевого и транспортного уровней исследуемого пакета. Никаких дополнительных действий, кроме анализа IP - адресов каждого отдельного пакета независимо от других и на основании этого принятия решений о разрешении/запрете прохождения пакета, не производится.

Брандмауэры данного класса являются наименее функциональными и в настоящее время в чистом виде практически не применяются. Это связано, прежде всего, с тем, что подмена IP — адресов (spoofing) не представляет никакой трудности для потенциального нарушителя.

Тем не менее, ни один МЭ не обходится без использования данной функциональности.

Функции брандмауэров данного класса могут выполнять маршрутизаторы с расширенным набором возможностей (при применении так называемой firewall feature set или firewall option pack).

2) МЭ сеансового уровня (circuit-level gateway, virtual circuit control). Особенностью данного класса МЭ является то, что помимо анализа IP — адресов (как в классе фильтрующих МЭ), осуществляется детальный настраиваемый контроль соединений, который подразумевает принятие решений на основе метаданных всех уровней вплоть до прикладного. При этом анализируются как протоколы с установкой соединения, так и без таковой (например, UDP). Для протоколов без установки соединения анализируется весь поток данных в рамках конкретного контекста. Возможен анализ архивных данных, а также большого набора смежной информации. Данная технология получила название Stateful inspection.

Технология Stateful inspection решает многие проблемы, обеспечивая полный контроль на уровне приложения без нарушения модели клиент-сервер. В случае Stateful inspection пакет перехватывается на сетевом уровне, после чего его проверкой занимается специально выделенная для этого виртуальная машина. Она извлекает информацию о контексте, необходимую для принятия решения, со всех уровней и сохраняет эту информацию в динамических таблицах для проверки последующих пакетов. Это обеспечивает решение с высоким уровнем безопасности, дающее максимальную производительность, масштабируемость и расширяемость.

При принятии решения о запрещении или разрешении прохождения пакета существенны следующие параметры соединения: длительность и время установления соединения, контекст соединения, информация об инициаторе соединения, а также об обратной стороне, прочие метаданные.

3) Прокси-МЭ (application layer gateway, application proxy). При установке соединения МЭ не является лишь только анализатором трафика с функцией контроля, - он принимает непосредственное участие в установлении соединения. Это расширяет его функциональность, которая рассредоточена на всех уровнях сетевого взаимодействия, включая прикладной.

Технология проксирования соединений значительно расширяет возможности контроля безопасности, хотя при этом незначительно замедляется скорость соединения за счет внедрения дополнительного звена.

В прокси-МЭ обычно включены возможности пакетного фильтра, а также большой набор других функций.

Как правило, корпоративный МЭ является одним из модулей программного, а чаще, программно-аппаратного комплекса защиты информации. Такие решения значительно более удобны и эффективны в связи с тем, что предоставляют ряд преимуществ перед гетерогенными системами защиты информации. Во-первых, значительно облегчается техническая поддержка и сопровождение системы, поскольку решение целиком принадлежит одной компании. Во вторых, такое решение будет заметно эффективнее системы, составленной, как набор слабо, а порой даже вовсе несовместимых модулей. В

третьих, такое решение обойдется дешевле.

Технология МЭ может также быть классифицирована по расположению модулей МЭ в системе. Встречаются такие понятия, как распределенные или персональные МЭ (distributed firewall, personal, desktop firewall).

При наличии в системе единого модуля МЭ, расположенного, чаще, на отдельно выделенной, хорошо защищенной машине, имеет место присутствие единого сетевого МЭ, настроенного таким образом, что все пакеты во внешнюю сеть проходят через него с соответствующей обработкой.

В случае модели распределенного МЭ на хостах сети (всех или некоторых) установлены модули – МЭ, реализованные в виде подсистемы, контролирующей входящий и исходящий трафик данного хоста, и осуществляющий его фильтрацию в соответствии с заранее определенными условиями. Каждый хост сети имеет индивидуальный, не зависящий от других, МЭ.

Отсюда легко определить особенности технологии распределенных МЭ:

- система сетевой защиты значительно усложняется за счет наличия большого числа компонент, установленных на хостах сети;
- усложняется централизованное управление и контроль за системой МЭ;
- часто присутствует возможность локального администрирования персонального МЭ владельцем компьютера.

Демилитаризованная зона (ДМЗ)

В соответствие с политикой безопасности большинства организаций, внутренние ресурсы компании не должны быть доступны извне. Но существует группа ресурсов, такие, как web- сервера, mail-, ftp- службы и пр., доступ к которым извне — необходим.

При организации подобного рода взаимодействия в большинстве случаев используют концепцию выделения отдельной защищенной подсети, независимой от основной, рабочей внутренней сети, т.н. Демилитаризованной зоны (Demilitarized zone, или DMZ).

Рисунок 3.2 – Демилитаризованная зона (ДМЗ)

На межсетевом экране выделяется отдельный интерфейс и задаются правила доступа в ДМЗ. При этом уровень безопасности хостов внутренней

сети не зависит от параметров настройки доступа в ДМЗ и остается прежним.

Таким образом, при помощи концепции ДМЗ хосты и информационные потоки внутренней сети - защищены, а ресурсы широкого доступа — открыты при обеспечении достаточной защищенности.

В большинстве случаев, ДМЗ надежно защищена особым набором правил МЭ. Часто используется схема построения сети, когда ДМЗ находится между двумя МЭ. В этом случае один МЭ служит первой линией обороны атак, направленных, как в саму сеть, так и в ДМЗ, а для того, чтобы достигнуть хосты внутренней сети, атакующему будет нужно преодолеть два МЭ

4 Методические указания по выполнению лабораторной работы

Описываются все шаги, необходимые для освоения ПО ViPNet [Клиент]:

- инсталляция ПО ViPNet [Клиент];
- изучение структуры каталога установки ПО ViPNet [Клиент];
- изменение ключевой информации без переинсталляции ПО;
- смена режимов работы программы Монитор;
- изучение настроек программы Монитор (меню Сервис);
- изучение настроек параметров безопасности в Мониторе и ДП;
- изучение работы с пользователями защищенной сети в Мониторе;
- изучение настроек работы через межсетевой экран;
- изучение работы с незащищенными компьютерами (Открытая Сеть);
- изучение работы с фильтрами;
- изучение журналов блокированных и IP-пакетов и их настроек;
- определение URL или IP-адреса;
- смена пользователя в Мониторе и ДП;
- настройка псевдонимов;
- работа с паролем администратора АП;
- настройки MFTP;
- обеспечение работы по Dial-Up;
- журнал конвертов MFTP;
- очередь конвертов MFTP;
- формирование нового письма, отсылка одному или нескольким адресатам;
- использование ЭЦП;
- использование прикладного шифрования писем;
- флаги упаковки, отправки, доставки и прочтения писем в ДП;
- изучение свойств письма;
- запуск внешних программ в ДП;
- настройка автопроцессинга;
- путь письма при его удалении (→ Удаленные → Аудит) в ДП;
- работа с ДП на АП, где зарегистрировано несколько коллективов;

Последовательность выполнения занятия:

Шаг 1(28)

Инсталляция ПО ViPNet [Клиент]

В каталоге **..\ViPNet [Клиент]** необходимо запустить программу инсталляции ПО ViPNet [Клиент] - файл **setup.exe.** После знакомства с лицензионным соглашением, перед Вами появится окно, в котором Вы сможете указать каталог установки, затем выбрать вид установки и компоненты (Рисунок 4.1) установки ПО ViPNet [Клиент].

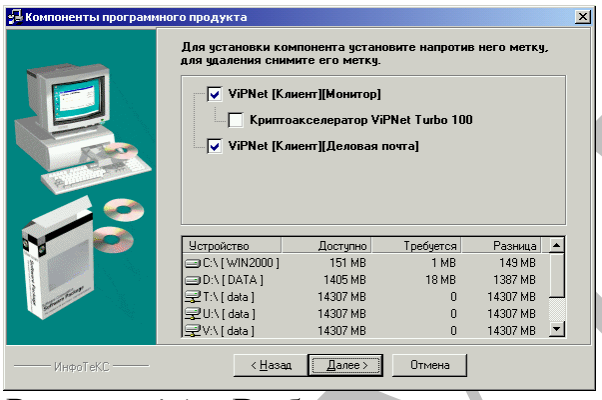

Рисунок 4.1 – Выбор типа установки

В окне выбора логического диска отображается информация о наличии свободного места на всех логических дисках Вашего компьютера и необходимого для установки ПО ViPNet [Клиент]. Убедитесь, что на выбранном логическом диске достаточно свободного места для установки.

Для завершения установки необходимо перезагрузить компьютер. Перед Вами появится приглашение ПО ViPNet [Клиент] (Рисунок 4.2) для ввода пароля. Вставьте дискету, которую Вам предоставит администратор, введите пароль и нажмите на клавишу *Принять***.**

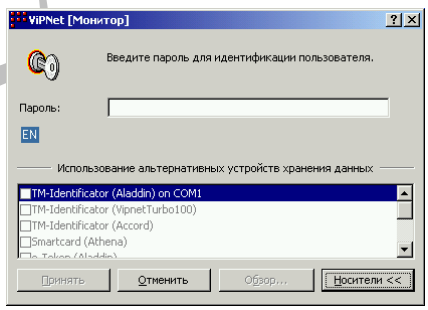

Рисунок 4.2 – Окно ввода пароля

При первом запуске, после ввода пароля, если персональная ключевая информация (КД) находится не на дискете и не в каталоге установки, необходимо воспользоваться кнопкой *Поиск ключевой папки*. При этом поиск будет производиться во всех подкаталогах указанного каталога. Например, если ключевая дискета расположена в C:\Program Files\InfoTeCS\Key_disk\, то достаточно выбрать путь C:\Program Files\InfoTeCS.

Также есть возможность записи пароля (И ТОЛЬКО ПАРОЛЯ!!!) на внешний носитель типа iButton, eToken и проч. Подробнее об этом можно узнать в документации по ViPNet.

После проверки правильности ввода пароля, Вы увидите на экране приглашение к работе, а затем - систему окон программы Монитор (Рисунок 4.3).

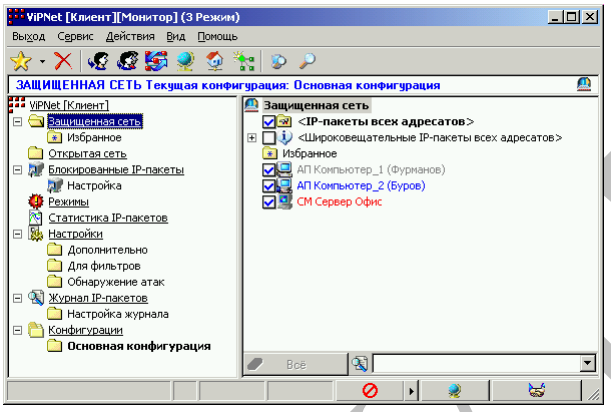

Рисунок 4.3 – Окно программы Монитор

Шаг 2(28)

Изучение структуры каталога установки ПО ViPNet [Клиент]

Каталог установки ПО ViPNet [Клиент] показан на Рисунке 4.4.

\Ccc – каталог обмена с ЦУС'ом (обновлений):

\Log – содержит файл rem**.txt,** в котором отражаются результаты проводимых обновлений;

\old - содержит старые адресные справочники, которые обновлялись;

\In, \Out, \Key, \New – рабочие каталоги.

\Database – содержит журнал IP-пакетов и файл конфигурации Монитора (**common.stg**)

\In – входящий транспортный каталог;

\Ipconfig – содержит файл с конфигурацией TCP/IP локального компьютера;

\Key_disk – ключевая дискета абонента;

\Media – файлы музыкального сопровождения событий;

\Ms – содержит файлы Деловой Почты – письма, вложения, папки;

\Out – исходящий транспортный каталог;

\Smtpin \Smtpout – входящий и исходящий транспортные каталоги при работе через SMTP/POP3 канал;

\Station – содержит ключевой набор абонента;

\Task_dir – каталог хранения файлов, подготовленных к файловому обмену и принятых по файловому обмену от других пользователей.

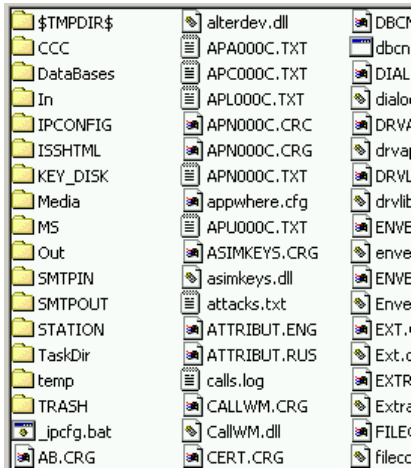

Рисунок 4.4 – Структура каталога установки.

Шаг 3(28)

Изменение ключевой информации без переинсталляции ПО

Для этого необходимо удалить каталоги, содержащие ключевую дискету (**KEY_DISK**), ключевой набор (**STATION**), адресные справочники (файлы **Apa*.txt, Apc*.txt, Apl*.txt, Apn*.txt, Apn*.crc, Apn*.crg** и **Apu*.txt** – находятся в каталоге установки ПО **ViPNet [Клиент]**) и файл лицензии **Infotecs.Re**. Если ранее производились обновления, то имена файлов, которые необходимо удалить, можно посмотреть в **\Ccc\Old.** После этого необходимо перезапустить Монитор и, с вводом пароля, указать путь к файлу ***.dst.**

Шаг 4 (28)

Смена режимов работы программы Монитор

В окне *ViPNet [Клиент]* необходимо выбрать Режимы. Поработать в каждом из режимов (Рисунок 4.5), понять, чем они отличаются и разобраться в возможностях, предоставляемых каждым режимом.

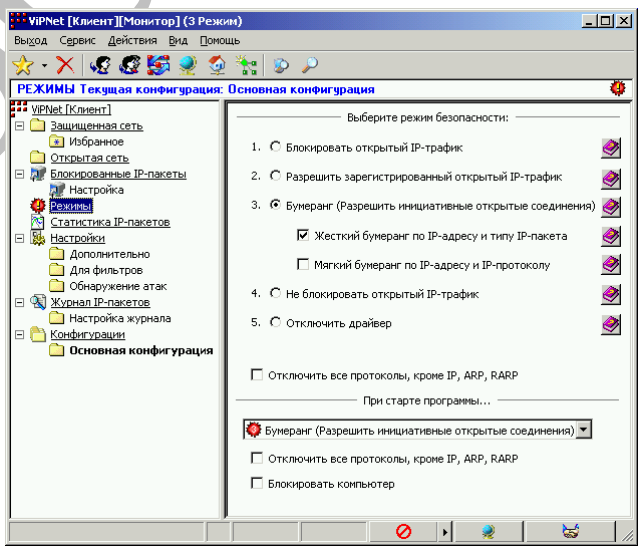

Рисунок 4.5 – Режимы безопасности

Шаг 5(28)

Изучение настроек программы Монитор (меню Сервис)

Данный пункт меню (Рисунок 4.6) позволяет настроить параметры безопасности (шаг 6), настройки транспорта, настроить вид окна *Защищенная сеть*, настроить цвета, шрифты и звуки, провести экспорт (импорт) псевдонимов и сменить пользователя СУ.

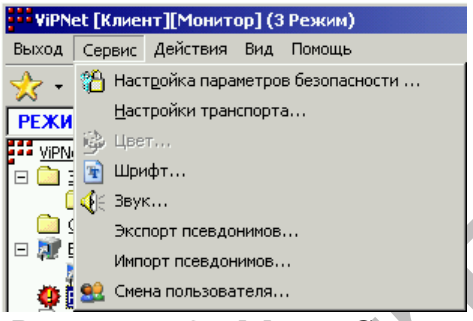

Рисунок 4.6 – Меню *Сервис*

Шаг 6 (28)

Изучение настроек параметров безопасности в Мониторе и ДП

Настройка параметров безопасности предназначена для настройки конфигурации, формирования запроса на новый сертификат ЭЦП пользователя, введения в действие сертифицированной в КЦ ЭЦП пользователя, просмотра действующего сертификата пользователя, смены пользователя и смены пароля пользователя. Выбираем пункт меню *Сервис* → *Настройка параметров безопасности* (Рисунок 4.7).

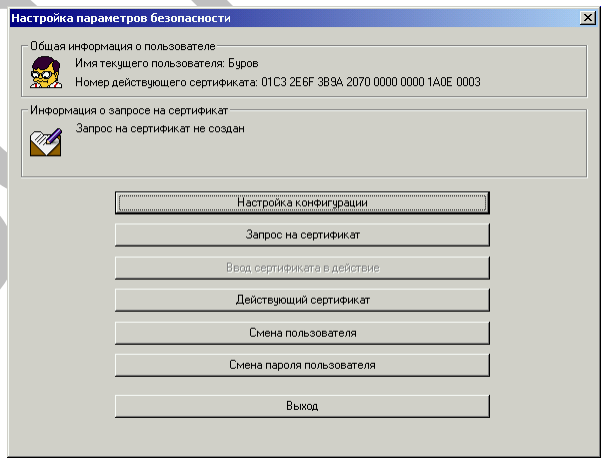

Рисунок 4.7 – Настройка параметров безопасности

По нажатию клавиши *Настройка конфигурации* перед Вами появится окно (Рисунок 4.8), в котором можно изменить срок действия новой подписи (в месяцах) и пароля пользователя (в днях), выбрать алгоритм шифрования (ГОСТ, DES, 3DES, RC6) и задать длину ключа (в байтах), разрешить смену асимметричных ключей и задать период их автоматической смены (в днях), определить тип пароля и задать параметры для случайной генерации пароля

(язык парольной фразы, количество парольных фраз, слов в фразе и букв в каждом слове).

Кнопка *Запрос на сертификат* предназначена для формирования запроса и отправки на сертификацию в КЦ нового сертификата ЭЦП абонента. В окне *Настройка параметров безопасности* (Рисунок 4.6) есть два информационных поля, в которых содержится текущая информация о сертификате подписи. Для формирования нового сертификата подписи нажимаем сначала на кнопку *Запрос на сертификат*, потом - на кнопку *Сформировать запрос* (Рисунок 4.9)**.** При этом будет выдан запрос на подтверждение формирования запроса на новый сертификат с указанием даты окончания действия текущего сертификата.

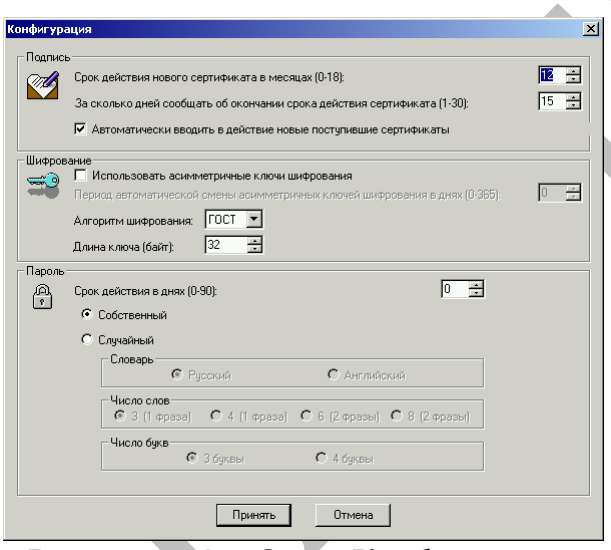

Рисунок 4.8 – Окно *Конфигурация*

Далее для формирования ключевой информации запустится *Электронная рулетка* и мы 8 раз нажмем на предлагаемые ею клавиши. В результате наших действий активируются кнопки *Посмотреть запрос* и *Отправить запрос*, которые до этого были отключены (Рисунок 4.9), а также изменится содержимое поля *Информация*, в котором будет указан срок действия сертификата, взятый из настроек конфигурации и написано, что запрос не отправлен для сертификации в КЦ (Рисунок 4.10).

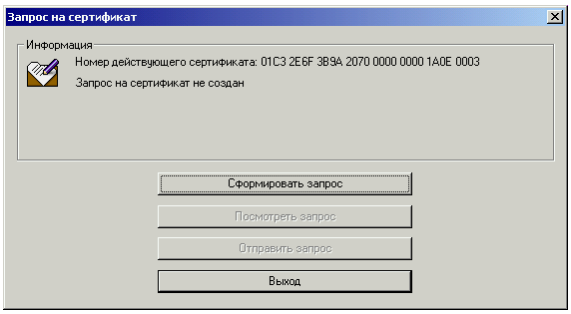

Рисунок 4.9 – Работа с подписью

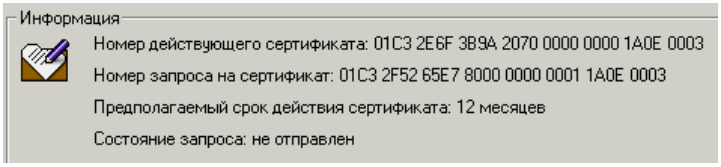

Рисунок 4.10 – Поле *Информация*

По нажатию кнопки *Посмотреть запрос*, можно посмотреть запрос на сертификат новой подписи (Рисунок 4.11). Данный образец можно сохранить в файле или распечатать, а потом сравнить с образцом сертифицированной подписи.

После формирования запрос должен быть отправлен на сертификацию в Ключевой Центр. Для этого нужно воспользоваться кнопкой *Отправить запрос* (Рисунок 4.9).

После сертификации подписи в КЦ и доставки ее абоненту, в поле *Информация о запросе на сертификат* (Рисунок 4.7) будет написано, что сертификат подписи доставлен, будет указано время и дата доставки. Теперь его необходимо ввести в действие. После нажатия одноименной клавиши (Рисунок 4.7) , открывается окно 4.10.1

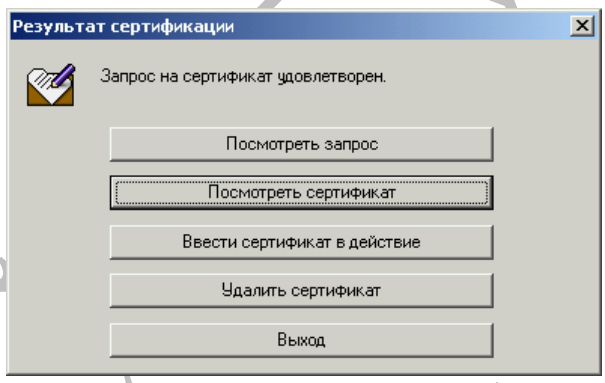

Рисунок 4.11 – Результат сертификации

Далее можно просмотреть запрос на сертификат, посмотреть сам сертификат ЭЦП (Рисунок 4.11) и распечатать его, ввести в действие .сертификат или удалить его.

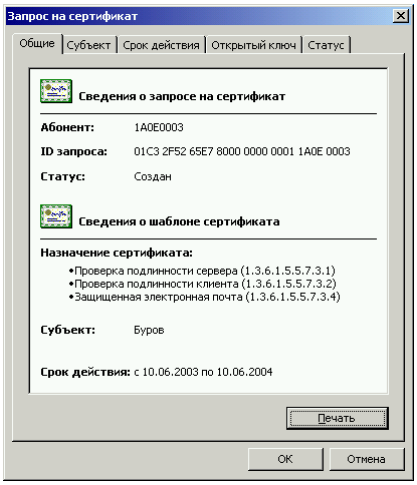

Рисунок 4.11 – ОЧ новой подписи

Смена пользователя

После нажатия одноименной кнопки (Рисунок 4.7), появится окно (Рисунок 4.2) с предложением ввести пароль нового пользователя.

Смена пароля пользователя

В зависимости от типа пароля (устанавливается в *Параметрах безопасности* (Рисунок 4.8), возможно два варианта.

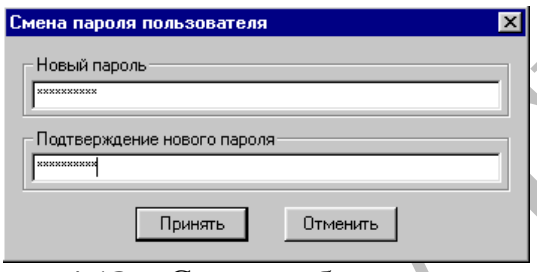

Рисунок 4.12 – Смена собственного пароля

Если тип пароля был установлен **собственный**, то откроется окно (Рисунок 4.12), в котором надо ввести придуманный Вами пароль и подтверждение правильности ввода. В случае ввода разных значений пароля программа выдаст соответствующее сообщение. Ввод пароля необходимо будет повторить.

Если тип пароля был установлен **случайный**, то после нажатия данной кнопки будет запущена программа *электронной рулетки*, если она еще не запускалась в данном сеансе работы программы Монитор, в которой 8 раз необходимо нажать на предложенные буквы. Программа автоматически сгенерирует пароль и выдаст его и парольную фразу для запоминания на экран (Рисунок 4.13).

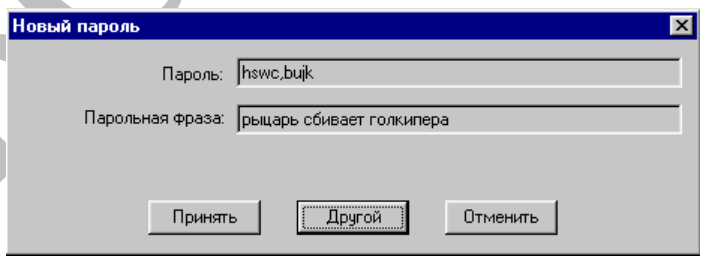

Рисунок 4.13 Пароль и парольная фраза

Если Вас устраивает сгенерированный пароль, нужно нажать на кнопку *Принять*. Если Вам не нравится пароль, можно выбрать другой, нажав на кнопку *Другой* или отказаться от смены пароля, нажав на кнопку *Отменить*.

Шаг 7(28)

Изучение работы с пользователями защищенной сети в Мониторе

Все, что можно сделать по отношению к другому пользователю защищенной сети, осуществляется установкой курсора на необходимого

пользователя и нажатием правой клавиши мыши, по которому вызывается сервисное меню (Рисунок 4.14).

Проверьте соединение (Проверить соединение) и, если оно установлено, организуйте обмен текстовыми сообщениями (Послать сообщение...), файловый обмен (Отправить файл...) и конференцию (Организовать конференцию...) (Рисунок 4.15).

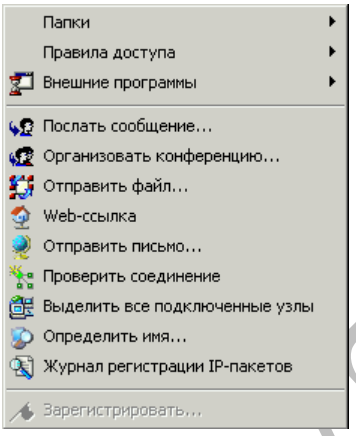

Рисунок 4.14 – Сервисное меню

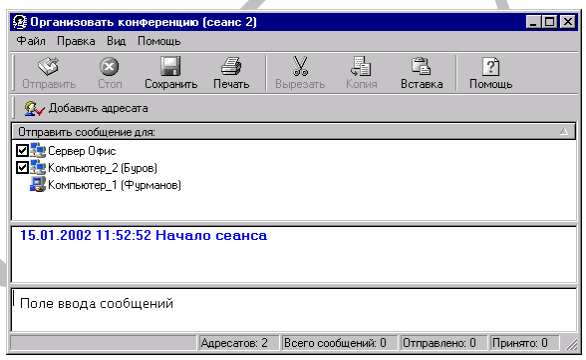

Рисунок 4.15 – Окно конференции

Конференция и обмен текстовыми сообщениями очень похожи. Разница заключается в том, что в обмене сообщениями участвуют несколько человек, а не два и при этом организатор конференции (Рисунок 4.15 – запись без отметки – Компьютер_1 (Фурманов)) может посылать сообщение кому-то из участников конкретно и его примет только этот участник, а вот ответ участника увидят уже все, кто участвует в конференции.

По окончании конференции или диалога, протокол беседы можно сохранить в файл.

Шаг 8(28)

Изучение настроек работы через межсетевой экран

Выбираете запись для своего абонентского пункта и два раза кликаете на ней мышкой. Появляется окно (Рисунок 4.16), в котором можно настроить работу АП за прокси (сетевым экраном). Если никаких настроек ранее не производилось, то правая часть этого окна – *Настройка межсетевого экрана (Firewall)* – будет отключена. Включается эта настройка установкой галочки в

чекбоксе *Настроить параметры работы через межсетевой экран* - внизу слева в окне настроек (Рисунок 4.16). Установив галочку в чекбоксе *Работа через Firewall*, мы получаем возможность выбрать тип прокси (UDP-Proxy или ViPNet-Proxy), после чего можно указать *IP-адрес Firewall* прокси и *порт доступа UDP* (по умолчанию это 55777).

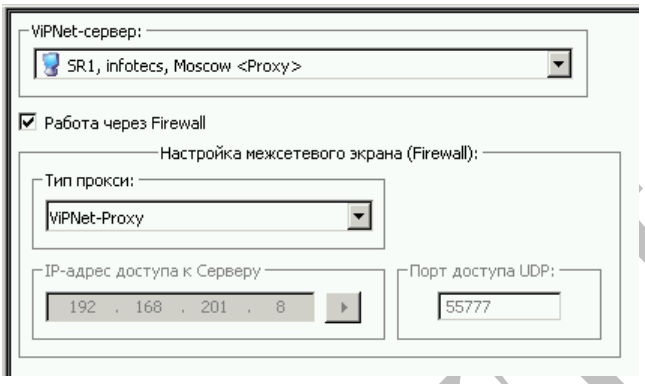

Рисунок 4.16 – Настройки АП

Шаг 9(28)

Изучение работы с незащищенными компьютерами (Открытая Сеть)

Выберите окно *Открытая сеть* и добавьте несколько записей для открытых компьютеров (Рисунок 4.17) (курсор установить на надпись ***Открытая сеть*** → *правая клавиша мышки* → *Правила доступа* → *Добавить IP-адрес*). В появившемся окне (Рисунок 4.18) введите IP-адрес (нажать на кнопку *Добавить)* или URL (строка *Имя компьютера*).

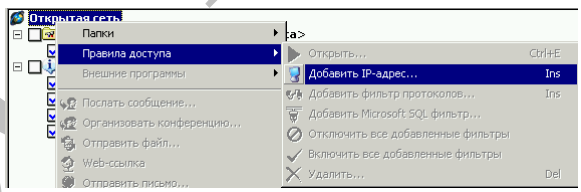

Рисунок 4.17 – Добавление адреса в открытой сети

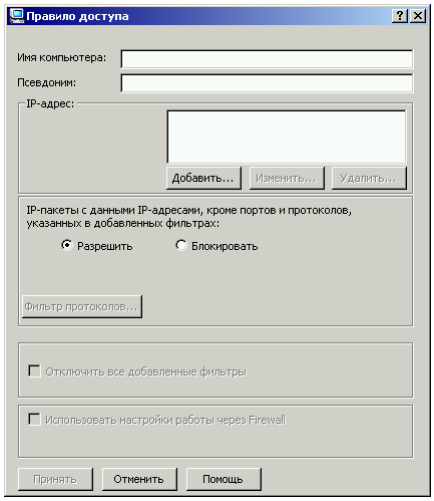

Рисунок 4.18 – Настройка фильтра

Возможность обращения к таким зарегистрированным открытым ресурсам будет регламентироваться режимом безопасности и фильтрами.

Шаг 10(28)

Изучение работы с фильтрами

Для любого пользователя (как защищенного, так и открытого) можно задать свою политику безопасности, определяя для него фильтры. Кроме того можно добавить глобальные фильтры как для защищенной сети, так и для открытой.

Чтобы добавить фильтр установите курсор на запись для пользователя (не важно: открытая сеть или защищенная), щелкните правой клавишей мыши и, в выпавшем меню (Рисунок 4.14), в пункте *Правила доступа* выберите пункт *Добавить* (если выбрать пункт *Изменить,* то появится окно (Рисунок 4.18), в котором станет доступна кнопка *Добавить фильтр*). В появившемся окне (Рисунок 4.19) выберите протокол и определите соответствующие для данного протокола параметры.

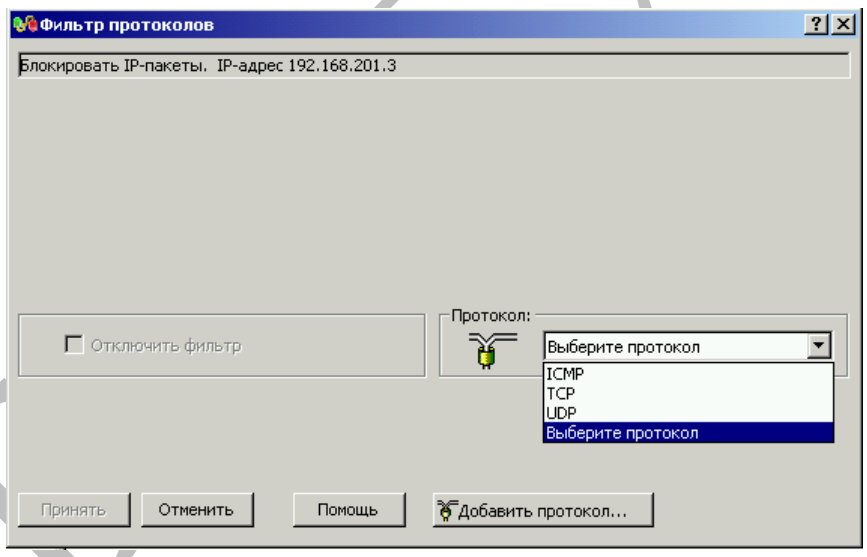

Рисунок 4.19 – Добавление фильтра

Шаг 11(28)

Изучение журналов блокированных и IP-пакетов и их настроек

В процессе работы Монитор ведет ряд журналов. Журнал блокированных IP-пакетов регистрирует только те пакеты, которые не прошли в сеть или из сети в результате работы фильтров. Как правило, для защищенных пользователей (по умолчанию) разрешено почти все, и поэтому в журнале содержаться, в основном, пакеты приходящие от открытых ресурсов (Рисунок 4.20). Анализируя этот журнал, можно определить попытку взлома Вашего компьютера (например, с одного адреса заблокировано множество пакетов, сканирующих Ваш компьютер на наличие слабых мест).

Рисунок 4.20 – Журнал блокированных пакетов

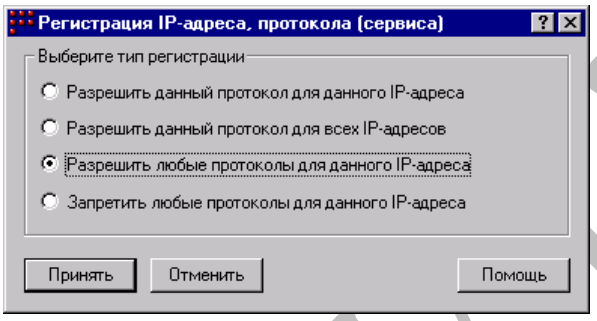

Рисунок 4.21 – Регистрация блокированного пакета

Также, в том случае, когда блокируются нужные пакеты, их можно зарегистрировать и, таким образом разрешить работу с данным открытым ресурсом либо полностью, либо по конкретному протоколу. Для этого на записи для блокированного пакета нажимаем правую клавишу мыши и, в появившемся меню, выбираем пункт Зарегистрировать (Рисунок 4.14). В появившемся окне (Рисунок 4.21) определим вид регистрации.

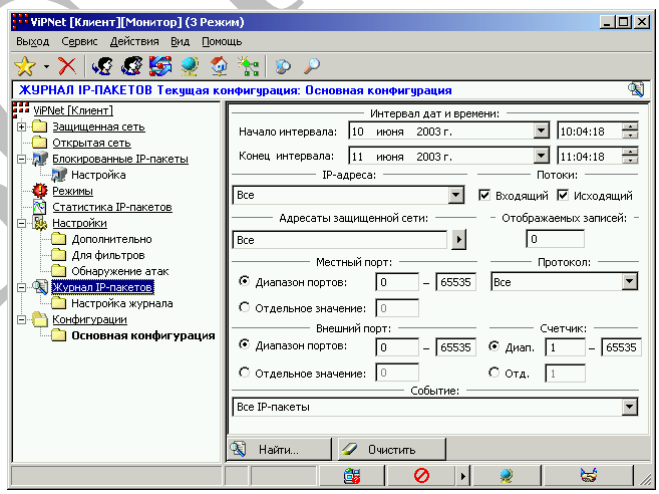

Рисунок 4.22 – Журнал IP-пакетов

Журнал IP-пакетов (Рисунок 4.22) регистрирует ВЕСЬ (!!!) информационный обмен, проходящий через сетевую карту Вашего компьютера. Для того чтобы не выводить много лишней информации, перед загрузкой журнала Вы можете определить различные параметры поиска (Рисунок 4.22).

Шаг 12(28)

Определение URL или IP-адреса

Установите курсор на адрес компьютера, имя отправителя которого Вы хотите определить (это может быть адрес в журнале блокированных пакетов или в открытой сети) и, нажав правую клавишу мышки, выберите пункт  (Определить имя...) (Рисунок 4.14). Перед Вами появится окно (Рисунок 4.23), в котором необходимо нажать кнопку *Найти.* Результат поиска отобразится в одноименном поле (Рисунок 4.23) – если удалось определить доменное имя, то оно и будет написано, в противном случае результатом будет фраза: *Событие 11004 – Верное имя, информация не найдена.*

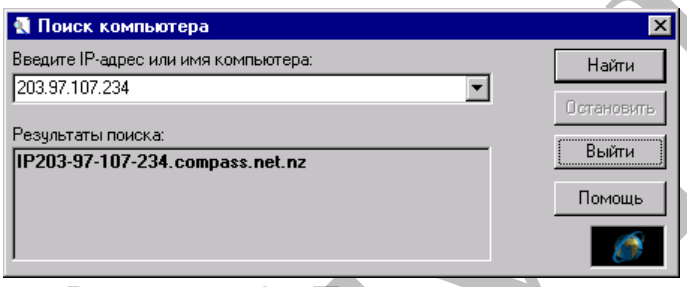

Рисунок 4.23 – Поиск компьютера

Шаг 13(28)

Смена пользователя в Мониторе и ДП

В том случае, когда на одном АП зарегистрировано несколько абонентов (сделать это можно в ЦУСе), активного абонента можно сменить не перезагружая компьютер. Для этого выбираем пункт меню *Сервис → Смена пользователя*. В результате появиться окно (Рисунок 4.2), в котором надо будет ввести пароль того абонента, которого мы хотим сделать активным.

Шаг 14(28)

Настройка псевдонимов

Псевдонимы удобно использовать для изменения имен СУ в списке *Защищенная сеть*, в том случае когда они не информативны (н-р, *АП_1, АП_2* и т.д.).

Псевдонимы задаются локально на каждом СУ, для этого выберите СУ в списке *Защищенная сеть* и два раза кликнете на нем левой клавишей мыши (или по правой клавише мыши выберите пункт *Изменить*). В появившемся

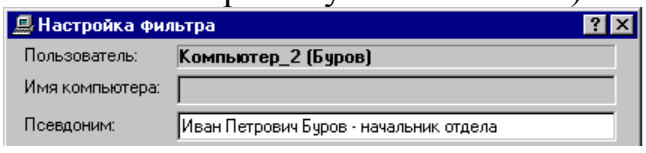

Рисунок 4.24 – Задание псевдонима для имени СУ

окне настроек (Рисунок 4.24) заполните строку *Псевдоним*, введя туда ту информацию, которую Вы хотите видеть в списке узлов защищенной сети вместо действительного имени СУ (н-р, *Иван Петрович Буров – начальник отдела*) (Рисунок 4.24).

Если Вы хотите, чтобы на всех компьютерах псевдонимы были одинаковыми, то их необходимо задать на одном из компьютеров вышеописанным способом. После этого необходимо экспортировать псевдонимы и разослать их всем абонентам защищенной. Для этого выбираем пункт меню *Сервис → Экспорт псевдонимов...* (Рисунок 4.6) и записываем псевдонимы в файл. На других компьютерах пользователи помещают присланный Вами файл с псевдонимами в подкаталог **..\SaveData** рабочего каталога программы Монитор и импортируют его, выбирая пункт меню *Сервис → Импорт псевдонимов...* (Рисунок 4.6).

Шаг 15(28)

Работа в режиме Администратора АП

Введите пароль Администратора АП: @@@@@xxxxxxxxx, где xxxxxxxxx – собственно пароль Администратора АП. После правильного ввода пароля будет задан вопрос, желаете ли Вы сменить пароль Администратора АП на данном конкретном СУ. Это дает возможность выставлять на разных СУ разные пароли Администраторов АП. Если пароль Администратора АП не менять (нажать *НЕТ*), то далее будет предложено ввести пароль абонента, собственно для которого Вы и хотите изменить настройки в режиме Администратора АП. В открывшемся окне Монитора появляется окно *Администратор*, в котором можно определить дополнительные параметры (Рисунок 4.25).

Кроме того в окне *Администратор* присутствует кнопка вызова журнала событий. По нажатию этой кнопки вызывается журнал событий (Рисунок 4.26), в котором отмечаются основные события, происходившие на АП, в частности можно определить дату и время попытки НСД (Рисунок 4.26).

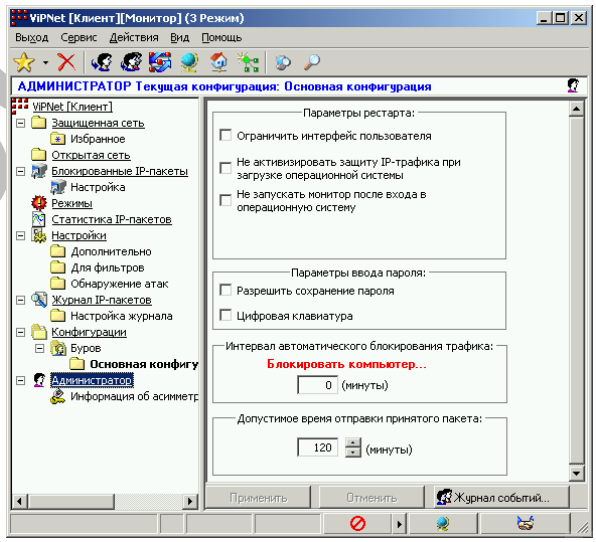

Рисунок 4.25 – Окно *Администратор*

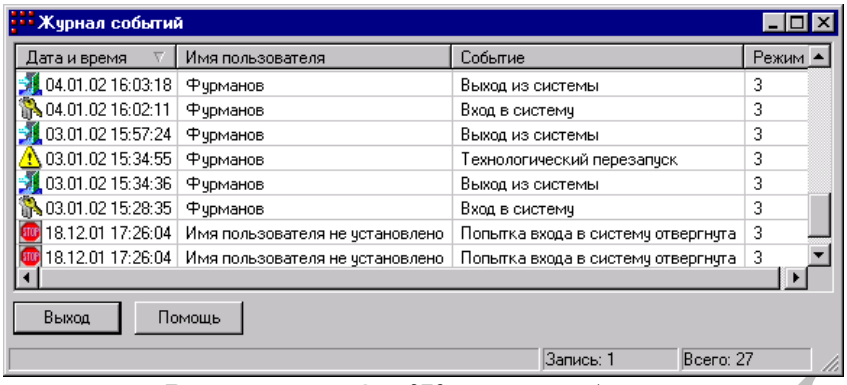

Рисунок 4.26 – Журнал событий

Помимо этого, в режиме администратора можно получить удаленно журнал IP-пакетов с любого другого СУ данной VPN. Для этого в окне Монитора выбираем *Журнал IP-пакетов* и нажимаем на кнопку *Удаленный запрос...* (Рисунок 4.27).

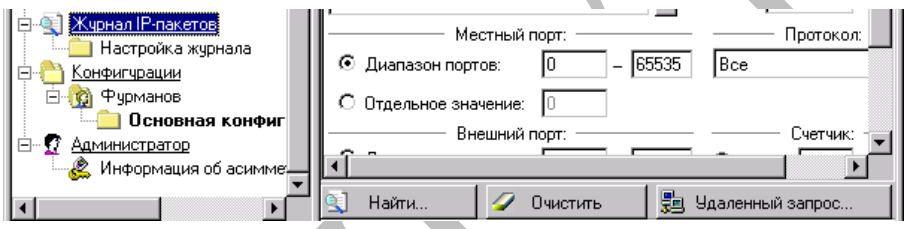

Рисунок 4.27 – Журнал IP-пакетов в режиме администратора

В появившемся окне выбираем интересующий нас СУ и нажимаем кнопку *Выбрать* (Рисунок 4.28). В результате, если соединение с выбранным СУ на данный момент есть, мы получим его журнал IP-пакетов.

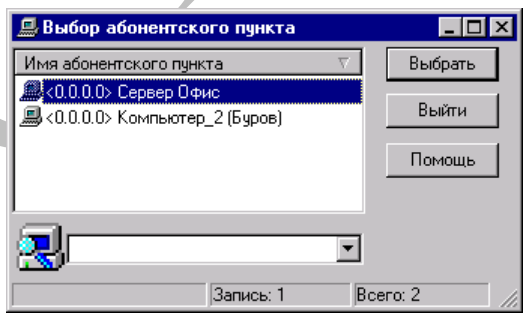

Рисунок 4.28 – Выбор АП для удаленного запроса журнала

Шаг 16(28)

Настройки MFTP

Запускаем MFTP и выбираем пункт меню *Настройки*. Перед нами появляется окно, содержащее несколько вкладок (Рисунок 4.29).

Для каждого СУ можно определить свой тип канала передачи данных (двойным нажатием левой клавиши мышки на какой-либо записи) (Рисунок 4.30) - *Через сервер, MFTP, SMTP/POP3, локальный*. Обеспечьте поочередно

для какого-либо СУ работу через разные каналы (*MFTP*-указать адрес, *SMTP/POP3* – указать e-mail, *локальный* - выбрать каталог).

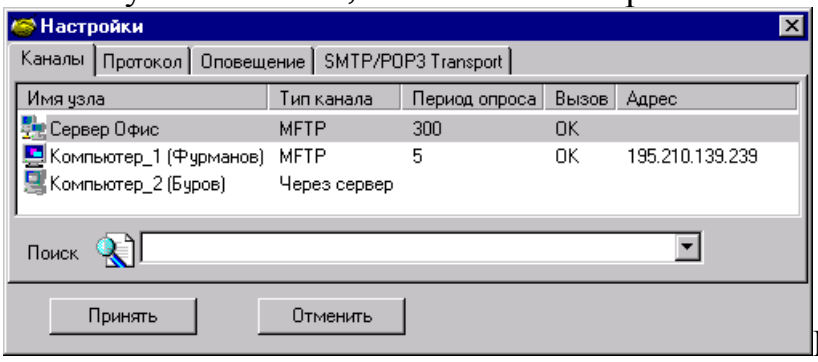

Рисунок 4.29 – Окно *Настройки*

По умолчанию, все АП работают через свой СМ для обеспечения гарантированной доставки передаваемой информации.

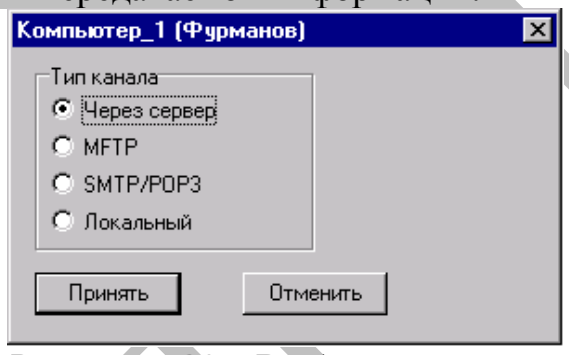

Рисунок 4.30 – Выбор типа канала

Шаг 17(28)

Обеспечение работы по Dial-Up

Если у Вас на компьютере установлен модем, в настройках MFTP появляется дополнительная вкладка Интернет (Рисунок 4.31), на которой необходимо выбрать соединение и задать его параметры по нажатию клавиши Настроить.

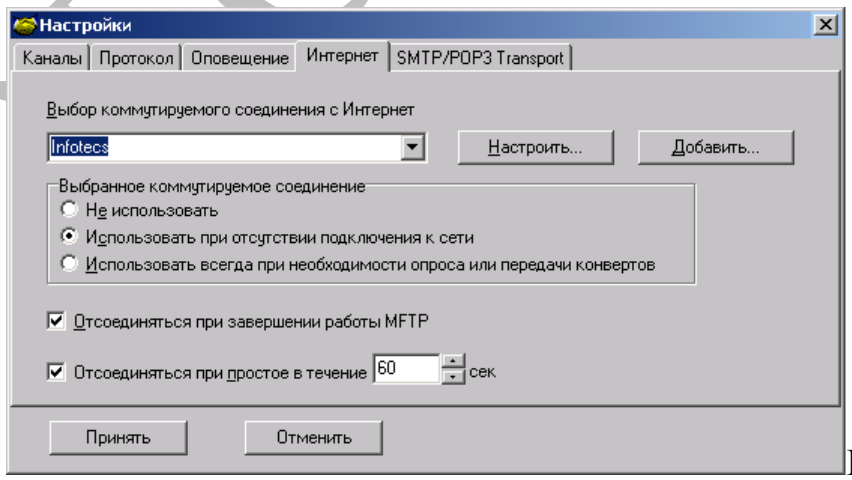

Рисунок 4.31 – Настройка вкладки *Интернет*

Внимание, если не убрать галочки *Отсоединяться при завершении работы* и *При простое*, то, по умолчанию, каждые 60 сек соединение с Интернет будет разрываться!!!

Шаг 18(28)

Журнал конвертов MFTP

В окне транспортного модуля выберите пункт меню *Журнал*. В появившемся окне (Рисунок 4.32) можно задать параметры поиска: имя файла, отправителя, получателя, установить временной интервал и задать маску событий. После этого перед Вами появится собственно окно журнала

(Рисунок 4.33), в котором имена конвертов @*.* означают письма, а остальные – это квитанции и управляющие сообщения.

Журнал фиксирует все принятые и отправленные конверты, в нем можно, при необходимости, найти нужный конверт и определить когда и кому он был послан или от кого был принят. Для писем, в графе *Описание* фиксируется тема письма (Рисунок 4.33).

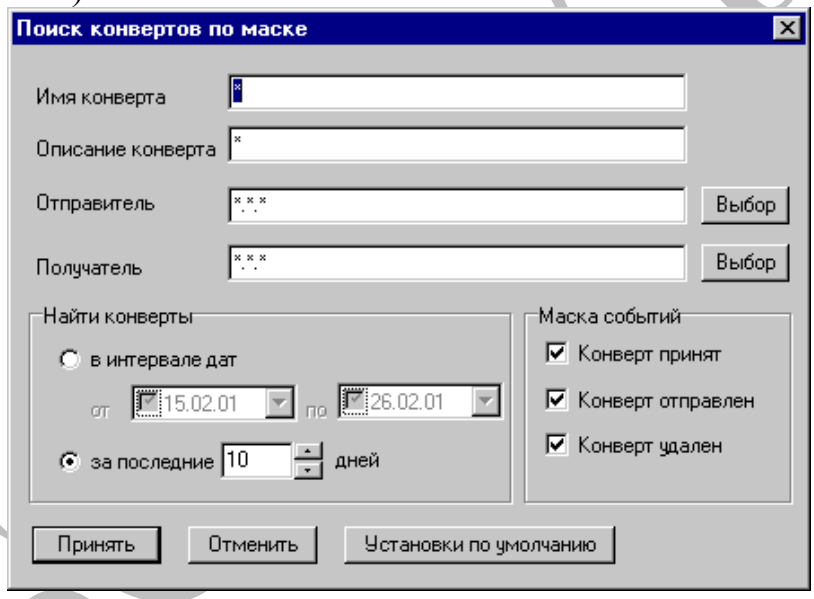

Рисунок 4.32 – Настройка журнала

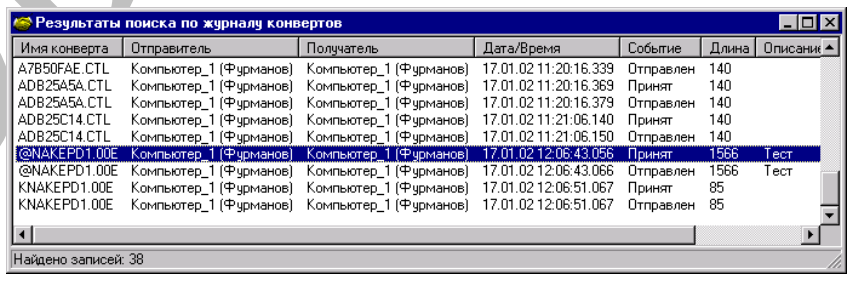

Рисунок 4.33 – Журнал MFTP

Шаг 19(28)

Очередь конвертов MFTP

В окне транспортного модуля выберите пункт меню *Очередь*. В появившемся окне (Рисунок 4.34) можно задать параметры просмотра: имя файла, отправителя, получателя и установить временной интервал. После этого

перед Вами появится собственно окно очереди, аналогичное окну журнала (Рисунок 4.33), в котором можно просмотреть список подготовленных к отправке конвертов.

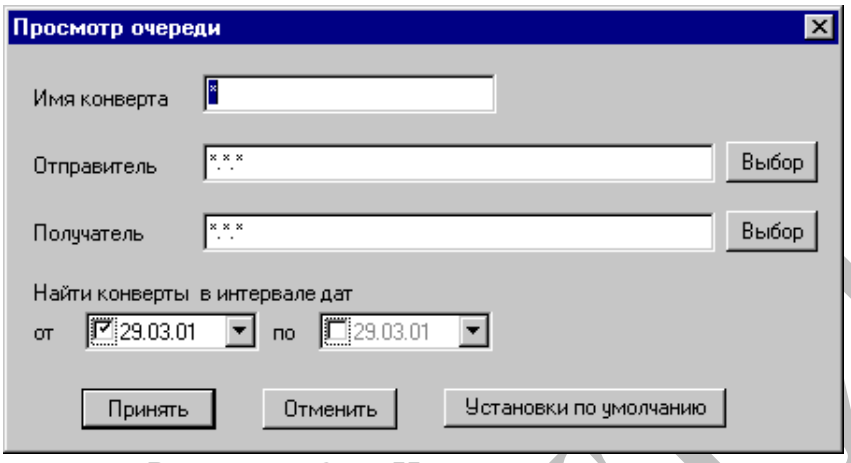

Рисунок 4.34 – Настройка очереди

Шаг 20(28)

Формирование нового письма, отсылка одному или нескольким адресатам

Находясь в Мониторе, установите курсор на пользователе защищенной сети и, вызвав сервисное меню (однократное нажатие правой клавиши мышки), выберите пункт  (Отправить письмо...) (Рисунок 4.14) или, находясь в Деловой Почте, нажмите на иконку  (Новое письмо). В появившемся окне *Исходящее* (Рисунок 4.35)

 (в ответ на нажатие иконки появится стандартное Windows окно для выбора необходимых файлов). Если письмо создается непосредственно в ДП, то выберите адресата  из адресной книги (Рисунок 4.36) (повторите последний шаг для выбора более, чем одного адресата).

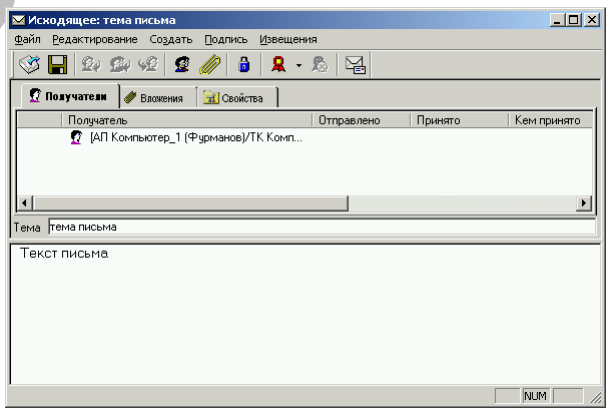

Рисунок 4.35 – Окно создания письма

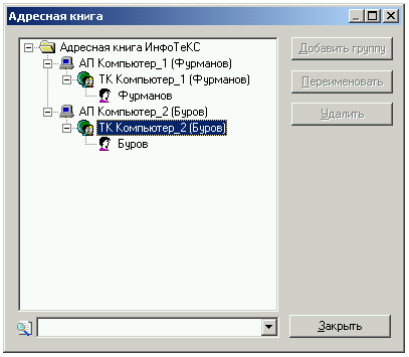

Рисунок 4.36 – Адресная книга

Перед отправкой можно просмотреть все письмо для исключения неточностей и упущений: вкладка *Получатели* содержит имена выбранных Вами адресатов, вкладка *Вложения* показывает файлы, прикрепленные к данному письму, вкладка *Свойства* отражает общую информацию о письме – регистрационный номер, дату и время создания письма, отправителя.

Шаг 21(28)

Использование ЭЦП

Подписать все письмо или только его текстовое содержание можно через меню *Подпись* в окне формирования письма (Рисунок 4.37). Все письмо можно подписать, нажав иконку  на панели инструментов в окне формирования письма (Рисунок 4.35).

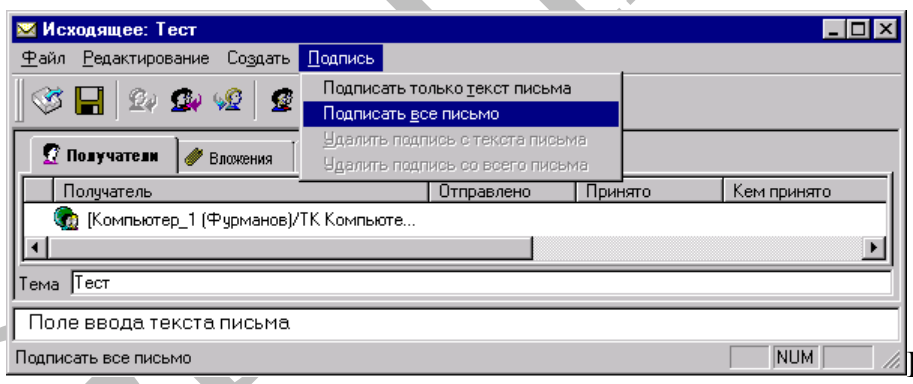

Рисунок 4.37 – Меню *Подпись*

Для проверки действительности подписи полученного письма необходимо нажать иконку  на панели инструментов.

Шаг 22(28)

Использование прикладного шифрования писем

Используя иконку  (Рисунок 4.35) можно зашифровать как все письмо, так и только вложения, в зависимости от того на какой вкладке при формировании письма Вы находитесь.

Примечание! По умолчанию сделаны настройки автоматического подписывания и шифрования писем. А при необходимости и наличии достаточных полномочий пользователь может эти настройки изменить.

Изменить эту настройку можно в меню ДП *Инструменты* → *Настройка...,* вкладка *Письмо,* поле *Безопасность* (Рисунок 4.38).

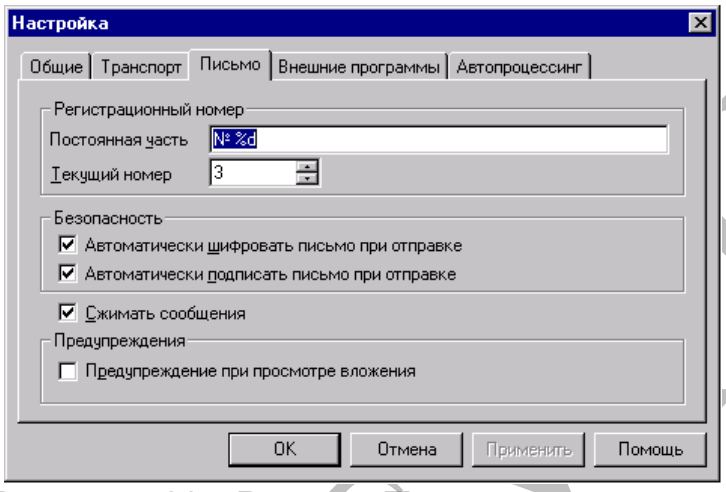

Рисунок 4.38 – Вкладка *Письмо* окна настроек

Шаг 23(28)

Флаги упаковки, отправки, доставки и прочтения писем в ДП

Путь прохождения письма от его создания до удаления получателем отмечается квитанциями, которые индицируются в графе *Атрибуты* основного окна ДП (Рисунок 4.39). Помимо квитанций здесь же отражаются флаги о статусе письма (зашифровано, подписано проч.)

- **П** - подписано письмо и все вложения;
- **п** - подписано либо письмо и/или вложения, но не все элементы подписаны;
- **Ш** - письмо и все вложения зашифрованы;
- **У** - письмо упаковано для всех выбранных получателей;
- **у** - письмо упаковано для некоторых получателей, но не для всех;
- **Д** - письмо доставлено всем получателям;
- **д** - письмо доставлено некоторым получателям, но не всем;
- **О** - письмо отправлено для всех выбранных получателей;
- **о** - письмо отправлено для некоторых получателей;
- **Ч** - письмо прочитано всеми получателями;
- **ч** - письмо прочитано некоторыми получателями.

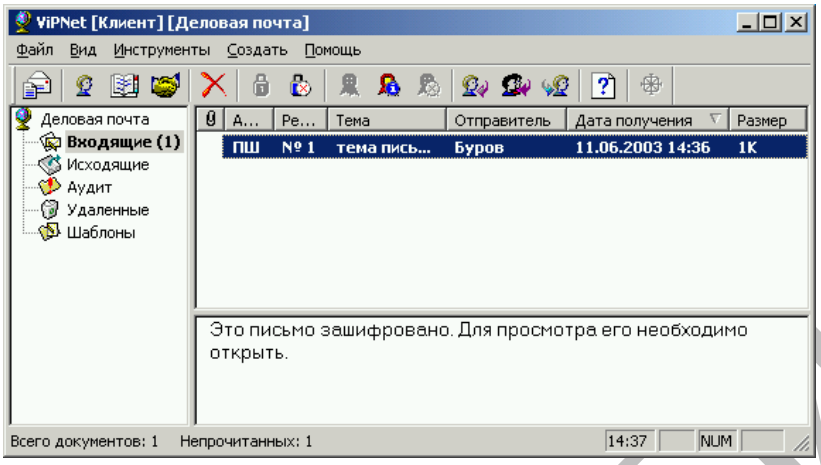

Рисунок 4.39 – Основное окно ДП

Шаг 24(28)

Изучение свойств письма

К свойствам письма мы отнесем его регистрационный номер, имя конверта, кто и когда получил, прочел и удалил.

Настройка регистрационного номера письма осуществляется на вкладке *Письмо* меню *Инструменты* → *Настройка...* (Рисунок 4.38). Регистрационный номер состоит из постоянной части (ее можно определить самому) и переменной (автоматически изменяется с каждым новым созданным письмом).

Информацию о том кто и когда прочитал письмо можно почерпнуть на вкладке *Получатели* отправленного письма (Рисунок 4.40).

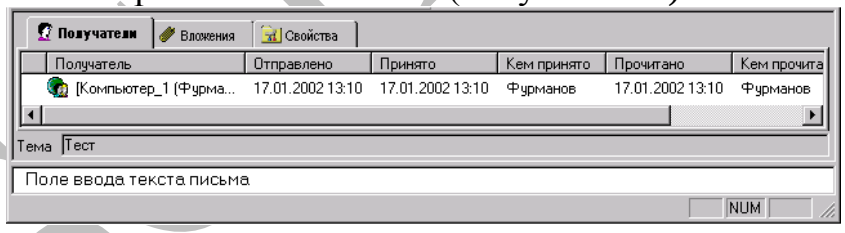

Рисунок 4.40 – Вкладка *Получатели*

Шаг 25(28)

Запуск внешних программ в ДП

Запуск внешних программ настраивается на вкладке *Внешние программы* в меню ДП *Инструменты* → *Настройка*... (Рисунок 4.41).

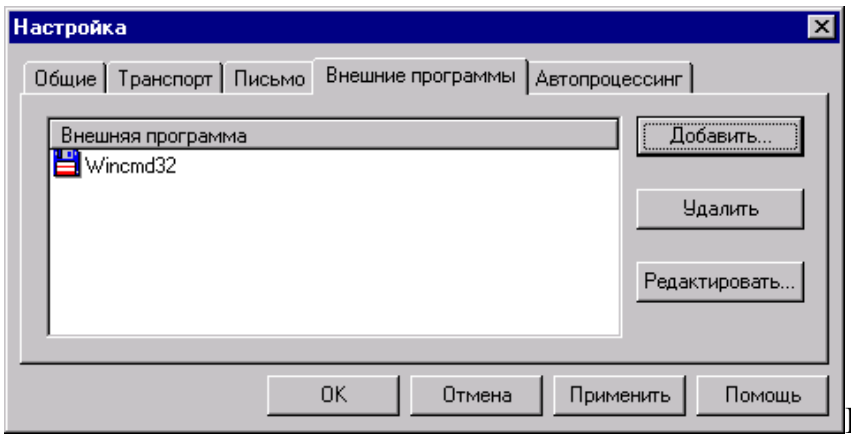

Рисунок 4.41 – *Внешние программы*

При этом можно *Добавить* и *Удалить* внешние программы, а также *Редактировать* (при нажатии этой кнопки откроется окно редактирования пути к данной внешней программе и ее названия). После настройки внешних программ на панели инструментов основного окна ДП (Рисунок 4.39)активируется иконка *Запуск внешних программ* .

Шаг 26(28)

Настройка автопроцессинга

Автопроцессинг предназначен для организации автоматизированного (без участия человека) документоооборота.

Выбрав вкладку *Автопроцессинг* в меню ДП *Инструменты* → *Настройка*... (Рисунок 4.42), можно настроить автоматическую обработку файлов и входящих писем.

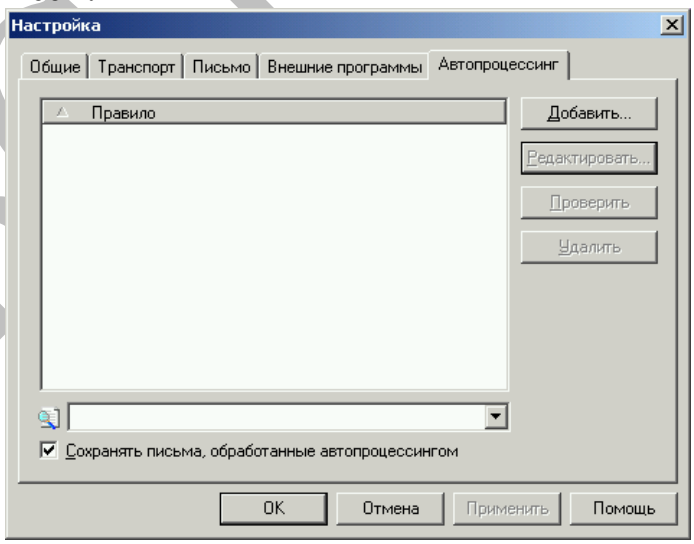

Рисунок 4.42 – Настройка автопроцессинга

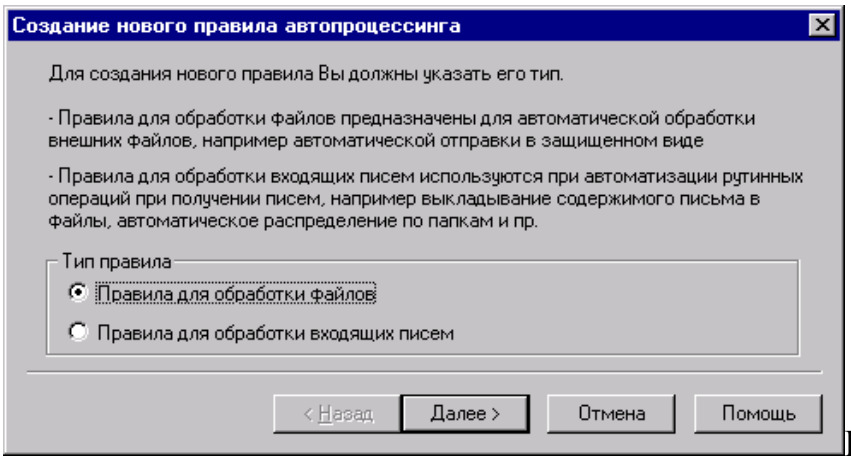

Рисунок 4.43 – Окно выбора правил

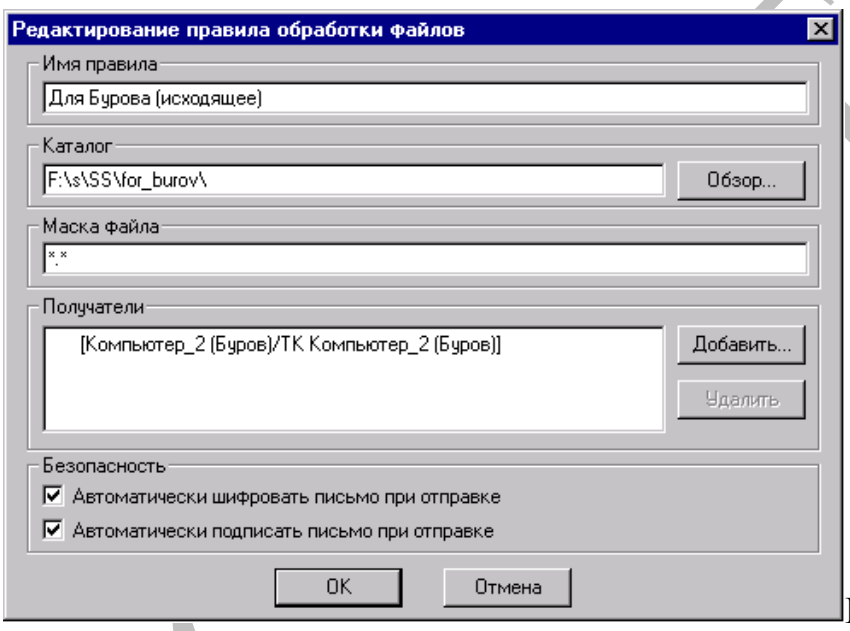

Рисунок 4.44 – Настройка исходящего правила

Обработка осуществляется в соответствии с различными правилами, задаваемыми пользователем. При нажатии кнопки *Добавить* откроется окно для выбора типа правила (Рисунок 4.43).

Правило для обработки файлов предназначено для автоматизации отправки файлов другим пользователям. Нажимаем кнопку *Далее* и, в появившемся окне (Рисунок 4.44), заполняем необходимые поля: *Имя правила*, *Каталог*, откуда будут забираться файлы, *Маска файла*, *Получатели* и определяем *Безопасность* установкой необходимых галочек на одноименном поле.

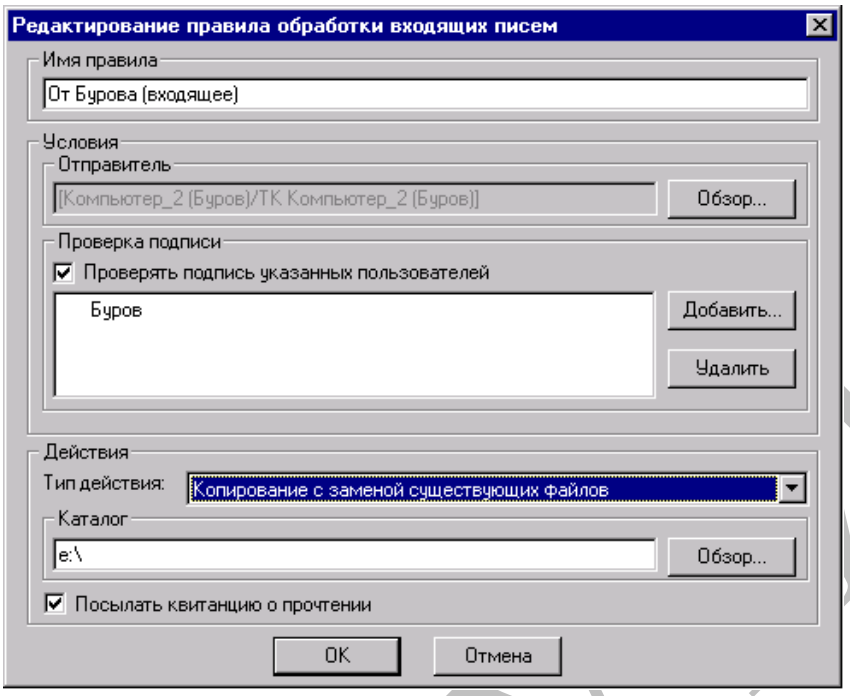

Рисунок 4.45 – Настройка входящего правила

Правило для обработки входящих писем предназначено для автоматической обработки входящих писем. При выборе данного типа откроется окно (Рисунок 4.45), в котором необходимо задать *Имя правила*, в поле *Отправитель* выбрать необходимого пользователя (пользователей), в поле *Проверка подписи* можно задать проверку подписи конкретных отправителей, в поле *Каталог* указать каталог для копирования вложений. Последним шагом является определение типа действия (Рисунок 4.46) в поле *Действия.* Также можно указать необходимость высылки квитанции о прочтении.

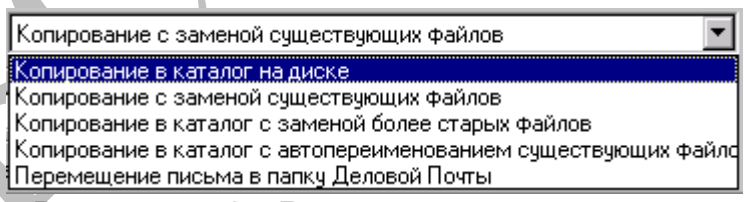

Рисунок 4.46 – Возможные типы действий

Шаг 27(28)

Путь ***письма при его удалении (→ Удаленные → Аудит) в ДП***

Удалите письмо из папки *Входящие*. Оно перемещается в папку *Удаленные* и хранится там в первоначальном виде (доступен текст и вложения). После удаления письма из папки *Удаленные* – письмо удаляется окончательно (текст и вложения не доступны), а заголовок письма помещается в папку *Аудит*, откуда удалить его можно **только в случае входа в ДП с правами администратора.**

Шаг 28(28)

Работа с ДП на АП, где зарегистрировано несколько коллективов

Письма для всех типов коллективов, определенных на АП в ЦУСе, приходят в одну папку *Входящие*, но прочитать письмо можно только если оно адресовано Вашему ТК, не зашифровано или адресовано не конкретному ТК, а абонентскому пункту.

Вопросы для самоконтроля

1 Назовите состав и функции ПО ViPNet [Клиент].

2 Классификация МЭ.

3 Необходимо переустановить «Деловую почту». Какие каталоги и файлы надо сохранить?

4 После первой установки ПО вместо адресов СУ стоят «0.0.0.0». Это - ошибка?

5 Как настроить работу со своим другом, не имеющим ViPNet?

6 Можно ли удаленно получить журнал IP-пакетов с другой машины?

7 Чем Демо-версия отличается от рабочей?

8 Что такое Monitor?

9 Для чего служит драйвер ViPNet?

10 Что делает MFTP?

11 Можно ли средствами ОАО «Инфотекс» обеспечить защиту передаваемой информации без драйвера ViPNet?

12 Для чего используется автопроцессинг?

13 Как определить производилась ли попытка взлома Вашего компьютера и кто ее осуществлял?

14 Какие возможности получает администратор, по сравнению с рядовым пользователем (введение пароля администратора) и как это осуществить?

15 Можно ли, и если да, то как отправить письмо нескольким пользователям из Монитора?

16 В какой программе производится настройка параметров безопасности?

17 В какой программе и как можно изменить канал работы одного АП с другим?

18 Можно ли послать сообщение пользователю в режиме offline?

19 Как настроить вызов внешних программ в ДП?