|  |
| --- |
|  |
|  |
|  |

**ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

**«СТАВРОПОЛЬСКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ»**

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к лабораторным работам

по дисциплине «Безопасность сетей ЭВМ»

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Ставрополь, 2021 г.

Методические указания составлены в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утвержденным приказом Минобрнауки России от 09.12.2016г. № 1553

Составитель:

Рассмотрено на заседании методического объединения укрупненных групп специальностей 09.00.00 «Информатика и вычислительная техника»; 10.00.00 «Информационная безопасность» Протокол № 5 от 24.05.2021 г.

Рекомендовано к использованию в учебном процессе Методическим советом СМК, протокол № 5 от 27.05.2021 г.

**Содержание**

[**Лабораторная работа №1** 7](#_Toc3273310)

[«Первоначальное развертывание защищенной виртуальной сети на базе комплекса ViPNet» 7](#_Toc3273311)

[**Часть 1** 18](#_Toc3273312)

[**Часть 2** 24](#_Toc3273313)

[**Часть 3** 29](#_Toc3273314)

[**Часть 4** 34](#_Toc3273315)

[Лабораторная работа№2 «Модификация защищенной сети ViPNet» 46](#_Toc3273317)

[**Часть 1** 49](#_Toc3273318)

[**Часть 2** 54](#_Toc3273319)

[Лабораторная работа№3 «Межсетевое взаимодействие защищенных сетей ViPNet. Часть первая – СММК» 65](#_Toc3273322)

[**Часть 1** 70](#_Toc3273323)

[**Часть 2** 85](#_Toc3273325)

[**Часть 3** 89](#_Toc3273326)

[**Часть 4** 91](#_Toc3273327)

[Лабораторная работа №4 «Межсетевое взаимодействие защищенных сетей ViPNet. Часть вторая – АММК.» 99](#_Toc3273329)

[**Часть 1** 105](#_Toc3273330)

[**Часть 2** 108](#_Toc3273331)

[**Часть 3** 115](#_Toc3273332)

[**Часть 4** 120](#_Toc3273333)

[**Часть 5** 123](#_Toc3273334)

[Лабораторная работа №5«Установка и настройка Защищённого Рабочего Места ViPNet [Клиент]» 137](#_Toc3273337)

### ВВЕДЕНИЕ

Дисциплина «Безопасность сетей ЭВМ» направлена на формирование способностей понимания сущности и значения информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдение основных требований информационной безопасности, в том числе защиты государственной тайны.

В процессе изучения дисциплины у обучающихся формируется целостное представление о владении основными методами, способами и средствами получения, хранения, переработки информации.

**Целью** освоения дисциплины «Безопасность сетей ЭВМ» является приобретение студентами знаний, умений и навыков применения современных технологий защиты данных посредством соответствующих программных комплексов.

**Задачи** дисциплины «Безопасность сетей ЭВМ» – дать студентам необходимые знания, умения и навыки, в том числе:

- представление об информации, методах её хранения, обработки и передачи;

- Первоначальное развертывание защищенной виртуальной сети на базе комплекса ViPNet

- использование средств автоматизированной обработки информации;

- Модификация защищенной сети ViPNet

- использование компьютера при решении профессиональных задач;

- использование прикладного программного обеспечения при решении профессиональных задач;

- Межсетевое взаимодействие защищенных сетей ViPNet.

**Лабораторная работа №1**

«Первоначальное развертывание защищенной виртуальной сети на базе комплекса ViPNet»

1. ***Цель работы***

Основной целью данного занятия является получение опыта создания защищенной сети по заданной желаемой схеме разделения доступа и политики безопасности в данной реальной сети. Также необходимо научиться четко понимать, что делают ЦУС и УКЦ на каждом шаге, какие файловые ресурсы при этом используются. Подобные знания в дальнейшем позволят более грамотно администрировать защищенную сеть.

1. ***Теоретические сведения и основные понятия программно- аппаратного комплекса ViPNet.***
   1. ***Технология ViPNet***

Технология ViPNet предназначена для создания целостной системы доверительных отношений и безопасного функционирования технических средств и информационных ресурсов корпоративной сети организации, взаимодействующей также и с внешними техническими средствами и информационными ресурсами. Доверительность отношений, безопасность коммуникаций и технических средств, безопасность и достоверность информационных ресурсов достигается путем создания в телекоммуникационной инфраструктуре корпоративной сети интегрированной виртуальной защищенной среды, которая включает в себя:

1. Распределенную систему межсетевых и персональных сетевых экранов, защищающую информационные ресурсы и пользователей как от внешних, так и внутренних сетевых атак.
2. Распределенную систему межсетевого и персонального шифрования трафика любых приложений и операционной системы, гарантирующую целостность и конфиденциальность информации, как на внешних, так и внутренних коммуникациях, и обеспечивающую разграничение доступа к техническим и информационным ресурсам.
3. Систему электронной цифровой подписи и шифрования информации на прикладном уровне, обеспечивающую достоверность и юридическую значимость документов и совершаемых действий.
4. Систему прозрачного для программных приложений шифрования данных при сохранении указанных данных в процессе работы этих приложений на сетевых и локальных жестких дисках, других носителях.

Система обеспечивает целостность и недоступность информации для несанкционированного использования в процессе ее хранения.

1. Систему контроля и управления связями, правами и полномочиями защищенных объектов корпоративной сети, обеспечивающую автоматизированное управление политиками безопасности в корпоративной сети.
2. Комбинированную систему управления ключами, включающую подсистему асимметричного распределения ключей (PKI), обеспечивающую информационную независимость пользователей в рамках заданных политик безопасности от центральной администрации, и подсистему распределения симметричных ключей, гарантирующую высокую надежность и безопасность всех элементов централизованного управления средствами ViPNet, в том числе защиту подсистемы PKI.
3. Систему, обеспечивающую защищенное взаимодействие между разными виртуальными частными сетями ViPNet путем взаимного согласования между администрациями сетей.

С помощью системы защиты информации ViPNet можно проводить контроль доступа к любому узлу (рабочая станция, сервер и т.д.) и сегменту сети (локальная сеть, сегмент локальной сети, группа сегментов сети и т.д.), включая фильтрацию трафика, правила которой могут быть определены для каждого узла отдельно, как с помощью набора стандартных настроек, так и с помощью индивидуальной настройки. Возможно организовать безопасную работу участников VPN с совместным информационным групповым и/или корпоративным информационным ресурсом и защитить от НСД к информационным ресурсам корпоративной сети, хранимым на рабочих станциях (мобильных, удаленных и локальных), серверах (WWW, FTP, SMTP, SQL, файл-серверах и т.д.) и других хранилищах группового доступа.

Технология позволяет проводить аутентификацию пользователей и сетевых объектов VPN как на основе использования системы симметричных ключей, так и на основе использования инфраструктуры открытых ключей (PKI) и сертификатов стандарта Х.509, а также оперативно управлять распределенной VPN-сетью (включая систему распределенных сетевых экранов) и политикой информационной безопасности на сети из одного центра с возможностью делегирования части полномочий локальным администраторам.

#### Состав программно-аппаратного комплекса ViPNet

**ViPNet [Администратор]** создает логическую инфраструктуру виртуальной сети, определяет политики безопасности в ней, осуществляет мониторинг и управление объектами сети. Также формирует симметричную ключевую информацию и первичную парольную информацию, выпускает сертификаты открытых ключей для объектов сети.

ViPNet [Координатор]:

* выполняет маршрутизацию почтовых и управляющих защищенных сообщений при взаимодействии объектов сети между собой и ViPNet [Администратором];
* в реальном времени осуществляет регистрацию и предоставление информации о состоянии объектов сети, их местоположении, значении их IP- адресов и др.;
* обеспечивает работу защищенных компьютеров локальной сети в VPN от имени одного адреса (функция proxy);
* осуществляет туннелирование пакетов от обслуживаемой ViPNet [Координатором] группы незащищенных компьютеров локальной сети для передачи трафика от них к другим объектам VPN в зашифрованном виде по открытым каналам Интернет/Интранет;
* фильтрует трафик от источников, не входящих в состав VPN, в соответствии с заданной политикой безопасности (функция межсетевого экрана);
* обеспечивает возможность работы защищенных по технологии ViPNet компьютеров локальной сети через сетевые экраны и прокси-серверы других производителей.

**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.

#### Понятия адресной и прикладной администрации

Сетевой уровень:

*Сетевой узел (СУ)* - это отдельный абонентский пункт (АП) или сервер- маршрутизатор (СМ)

*Сетевая группа (СГ)* - это совокупность сетевых узлов, которые должны иметь возможность связываться друг с другом

*Сетевые объекты (СО)* - это совокупность сетевых узлов и сетевых групп *Абонентский пункт (АП)* - это сетевой узел, на котором работают прикладные задачи пользователя. Каждый абонентский пункт подключается к одному координатору.

Прикладной уровень:

*Прикладная задача (ПЗ)* - определенная функция сетевого узла (способность выполнять на сетевом узле определенные клиентские или серверные задачи),

например, "Деловая почта", "Диспетчер", "Система платежей", "Центр управления сетью", "Ключевой центр" и др.

*Коллектив (К)* - это множество абонентов, работающих на одном сетевом узле и зарегистрированных в одном подразделении. Именно коллективы *являются отправителями и получателями сообщений в сети ViPNet.*

*Главный коллектив-*коллектив, ключ которого используется абонентом для шифрования документов независимо от АП, на котором осуществляется это шифрование.

*Открытый коллектив (для абонента)* - коллектив, абонент которого виден другими абонентами в адресных справочниках АП

*Скрытый коллектив (для абонента)* - коллектив, об абоненте которого не будут знать абоненты коллектива, хотя такому абоненту доступна вся информация, адресованная абонентам данного коллектива

Тип коллектива или подразделение (ТК) - объект разграничения доступа (по смыслу это организационное подразделение)

*Связь коллективов* - это возможность обмениваться информацией в зашифрованномвиде. Если два коллектива связаны, то для них создается симметричный ключ шифрования для обмена информацией.

*Абонент (Аб)* - пользователь сети ViPNet, зарегистрированный на одном или нескольких СУ (в одном или нескольких подразделениях)

#### Сеть ViPNet с точки зрения маршрутизации сообщений

С точки зрения маршрутизации сообщений сеть ViPNet является иерархической. В ней выделяются два типа сетевых узлов: абонентские пункты и координаторы. Иерархическая структура сети ViPNet находит свое отражение в сетевом адресе. Сетевой адрес имеет бинарное и символьное представления. В бинарном представлении сетевой адрес есть

struct {

word Select, // поле селекторов word NumNet, // номер сети

word NumSrv, // номер координатора

word NumAP // номер АП в области данного координатора

};

Таким образом, структура сетевого адреса позволяет иметь до 65535 сетей ViPNet, не пересекающихся по сетевым адресам. В каждой сети может быть размещено до 65535 координаторов, к каждому из которых может быть подключено до 65535 АП.

Поле селекторов в настоящее время является нулевым и зарезервировано для дальнейшего использования (в частности, для групповой и широковещательной адресации). Нулевое поле селекторов означает, что адрес принадлежит отдельному сетевому узлу. Поле NumAP в адресе

координатора является нулевым. Символьное представление сетевого адреса получается из бинарного путем преобразования каждого 2-байтного поля в 4 шестнадцатеричных символа. Каждой сети ViPNet лицензируется уникальный номер. Уникальность этого номера, в принципе, не имеет значения при автономном функционировании сети ViPNet. Однако это становится важным, если две сети ViPNet захотят установить между собой защищенную связь. Реальное сетевое соединение может быть установлено только между теми СУ, ТК, которые связаны. Один абонент может входить в несколько коллективов, в том числе расположенных на разных сетевых узлах. На каждом сетевом узле всегда имеется, по крайней мере, один коллектив (называемый общим), в который входят все абоненты, зарегистрированные на данном сетевом узле. Отправителем и получателем зашифрованной информации всегда являются некоторые коллективы, поэтому коллектив является минимальной группой с точки зрения доступа к зашифрованной информации.

Каждый абонент имеет возможность зашифровывать информацию от имени тех коллективов, в которые он входит, и расшифровывать информацию, предназначенную для коллективов, в которые он входит. Два абонента сети имеют засекреченную связь тогда и только тогда, когда имеется связь между коллективами, в которые они входят.

Смысл введения понятия ТК заключается в том, что все коллективы одного и того же ТК автоматически (по умолчанию) связаны друг с другом. Для того чтобы ввести связь коллективов разных подразделений, необходимо явно задать такую связь. Задание связи ТК означает введение попарной связи всех коллективов этих ТК. Если по отношению к шифрованию абонент выступает, как представитель коллектива, то по отношению к ЭЦП абонент выступает, как индивидуум. Каждый абонент имеет возможность производить формирование электронной подписи документов от своего имени (если это разрешено ЦУСом), а также осуществлять проверку электронной подписи под документами, поставленной другими абонентами.

#### Особенности ключевой структуры сети ViPNet

Система защиты информации ViPNet использует комбинацию криптографических алгоритмов с симметричными и асимметричными ключами. Симметричные алгоритмы используются для шифрования и проверки целостности информации. Асимметричные алгоритмы используются для обмена ключами и электронно-цифровой подписи. Особенность комбинирования криптографических алгоритмов с симметричными и асимметричными ключами заключается в том, что шифрование информации происходит на комбинации симметричного ключа, созданного администратором УКЦ и ключа, созданного на основе асимметричных ключей, создаваемых пользователями. Такая схема позволяет

ограничить доступ к информации со стороны администратора безопасности, которому известны все симметричные ключи в сети, но неизвестны асимметричные ключи пользователей.

Используются следующие симметричные алгоритмы: ГОСТ (256 бит), DES (56 бит), 3DES (168 бит) и RC6 (256 бит). В асимметричных алгоритмах распределения ключей и электронно-цифровой подписи используются ключи (открытый и секретный) длиной 512 бит (1024 бит).

Когда говорят, что какой то объект, определенный в продуктах ViPNet (это может быть сеть, сетевой объект, коллектив) имеет секретный асимметричный ключ, то это означает, что данный объект сам создал случайным образом этот ключ и хранит этот ключ в строжайшем секрете от всех остальных. Кроме того, он для этого ключа создал соответствующий ему открытый ключ и сделал его общеизвестным. Как правило, все открытые ключи помещаются в какие-то справочники, и эти справочники рассылаются всем, кому только можно. В ViPNet рассылка таких справочников выполняется более строго. Во-первых, эти справочники рассылаются под защитой симметричных ключей, во-вторых, они рассылаются только тем сетевым объектам, с кем разрешены связи. Это обеспечивает значительно более высокий уровень их защиты от подмены, по сравнению с системами, использующими только открытую схему распределения ключей. В технологии ViPNet используется два типа асимметричных ключей - асимметричные ключи подписи и асимметричные ключи шифрования.

Асимметричные ключи шифрования используются для шифрования информации. На основе своего секретного ключа и чужого открытого вырабатывается некий ключ, который никто, кроме данных двух абонентов получить не может. Полученный ключ используется для шифрования информации. Таким образом, каждый абонент хранит в тайне только свой секретный асимметричный ключ, а открытые асимметричные ключи всех абонентов делаются общеизвестными. В этом большой выигрыш по сравнению с симметричными ключами, где каждый абонент должен хранить в секрете ключи парной связи со всеми остальными абонентами.

Асимметричные ключи подписи используются несколько иначе. Секретный асимметричный ключ позволяет подписывать информацию, а открытый асимметричный ключ позволяет проверять правильность этой подписи. Знание открытого асимметричного ключа не дает возможности подписания информации от имени владельца секретного асимметричного ключа (это второе замечательное свойство систем с открытым ключом). В технологии ViPNet не используется система рассылки справочников для открытых асимметричных ключей подписи. Каждый открытый асимметричный ключ прикрепляется к подписанной информации, хранится и рассылается вместе с ней, что значительно упростило систему поддержки контроля над сроками действия подписи.

Так как асимметричные ключи шифрования и подписи формируются непосредственно абонентами, то необходимо подтверждение того, что открытые ключи шифрования и подписи сформированы именно этим

абонентом. Для реализации этой процедуры в системе защиты информации ViPNet введено понятие «Главный абонент». Главных абонентов в сети может быть один или несколько и им доверяется сертифицировать (подписывать) открытые ключи подписи абонентов своей сети. Роль сертификационного центра выполняет Ключевой и Удостоверяющий Центр. Открытые асимметричные ключи подписи главных абонентов сети помещаются на ключевые дискеты абонентов. Открытые асимметричные ключи шифрования сертифицируются опосредованно: эти ключи подписываются абонентами их сформировавшими. Подпись которых сертифицирована «Главным абонентам»

Всю ключевую информацию, используемую в ViPNet можно условно разделить на две группы: ключевая информация для каждого узла и его коллективов и хранящаяся на жестком диске в каталоге STATION. Здесь могут содержаться большие массивы симметричных и асимметричных ключей для обеспечения связи данного узла и его коллективов с другими узлами и коллективами, с которыми такая связь разрешена ЦУС. Индивидуальная ключевая информация для каждого абонента, хранящаяся на его ключевой дискете или другом носителе. Здесь хранится небольшой объем ключевой информации, предназначенной для получения доступа (расшифрования) к разрешенной для него информации в каталоге STATION, а также некоторые другие персональные ключи, доступные только данному абоненту, в том числе секретный ключ подписи (АСКП).

Индивидуальная ключевая информация зашифрована на пароле, а ключи в каталоге STATION зашифрованы на некоторых ключах, входящих в индивидуальную ключевую информацию пользователей. Формирование ключевой информации производится на нескольких этапах:

* При первоначальном развертывании сети
* При модификации ключевой информации в связи с изменением структуры сети
* При обновлении ключевой информации в связи с истечением сроков действия различных ее компонент
* При обновлении ключевой информации в связи с компрометацией различных ее компонент на различных участках сети.

#### ViPNet [АДМИНИСТРАТОР]

ViPNet [Администратор] включает в себя программы:

* Центр Управления Сетью
* Ключевой и Удостоверяющий Центр

*Центр Управления Сетью (ЦУС)* является регистрационным центром и предназначен для конфигурации и управления виртуальной сетью. ЦУС выполняет следующие функции:

* централизованное управление сетью;
* формирование структуры VPN;
* формирование справочной информации;
* управление "логикой" работы VPN;
* централизованное обновление ПО и функционала компонентов VPN;
* мониторинг событий VPN;
* удаленное управление ресурсами VPN.

*Ключевой и Удостоверяющий Центр (УКЦ)* предназначен для обеспечения ключевой информацией всех участников VPN и выполнения функций удостоверяющего центра. При этом первичные клиентские ключевые наборы могут быть записаны на дискеты, смарт-карты, touch memory, e-token и прочее для передачи участникам VPN. Последующее обновление ключевой информации осуществляется автоматически по защищенным каналам VPN. УКЦ выполняет следующие функции:

* формирование и автоматическое обновление через ЦУС симметричной ключевой информации и первичной парольной информации для объектов и пользователей сети;
* выполнение функций удостоверяющего центра сертификатов цифровых подписей.

#### Особенности взаимодействия ЦУС и УКЦ

Административная часть в ПО ViPNet в целях повышения безопасности разделена на две части, отвечающие за разные аспекты её функционирования. При этом ни та, ни другая части администрации по отдельности не могут оказать существенного влияния на функционирование сети, т.е. возможности несанкционированного доступа к информации абонентов тем или иным администратором сведены к минимуму. Для обеспечения работоспособности сети, созданной с помощью технологии ViPNet необходимо:

1.Создать (изменить) её структуру в ЦУС и скопировать в УКЦ данные, необходимые ему для

генерации ключевой информации.

2.Сгенерировать в УКЦ ключевую информацию.

3.Предоставить необходимые наборы абонентам вновь созданных абонентских пунктов или

разослать их на уже существующие абонентские пункты.

Для того чтобы один абонент с одного абонентского пункта мог обмениваться защищенной информацией с другим абонентом другого абонентского пункта, каждому абоненту необходимо получить:

1.Инсталляционный пакет той или иной программы.

2.Адресную информацию для абонентского пункта, предоставляемую

ЦУС.

3.Ключевую и парольную информацию для абонентского пункта,

предоставляемую УКЦ.

*Адресная и ключевая информация* для упрощения работы с ней предоставляется в виде единого файла (дистрибутива). В процессе изменения структуры сети ЦУС автоматически доставляет и устанавливает обновленную адресную и ключевую информацию, не требуя от пользователя каких либо дополнительных действий.

*Файл-дистрибутив* (или дистрибутив для начальной инсталляции) - файл, создаваемый для каждого абонента сетевого узла и содержащий следующую информацию (в склеенном виде): набор ключей для абонентов и сетевого узла (из УКЦ), регистрационный файл (infotecs.re), а также адресные справочники (из ЦУС). Эта информация необходима для обеспечения первичного запуска прикладной программы сети ViPNet. Различают два вида дистрибутивов: полный и минимальный. Полный дистрибутив содержит полный набор файлов справочников, ключевую дискету абонента и ключевой набор для сетевого узла.

Минимальный дистрибутив содержит выборку файлов справочников и ключевую дискету абонента. Использование минимального дистрибутива достаточно для того, чтобы войти в прикладную программу и дистанционно принять от ЦУСа всю остальную ключевую и адресную информацию (полный набор адресных справочников и ключевой набор для сетевого узла). Учитывая малый объем информации на ключевой дискете, эту информацию можно также размещать на Touch memory или смарткарте для первичной выдачи абоненту. Формирование полного дистрибутива целесообразно, если связь с ЦУСом по каким-либо причинам невозможна. Но в то же время необходимо учитывать, что при большом размере сети файл полного дистрибутива может не поместиться на дискете.

Ключевые дискеты абонентов (КД). Для каждого абонента в УКЦ создается своя ключевая дискета. Основное содержание ключевой дискеты абонента - информация, идентифицирующая абонента и позволяющая работать с прикладными задачами сети ViPNet. Кроме того, на дискете находится электронная цифровая подпись (ЭЦП) данного абонента, если ЦУС разрешил абоненту подписывать документы, а также хэш-функция, служащая для проверки пароля.

Для удобства отправки ключевая дискета создается в склеенном виде (*Склеенный вид* — файлы в неизменном виде склеиваются в один файл с добавлением информации для расклейки). Перед использованием ключевой дискеты ее надо обязательно расклеить (Расклеить ключевую дискету означает преобразовать файл из склеенного вида к набору из нескольких файлов).

Ключевые наборы для сетевых узлов (КН). Для каждого сетевого узла создается один ключевой набор, и все абоненты этого сетевого узла пользуются им при шифровании и расшифровании. Основное содержание ключевого набора — ключи для шифрования между коллективами и между сетевыми узлами. Для удобства отправки ключевой набор создается в склеенном виде. Перед использованием ключевого набора его надо обязательно расклеить.

#### Уровень полномочий

*Полномочия пользователя ViPNet* — это правомерность действий пользователя сетевого узла (АП или СМ) по изменению настроек в различных приложениях ПО ViPNet (совокупность настроек определяет функциональность ПО). Допустимость действий пользователя определяется уровнем полномочий. Уровень полномочий для каждого узла ViPNet задается программой ЦУС. Существует четыре уровня полномочий, три из которых определяются цифрой, а именно: уровень 0 -минимальные полномочия, уровень 1 - средние полномочия и уровень 2 - максимальные полномочия. Четвертый уровень называется уровнем специальных полномочий и имеет несколько значений, каждое из которых определяется специальным символом (цифра или буква).

Полномочия максимального уровня не имеют ограничений по использованию функций ПО пользователем. Полномочия, определяемые другими уровнями, ограничивают действия пользователей по функциям ПО. Все ограничения, накладываемые полномочиями среднего, минимального и специального уровней, снимаются при вводе пароля Администратора сети ViPNet. Программа ЦУС задает полномочия пользователя, работающего на: АП и СМ, зарегистрированных в задаче Защита трафика. Уровень полномочий, заданный для этих сетевых узлов, будет определять функциональность ПО ViPNet [Клиент или Координатор] [Монитор] и ViPNet [MFTP]. АП, зарегистрированных в задаче Деловая почта. Уровень полномочий, заданный для этих сетевых узлов, будет определять функциональность ПО ViPNet [Клиент] [Деловая почта].

#### Методические указания по выполнению лабораторной работы

Шаги, необходимые для первоначального развертывания защищенной сети ViPNet, включающие

* теоретическую проработку схемы защищенной сети;
* инсталляцию рабочего места Администратора защищенной сети;
* первоначальную настройку ЦУС;

-формирование транспортной структуры сети на уровне адресной администрации;

-формирование прикладной структуры сети и ее связывание, задание полномочий абонентов;

* регистрацию СУ в прикладных задачах;
* получение отчета по структуре защищенной сети;
* формирование всех справочников;
* первоначальную настройку УКЦ;
* определение главных абонентов сети и формирование для них персональной ключевой информации;
* генерацию ключевой информации для всех остальных объектов сети;
* распределение готовых ключей и справочников.

###### Задание на занятие:

Сформировать защищенную сеть, исходя из нижеперечисленных условий и приведенной схемы реальной сети (Рис. 1.1).

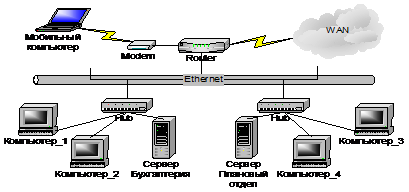


Рис. 1.1. Топология реальной сети.

###### Условия построения защищенной сети:

1.В защищенную сеть включаются следующие СУ: Сервер Бухгалтерия, Компьютер\_1, Компьютер\_2, Сервер Плановый отдел, Компьютер\_3, Компьютер\_4, Мобильный компьютер;

2.Компьютер\_1, Компьютер\_2 и Мобильный компьютер на транспортном уровне в качестве сервера должны использовать Сервер Бухгалтерия;

3.Компьютер\_3, Компьютер\_4 на транспортном уровне в качестве сервера должны использовать Сервер Плановый отдел;

4.Бухгалтерия и Плановый отдел на транспортном уровне должны иметь связь;

5.На Компьютере\_1 постоянно работает один человек (абонент Петров); 6.На Компьютере\_2 могут работать два человека (абоненты Сидоров и

Васечкин), они не должны иметь доступ к информации друг друга на транспортном уровне;

7.На Компьютере\_3, Компьютере\_4 и Мобильном компьютере постоянно работают по одному человеку (абоненты Лялин, Свиридова и Кузовкин соответственно);

8.На каждом сервере регистрируется по абоненту: Администратор Сервера Бухгалтерия и Администратор Сервера Планового отдела;

9.В защищенной сети все видят всех за исключением Васечкина, который не должен иметь связи с Петровым;

10.Дополнительно требуется, чтобы Кузовкин имел возможность получить доступ к Компьютеру\_4 и защищенной информации Свиридовой;

11.Администратором защищенной сети будет Лялин.

Последовательность выполнения занятия:

**Часть 1**

Шаг 1(12)

*Теоретическая проработка схемы защищенной* сети

Итак, вы администратор защищенной сети. Перед вами лежит схема вашей обычной сети (Рис. 1.1) и задание на формирование на ее основе VPN (здесь и далее под VPN понимается Виртуальная Частная Сеть). С чего начинать?

Первым шагом должна стать теоретическая проработка схемы защищенной сети. Необходимо уяснить, что это наиболее важный шаг, так как от того насколько грамотно составлена эта схема, будут зависеть: удобство ее администрирования, отказоустойчивость, требования к оборудованию, настройка и, в конечном итоге, удобство работы с этой сетью конечных пользователей. Постараемся показать и последовательно пройти наиболее типичный порядок выполнения действий, который приведет нас к выработке схемы защищенной сети. Естественно, не стоит воспринимать все ниже перечисленные действия, как жесткую инструкцию. Вопрос выработки схемы VPN – это искусство поиска компромисса между требованиями политики сетевой безопасности, принципов функционирования сегментов сети, включаемых в VPN, желаниями пользователей получить доступ к той или иной информации и возможностями системы, на основе которой, собственно, строится защищенная сеть. Однако, можно однозначно выделить два ключевых момента, которые всегда присутствуют при решении этой проблемы: построение сетевой структуры VPN, построение прикладной структуры VPN.

*1)Построение сетевой структуры VPN*

Чаще всего сетевая структура защищенной сети, т.е. распределение и привязка АП и СМ, совпадает с реально существующей структурой обычной сети. Исходя из этого, по мотивам схемы, приведенной на рис.1.1., мы можем составить следующую сетевую структуру VPN:



АП

Мобильный компьютер (Кузовкин)

Межсерверный канал

АП

Компьютер 1 (Петров)

АП

Компьютер 2 (Сидоров, Васечкин)

АП

Компьютер 3 (Лялин)

АП

Компьютер 4 (Свиридова)

СМ

Сервер Плановый

отдел

СМ

Сервер Бухгалтерия

Рис. 1.2. Сетевая структура защищенной сети.

Здесь кружками обозначены абонентские пункты – рабочие станции, на которые будет производиться установка ViPNet Клиента, квадратами – рабочие станции или сервера с ViPNet Координаторами. Стрелками показаны связи транспортного уровня или – пути следования транспортных конвертов (писем Деловой Почты, файлов, отправляемых через защищенный Файловый обмен, служебных файлов системы). В нашем случае количество СУ совпадает с реальным количеством машин в сети, что является наиболее типичной ситуацией, хотя на одной машине возможно размещение и нескольких АП. Обычно, это делается в том случае, если требуется совмещение на одной машине функций СМ и АП. Так как подобная ситуация является скорее исключением, чем правилом и требует отдельной проработки, в дальнейшем мы не будем рассматривать этот случай.

Приведенные связи являются исключительно логическими, и их не следует отождествлять с реально существующей трассировкой соединений в компьютерной сети.

Несложно увидеть, что представленная схема полностью удовлетворяет требованиям задания в части пунктов 1-4.

*2)Построение прикладной структуры VPN*

После того как построена сетевая структура, можно переходить к построению структуры прикладной. Образно её можно представить как второй слой, накладываемый поверх слоя сетевой структуры. Слои не пересекаются, поэтому связи слоя сетевой структуры теряют значение для связей ТК, задаваемых во втором слое – прикладной структуре. Для привязки слоев друг к другу используется понятие области видимости, которое задаёт, какие из объектов слоя прикладной структуры «возможно увидеть сквозь» СУ слоя сетевой структуры. Вопрос построения прикладной структуры является более сложным, чем вопрос построения сетевой структуры, поэтому следует разбить его на несколько этапов. Первый этап будет отвечать за связывание прикладного слоя со слоем сетевой структуры. На втором этапе мы будем связывать уже объекты внутри прикладного слоя.

На первом этапе используем сетевую структуру (см. рис.1.2) и определим области видимости ТК, другими словами, каким образом ТК будут привязаны к СУ сетевой структуры. Так как в предложенном задании нет требований, чтобы все или часть машин объединялись в некие группы с правом доступа членов такой группы к той или иной информации, то используем наиболее простую схему – каждому СУ назначается в соответствие его собственный ТК. Это даст возможность отождествить СУ с его ТК, то есть всегда существует лишь один СУ-отправитель и один СУ- получатель информации в случае, если информация передается от имени одного ТК другому. Высказанные соображения приводят нас к следующей схеме:

СМ

Сервер Плановый

отдел



ТК

Сервер Плановый

отдел



АП

Компьютер 2 (Сидоров, Васечкин)

ТК

Компьютер 2 (Сидоров)

ТК

Компьютер 2 (Васечкин)



ТК

Сервер Бухгалтерия

СМ

Сервер Бухгалтерия



АП

Мобильный компьютер (Кузовкин)

ТК

Мобильный компьютер (Кузовкин)

АП

Компьютер 1 (Петров)

ТК

Компьютер 1 (Петров)



АП

Компьютер 3 (Лялин)

ТК

Компьютер 3 (Лялин)

АП

Компьютер 4 (Свиридова)

ТК

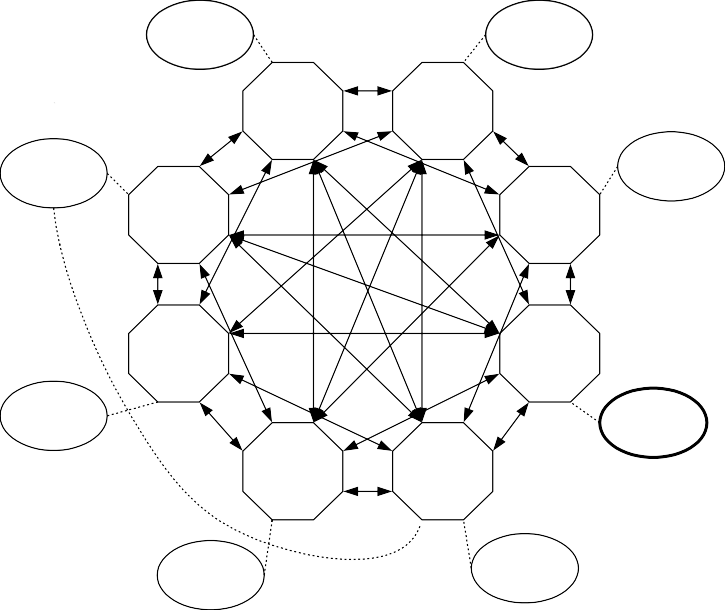
Компьютер 4 (Свиридова)

Рис. 1.3. Назначение областей видимости.

Исключением в данной схеме является лишь АП Компьютер\_2, к которому привязаны два ТК: ТК Компьютер\_2 (Сидоров) и ТК Компьютер\_2 (Васечкин). Это сделано для того, чтобы удовлетворить требованиям п.6 задания. Приведенная схема назначения областей видимости, за исключением выше сделанной оговорки, может быть реализована программой ЦУС автоматически, но, несмотря на это, необходимо всегда помнить об этом этапе и контролировать действия программы.

Второй этап мы начнем с того, что вернемся к заданию и уясним, кому из абонентов и с кем требуются связи в защищенной сети и как это можно достигнуть, исходя из идеологии построения защищенной сети на базе ViPNet. О том, каким образом должны быть распределены абоненты защищенной сети по СУ, мы можем узнать из п.6-8 задания – опять таки, единственным исключением будет СУ АП Компьютер\_2, где должны уживаться два абонента: Сидоров и Васечкин - для них мы уже предусмотрели по ТК (Рис. 1.3). Информацию о необходимых связях берем из

п.9-10. Последний штрих – назначение Главных абонентов защищенной сети. Так как в задании нет специальных требований на наличие нескольких Главных абонентов, т.е. людей, чьими электронно-цифровыми подписями будут заверяться подписи всех остальных абонентов, то назначим Главным абонентом Администратора VPN. По требованию п.11 задания им будет Лялин. В итоге получаем следующую схему связей прикладного уровня (слоя):



Бухгалтерия

Сидоров

ТК

Сервер Бухгалтерия

ТК

Компьютер 2 (Сидоров)

Кузовкин

Васечкин

ТК

Мобильный компьютер (Кузовкин)

ТК

Компьютер 2 (Васечкин)

ТК

Компьютер 1 (Петров)

ТК

Компьютер 3 (Лялин)

Петров

Лялин

ТК

Сервер Плановый

отдел

ТК

Компьютер 4 (Свиридова)

Плановый отдел

Свиридова

Рис. 1.4. Связи прикладного уровня.

Здесь сплошными двунаправленными стрелками обозначены связи прикладного уровня. Заметьте, у Васечкина нет связи с Петровым, как того и требует п.9 задания. Овалами обозначены абоненты VPN и их привязка к соответствующим типам коллектива. Требования п.10 мы выполняем, включив в ТК Компьютер\_4 (Свиридова) абонента Кузовкина. Так как Кузовкин числится в нескольких ТК, то необходимо назначить Главный для него ТК, где он будет получать свою защищенную почту и обновления адресной и ключевой информации. На схеме это никак не отображено, но будем считать, что Главным ТК для абонента Кузовкина является ТК Мобильный компьютер (Кузовкин). Жирной линией выделен Главный абонент защищенной сети Лялин.

Следует обратить особое внимание на то, что в последней схеме не присутствуют СУ сетевого уровня. Таким образом, абоненты непосредственно не привязаны к СУ, что делает VPN на базе ViPNet очень

гибкой системой, позволяющей реализовать любую необходимую политику безопасности и доступ людей к компьютерам и сетевым ресурсам.

Совокупность приведенных схем (Рис. 1.3. и 1.4.) представляет собой структуру прикладного уровня защищенной сети.

Шаг 2(12)

*Инсталляция рабочего места Администратора защищенной сети*

Для инсталляции рабочего места Администратора защищенной сети нам понадобится программа установки Setup.exe, расположенная в каталоге ViPNet

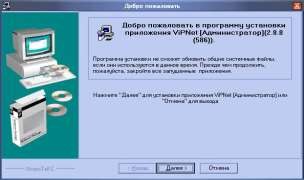


Рис. 1.5. Программа установки ViPNet Администратор.

Администратор инсталляционного комплекта, набор регистрационных файлов ОАО «ИнфоТеКС»: infotecs.re, infotecs.reg; и порядка 25 Мбайт свободного места на жестком диске компьютера.

После удовлетворения этих требований можно переходить, собственно, к инсталляции. Из любого файлового менеджера запускаем программу Setup.exe (Рис. 1.5.), далее жмем Next > (Далее – в локализованных версиях Windows), знакомимся с лицензионным соглашением, и в случае согласия – еще раз Next >. Вводим имя пользователя и название организации, жмем Next

>. После чего попадаем в окно «Папка установки» (Рис. 1.6.):

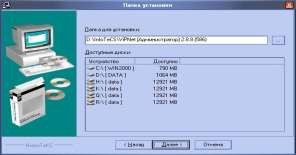


Рис. 1.6. Выбор вида установки программы.

После чего попадаем в окно «Тип установки» (Рис. 1.7.):

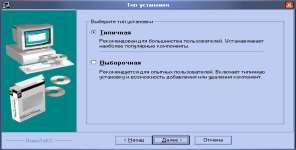


Рис. 1.7. Выбор вида установки программы.

Если нам необходим полный набор программного обеспечения рабочего места Администратора (ЦУС, УКЦ и ViPNet Клиент), то оставляем выбранным пункт «Типичная» установка и жмем Next >, иначе выбираем пункт «Выборочная», задаем каталог установки и тоже жмем Next >. В последнем случае программа установки выдаст следующее окно (Рис.1.8):

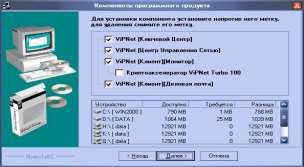


Рис. 1.8. Компоненты программного продукта.

Здесь можно задать состав устанавливаемого ПО. Обычно, такая необходимость возникает, если политика безопасности требует вынесения УКЦ из общего списка и его установку на отдельный компьютер. Также, в качестве примера можно привести установку места Администратора вместе с ViPNet Координатором на один компьютер. В этом случае в настройках необходимо снять галочку «ViPNet [Администратор][Монитор]», что приведет к пропуску шагов программы, касающихся установки низкоуровневого драйвера защиты ViPNet и программы Монитор. В дальнейшем эти компоненты должны быть установлены из комплекта ViPNet Координатор. После выбора необходимых компонентов жмем Next >. Удостоверившись, что все настройки сделаны правильно, жмем Finish и ждем, пока программа завершит копирование необходимых файлов на жесткий диск компьютера.

Если была выбрана «Типичная» установка, то также будет необходимо выбрать значки для размещения на рабочем столе Windows и нажать Finish.

Для завершения шага инсталляции рабочего места Администратора защищенной сети необходимо выполнить следующие действия:

-скопировать файл infotecs.re в подкаталоги KC, NCC и SS каталога установки, который был выбран в ходе проведения установки (см. выше);

-скопировать файл infotecs.reg в подкаталог NCC.

-для возможности использования русских букв в ЦУС необходимо скопировать русификатор – файл RK.com в подкаталог Центра Управления Сетью – NCC. Запуск программ производится либо из созданного программой установки системного меню (Start  Programs  ViPNet… или Старт  Программы  ViPNet …), либо из подкаталогов каталога установки:

-для запуска УКЦ: из подкаталога KC программа key\_center.exe;

-для запуска ЦУС: из подкаталога NCC программа \_start.bat;

-для запуска Монитора: из подкаталога SS программа Monitor.exe;

-для запуска Деловой Почты: из подкаталога SS программа Wmail.exe;

-для деинсталляции или переустановки ПО: из каталога установки программа Setup.exe.

**Часть 2**

Шаг 3(12)

*Первоначальная настройка ЦУС*

Запускаем программу ЦУС (см. рекомендации в конце предыдущего шага). После первого запуска программа выдает следующее окно (Рис. 1.10.):



Рис. 1.10. Настройка путей ЦУС.

Большую часть путей программа уже прописала автоматически и без необходимости менять их не следует. Остается лишь прописать путь к Каталогу личных ключей (место, где будет храниться Ключевая Дискета Администратора защищенной сети). Если ключи будут выкладываться на дискету, то в пятой строке необходимо написать A:\, но обычно КД размещают на жестком диске в подкаталоге SS. В этом случае в пятой строке прописываем ..\SS\. Жмем мышкой кнопку Принять или просто <Enter> на

клавиатуре. На все вопросы программы о создании новых подкаталогов отвечаем утвердительно, нажимая <Enter>.

В следующем окне программа предложит выбрать настройки по умолчанию. Рассмотрим более подробно, какие настройки за что отвечают:

-«Автоматически связывать новый ТК со всеми другими ТК» – если в защищенной сети большая часть ТК должны иметь связи друг с другом, то эта настройка позволит упростить задание связей. В нашем случае только ТК Компьютер\_1 (Петров) не связан с ТК Компьютер\_2 (Васечкин) (Рис. 1.4), поэтому логичным будет выставить эту настройку и потом лишь удалить одну связь, нежели чем создавать все остальные связи;

-«Автоматически создавать ТК и абонента для нового узла» – эта настройка выставлена по умолчанию, потому что всегда проще переименовать ТК и абонента, чем проходить полный цикл привязки ТК к СУ, а абонента к ТК;

-«Уровень полномочий» – здесь задается уровень полномочий абонента при работе на АП. При первоначальном развертывании сети рекомендуется устанавливать Максимальные полномочия. Это упростит развертывание сети, а в дальнейшем тому или иному абоненту всегда можно выслать обновление справочной информации и изменить его полномочия. Специальный уровень полномочий – может быть использован только специалистами ОАО «ИнфоТеКС» для отладки ПО;

-«Включать в дистрибутив» - менять, выставленную по умолчанию настройку следует только в том случае, если планируется создание большой VPN (~1000 СУ). В этом случае полный дистрибутив справочно-ключевой информации может достигнуть размера 1,5 Мбайта и выше, что не удобно при передаче конечному пользователю;

-«Автоматически регистрировать СУ» – здесь речь идет о регистрации СУ в прикладных задачах (ПЗ). Эти настройки можно вообще не трогать, т.к. программа сама следит за соответствием количества выданных лицензий и текущего количества зарегистрированных задач. В случае наличия проблем выдается предупреждение, и очередной СУ не регистрируется в задаче, приведшей к конфликту с лицензией. Более подробно вопрос регистрации АП в ПЗ мы рассмотрим ниже, на шаге 6(12).

В конечном итоге мы должны получить следующее окно настроек по умолчанию (Рис. 1.11.):

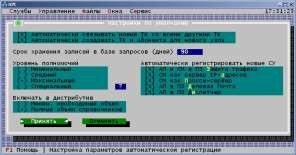


Рис. 1.11. Настройки по умолчанию.

Для активизации настроек жмем кнопку Принять и переходим к следующему шагу нашего занятия. Помните, что вы всегда можете вызвать контекстно-зависимую справку по каждому из окон программы, нажав клавишу <F1> на клавиатуре компьютера.

Шаг 4(12)

*Формирование транспортной структуры сети*

После завершения предыдущего шага программа выдаст окно с вопросом о вызове адресной администрации. Отвечаем утвердительно, нажав Да. После этого программа загружает утилиту формирования сетевого уровня защищенной сети (Рис. 1.12.).

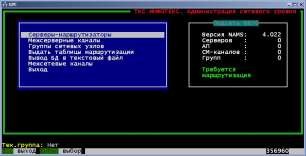


Рис. 1.12. Главное окно администрации сетевого уровня.

Далее, вспоминаем о шаге 1 в части, касающейся выработки структуры сетевого уровня (Рис. 1.2), и начинаем ее формировать, выбрав пункт «Серверы-маршрутизаторы» и нажав <Enter>. В появившемся окне запроса вводим имя первого сервера нашей будущей защищенной сети – «СМ Сервер Бухгалтерия» - жмем <Enter>. Программа отобразит окно «Серверы- Маршрутизаторы» и строку с именем вновь введенного сервера и его атрибутами. Для добавления еще одного сервера (Рис. 1.2), нажимаем сочетание клавиш <Alt>+<I>, вводим имя «СМ Сервер Плановый отдел».

Если необходимо изменить имя сервера, то достаточно «подсветить» этот сервер в меню и нажать <Alt>+<E>. Еще раз напомним, что подсказку по любому окну программы можно вызвать, нажав <F1>.

Теперь установим Межсерверный канал, как того требует наша структура. Для этого «подсвечиваем» «СМ Сервер Бухгалтерия» и нажимаем

<Alt>+<M>. Слева от записи должен появиться значок «\*>», сообщающий нам, что данный СМ выбран для образования канала. Далее, «подсвечиваем» второй сервер и опять жмем <Alt>+<M> - появиться значок «->». Последний шаг – нажимаем <Alt>+<C>, образовывая тем самым межсерверный канал. При этом атрибут «МСК» обоих серверов должен стать равным 00001.

В результате всех наших действий мы должны получить окно программы следующего вида (Рис. 1.13):

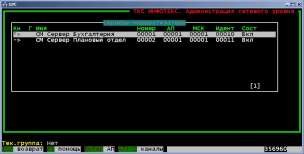


Рис. 1.13. Регистрация серверов-маршрутизаторов.

Сервера у нас уже есть, поэтому переходим к регистрации АП на этих СМ. Согласно структуре сетевого уровня (Рис. 1.2) к СМ Сервер Бухгалтерия мы должны привязать 3 АП: АП Мобильный компьютер (Кузовкин), АП Компьютер\_1 (Петров) и АП Компьютер\_2 (Сидоров, Васечкин). Чтобы это сделать, «подсвечиваем» «СМ Сервер Бухгалтерия» и нажимаем <Enter>. Откроется новое окно с пустым списком АП, привязанных к данному СМ. Добавление АП в этот список производится путем нажатия

<Alt>+<I>, введения имени АП и нажатия <Enter>. Проделав все это для СМ Сервер Бухгалтерия получим следующий список (Рис. 1.14):

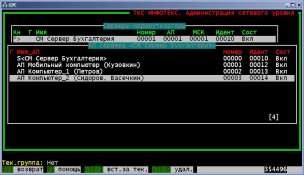


Рис. 1.14. Список АП СМ Сервер Бухгалтерия.

Теперь жмем <Esc>, «подсвечиваем» второй СМ и проводим аналогичные действия для СМ Сервер Плановый отдел. Это даст нам следующий список (Рис. 1.15.):

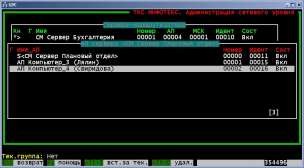


Рис. 1.15 Список АП СМ Сервер Плановый отдел.

Для завершения шага формирования сетевого уровня VPN выходим в основное меню программы (см. рис.1.12). Проверяем наличие межсерверного канала, войдя в пункт меню «Межсерверные каналы» (Рис. 1.16):



Рис. 1.16. Межсерверные каналы.

После этого в основном меню необходимо вызвать пункт «Выдать таблицы маршрутизации»; строка «Требуется маршрутизация» в правом поле окна программы должна погаснуть. Дополнительно, можно выдать отчет о сетевой структуре сети, вызвав пункт меню «Выдать БД в текстовый файл» и задав имя файла для сохранения отчета. Нажав <Esc> в основном меню утилиты формирования сетевой структуры, попадаем в основное окно ЦУС и завершаем этот шаг.

**Часть 3**

Шаг 5(12)

*Формирование прикладной структуры сети*

Формирование прикладной структуры будем производить в соответствии с выработанной на шаге 1 схемой (Рис. 1.3, 1.4). Так же, как и на первом шаге разобьем всю процедуру на два этапа: связывание ТК, их переименование и назначение областей видимости; привязку абонентов и их переименование.

Для реализации первого этапа из основного окна ЦУС вызываем Службы  Прикладная администрация  Регистрация типов коллективов… В итоге приходим к следующему окну (Рис. 1.17):

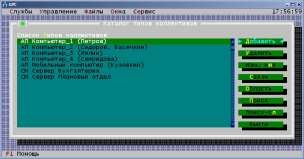


Рис. 1.17. Каталог типов коллективов.

Мы видим, что программа автоматически создала ТК с именами ранее созданных СУ (шаг 4). Если нажать Область, то мы также увидим, что вновь созданным ТК уже назначены области видимости. Все это программа проделала благодаря заранее выставленным нами настройкам по умолчанию (шаг 3). Все что осталось сделать на этом этапе: убрать из названия ТК заголовки «АП» и «СМ», заменив их на «ТК», для АП Компьютер\_2 (Сидоров, Васечкин) завести вместо одного два ТК (Рис. 1.3), удалить связь между ТК с абонентами Васечкиным и Петровым.

Первое выполняется путем «подсвечивания» необходимого ТК и нажатия кнопки Изм.имя. Вам будет предложено изменить уже существующее имя. После изменения нажимаем <Enter> и возвращаемся обратно в общий каталог ТК (Рис. 1.17).

Второе – ТК Компьютер\_2 (Сидоров, Васечкин) переименовываем в ТК Компьютер\_2 (Сидоров). Жмем Добавить и вводим имя нового ТК: «ТК Компьютер\_2 (Васечкин)». После нажатия кнопки Принять программа выдаст новое окно и предложит нам выбрать область видимости вновь созданного ТК; выбираем АП Компьютер\_2 (Сидоров, Васечкин) и жмем Принять. На вопрос программы о связи нового ТК с остальными отвечаем утвердительно.

Третье – «подсвечиваем» ТК Компьютер\_1 (Петров) и жмем Связи. В появившемся окне «подсвечиваем» ТК Компьютер\_2 (Васечкин) и нажимаем Удалить; подтверждаем удаление. Далее жмем Выйти или <Esc>.

В итоге всех манипуляций вид Каталога типов коллективов будет следующим (Рис. 1.18):



Рис. 1.18. Окончательный вид каталога ТК.

На этом необходимые операции с ТК можно считать законченными, поэтому переходим к следующему этапу: работе с абонентами. Для этого нажимаем в текущем окне Выйти или <Esc> и попадаем в основное окно ЦУС. Далее выбираем Службы  Прикладная администрация  Регистрация абонентов…, программа при этом должна выдать следующее окно (Рис. 1.19):

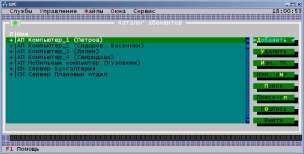


Рис. 1.19. Каталог абонентов.

Как мы видим, абоненты уже заведены, но программа выдала им имена тех СУ, к которым они относятся (связь через ТК). Поэтому, для начала, переименуем их в соответствии с разработанной схемой связей

прикладного уровня (Рис. 1.4). Для этого достаточно «подсветить» нужного абонента и нажать Изм. имя. Перед изменением имени желательно проконтролировать, к какому ТК относится тот или иной абонент. Чтобы это сделать, также «подсвечиваем» необходимого абонента в каталоге и жмем Изм. ТК.

Повышенное внимание следует уделить назначению абонентов Сидорова и Васечкина. Это связано с тем, что они оба должны быть зарегистрированы на одном СУ, но в разных ТК. Последовательность действий при этом должна быть следующей:

-«подсвечиваем» запись в каталоге «АП Компьютер\_2 (Сидоров, Васечкин)», жмем Изм . имя;

-в окне «Введите новое имя абонента» меняем имя на «Сидоров»;

-строку с псевдонимом оставляем пустой, т.к. псевдонимы можно всегда назначить позже из пользовательского ПО;

-жмем Принять и возвращаемся в окно каталога абонентов;

-«подсвечиваем» запись «Сидоров», нажимаем Изм. ТК и убеждаемся, что абонент Сидоров включен в ТК Компьютер\_2 (Сидоров). Возвращаемся по

<Esc> в предыдущее окно;

-нажимаем Добавить, в строке запроса вводим имя «Васечкин» и жмем

<Enter>;

-в новом окне «Список типов коллективов абонента» жмем Добавить, в окне

«Выберите тип коллектива» «подсвечиваем» ТК Компьютер\_2 (Васечкин) и нажимаем Принять;

-фиксируем для себя, что Васечкину назначен его ТК, созданный ранее при регистрации ТК, жмем <Esc> или Выйти.

Далее следует переименовать всех остальных абонентов, если это не было сделано ранее. В итоге получим следующее окно каталога абонентов (Рис. 1.20).

Значок «+» слева от записи абонента сообщает нам о том, что данному абоненту разрешено иметь собственную электронно-цифровую подпись. Изменение этого параметра производится путем нажатия на кнопку Подпись.

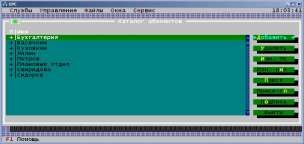


Рис. 1.20. Окончательный вид каталога абонентов.

Последнее, что осталось сделать – назначить абоненту Кузовкину в соответствии с п.10 задания и схемой связей прикладного уровня (Рис. 1.4)

ТК абонента Свиридовой. Для этого подсвечиваем запись «Кузовкин», нажимаем Изм. ТК. В появившемся окне жмем Добавить, выбираем «ТК Компьютер\_4 (Свиридова)» и нажимаем Принять. Получаем (Рис. 1.21).

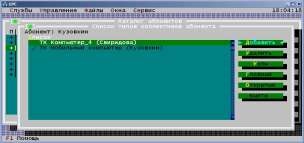


Рис. 1.21. Список ТК абонента Кузовкина.

Значок «» напротив записи «ТК Мобильный компьютер (Кузовкин)» говорит о том, что данный ТК является для абонента Главным, то есть тем ТК, куда данному абоненту будут приходить конверты транспортного уровня (защищенная почта и обновления). В нашем случае менять существующую настройку не стоит.

Нажимаем два раза <Esc> или Выйти. На этом шаг 5 можно считать пройденным.

Шаг 6(12)

*Регистрация СУ в прикладных задачах*

На шаге 3 уже шла речь о регистрации АП и СМ в ПЗ. Обратимся к пунктам меню программы, которые позволят нам индивидуально для каждого АП задавать регистрацию в тех или иных ПЗ. Для этого вызываем Службы  Прикладная администрация  Регистрация АП и СМ в ПЗ  Регистрация АП во всех ПЗ…, попадаем в окно, отображающее сводный список по регистрации АП во всех ПЗ. Регистрацию АП в конкретной ПЗ можно задавать и из других подпунктов пункта меню Регистрация АП и СМ в ПЗ (Службы  Прикладная администрация ). Ниже мы остановимся на рассмотрении одного из них, а сейчас вернемся к окну программы

«Регистрация АП в прикладных задачах». Как видите, программа, согласно настройкам по умолчанию (шаг 3), зарегистрировала наши АП во всех возможных ПЗ за исключением задач ЦУС и УКЦ (столбец «ЦК» в списке). Предполагается, что этот ответственный шаг необходимо выполнить вручную. Для этого мы должны «подсветить» тот АП, на котором предполагается держать ЦУС и УКЦ, нажать Регистрация и включить в появившемся окне пункты «ЦУС» и «Ключевой центр».



Рис. 1.22. Регистрация АП в ПЗ.

В принципе, допускается раздельная регистрация ЦУС и УКЦ на разных АП, но так как в задании такого требования нет, зарегистрируем эти задачи на АП администратора VPN Лялина. В итоге окно со списком АП должно принять вид (Рис. 1.22).Жмем <Esc> или Выйти и переходим к этапу регистрации СМ в ПЗ. Для этого вызываем Службы  Прикладная администрация  Регистрация АП и СМ в ПЗ  Сервер IP-адресов…(Рис. 1.23).

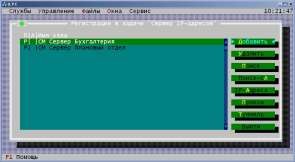


Рис. 1.23. Регистрация СМ в задаче «Сервер IP-адресов».

Здесь мы видим записи с именами наших СМ. Напротив записей стоят значки «P» – это говорит о регистрации наших серверов в задаче Proxy для защищенной сети. Если заранее известно, что такая функция не потребуется, то регистрацию можно снять нажатием кнопки Proxy. Если мы заранее знаем, на какие IP-адреса будут устанавливаться сервера, то их можно задать, нажав IP-Адреса. Это может облегчить настройку сети в дальнейшем. В нашем случае никаких требований на этот счет нет, поэтому в данном окне менять ничего не надо. Нажимаем <Esc> или Выйти и возвращаемся в основное окно ЦУС.

Шаг 7(12)

*Получение отчета по структуре защищенной сети*

Для получения отчета по структуре сети необходимо обратиться к пункту основного меню программы Службы  Выборки  Структура сети (Рис. 1.24). Далее, если мы хотим получить отчет в виде таблицы, необходимо выбрать пункт В широком формате… - программа отобразит содержание файла struct.rep, который и является отчетом. Однако, более удобным может оказаться отчет, выданный В узком формате… Отчет также будет помещен в файл struct.rep, который можно найти в подкаталоге NCC каталога установки ПО ViPNet.



Рис. 1.24. Получение отчета по структуре защищенной сети.

В принципе, данный шаг не является обязательным и может быть пропущен при формировании защищенной сети. Создание отчета по структуре VPN как при создании, так и при модификации VPN, можно считать одним из полезных правил администрирования, потому что позволяет не только самому администратору, но и специалистам ОАО «ИнфоТеКС» быстрее разбираться с возникающими вопросами по функционированию защищенной сети.

**Часть 4**

Шаг 8(12)

*Формирование всех справочников*

Это самый простой шаг – все вопросы с определением того, какие справочники должны быть сформированы при первоначальном развертывании, программа берет на себя. Убедиться в том, что вся информация о структуре сети была введена правильно можно в пункте меню Службы  Проверка конфигурации. Здесь должно быть выдано такое окно (Рис. 1.25):



Рис. 1.25. Информационное окно.

Если же такого окна нет, то необходимо вернуться к шагу 4 и проверить правильность выполнения всех шагов вплоть до данного. Ни в коем случае не следует продолжать процедуру формирования справочников, пока не будут выявлены и исправлены все аномальные ситуации!

А  этом вся необходимая информация будет передана в Ключевой Центр.

Шаг 9(12)

*Первоначальная настройка УКЦ*

Запускаем программу «Ключевой центр» (см. шаг 2). Первым делом, программа попросит указать тип пароля: «Собственный» или «Случайный» (Рис. 1.26). Выбрав первый тип и нажав Принять, мы попадем в окно ввода и подтверждения пароля. Вводим два раза пароль (не менее 5 символов) и жмем Принять. Если оба раза был введен один и тот же пароль, то программа предложит нам сделать настройки работы по умолчанию.

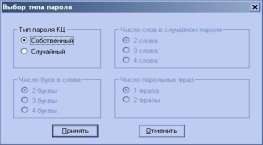


Рис. 1.26. Выбор типа пароля.

Если мы выбрали тип пароля «Случайный», то будут активизированы дополнительные настройки, позволяющие задать способ формирования случайного пароля. После нажатия на кнопку Принять, программа запустит электронную рулетку. Здесь, как и в первом случае (с «Собственным» паролем), нас попросят 8 раз нажать на заданные клавиши (ошибки не страшны). На основании информации о временных интервалах между

нажатиями клавиш программа выработает некое случайное число, которое будет использоваться для генерации всей ключевой информации в системе, в том числе и «Случайного» пароля. Как только будет отработана электронная рулетка, программа выдаст окно с выработанным паролем и парольной фразой.

**ВНИМАНИЕ!** Пароль для входа в УКЦ – это САМЫЙ важный пароль во всей системе, так как на нем производится шифрование мастер- ключей системы. Поэтому его ни в коем случае нельзя забывать и, уж тем более, сообщать неуполномоченным лицам. Потеря пароля УКЦ приведет к необходимости смены всех ключей в защищенной сети. При задании

«Собственного» пароля рекомендуется использовать как цифры, так и буквы со знаками препинания, сам пароль должен быть бессмысленным набором символов – это все усложнит его возможный взлом. Этот пароль после входа в УКЦ можно сменить.

После процедуры ввода пароля мы попадаем в окно настроек программы.

Первая вкладка «Каталоги приема /отправки» (Рис. 1.27):

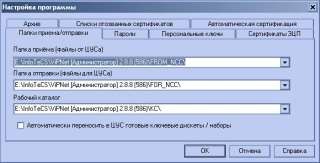


Рис. 1.27. Настройки УКЦ – Каталоги приема/отправки.

Здесь в строках ввода имен каталогов для связи с ЦУС программа уже содержит пути, используемые системой по умолчанию. Если при настройке ЦУС (шаг 2) пути по умолчанию не были изменены, то здесь менять пути тоже не следует, в противном случае необходимо проследить, чтобы имена каталогов для файлов ЦУС и УКЦ совпадали в обеих программах.

В нижней части окна можно настроить УКЦ для автоматического переноса сформированной ключевой информации в ЦУС. Делать этого в нашей работе при первоначальном развертывании сети не следует, потому как сформированная ключевая информация потребуется нам именно в УКЦ. Переходим к следующей вкладке «Пароли» (Рис. 1.28).

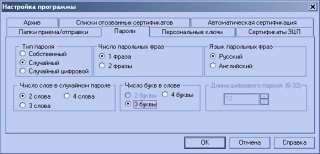


Рис. 1.28 Настройки УКЦ – Пароли

Выбираем тип задания пароля для АП. Здесь процедура полностью аналогична вышеописанной. Рекомендуется выбирать «Случайный» тип пароля. Это освободит вас от ручного ввода пароля для всех АП. При этом рекомендуем выбрать минимальное значение пароля (одна фраза на русском из двух слов, из которой будет взято по три буквы!) В дальнейшем каждый пользователь АП сможет самостоятельно поменять свой пароль. Все остальные настройки (вкладки «Персональные ключи», «Сертификаты ЭЦП», «Архив», «Списки отозванных сертификатов» и «Автоматическая сертификация») оставляем без изменений. В случае необходимости следует обратиться к документации пользователя по программе Ключевой Центр. Нажимаем кнопку Ok и переходим к следующему шагу.

Шаг 10(12)

*Определение главных абонентов сети и формирование для них персональной ключевой информации*

После принятия настроек УКЦ программа выйдет в свое основное окно. Для определения главных абонентов в сети необходимо выбрать меню Конфигурация  Главные абоненты. Попадаем в окно выбора Главных абонентов защищенной сети (Рис. 1.29):

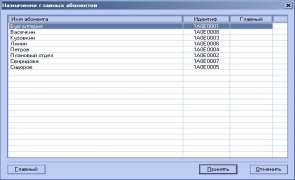


Рис. 1.29. Выбор Главных абонентов.

Логично выбрать в качестве Главного абонента Администратора защищенной сети (Лялин). Назначать Главным абонентом другое лицо имеет смысл только лишь в случаях, специально оговоренных требованиями безопасности. Поэтому «подсвечиваем» запись с абонентом Лялиным и жмем Главный. Справа от идентификатора этого абонента должна появиться звездочка (Рис. 1.29). Так как больше Главных абонентов задавать не нужно, то жмем Принять. Следующим действием будет формирование основного мастер-ключа. В основном окне УКЦ выбираем меню Программа  Генерация мастер-ключей  Основной мастер-ключ, в результате мы должны на экране увидеть следующее окно (Рис. 1.30). Внимательно читаем содержимое окна и нажимаем Создать мастер-ключ. Подтверждаем свои действия, кликнув Ok. Еще раз жмем Ok.

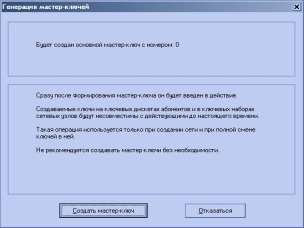


Рис. 1.30. Генерация мастер-ключей.

Теперь программа готова к формированию КД для главного абонента. В левой части окна программы УКЦ выбираем раздел Ключевой центр  Абоненты  Своей сети. В выпавшем окне (Рис. 1.31) нам будет предложено выбрать абонентов, для которых в первую очередь будут сгенерированы Ключевые Дискеты (КД). Здесь выделяем только Главного абонента – для всех остальных КД вообще не нужны (им сразу автоматически будут сделаны дистрибутивы справочно-ключевой информации).

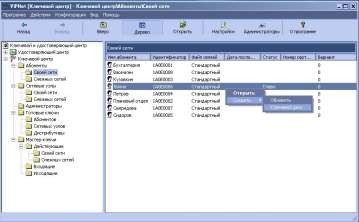


Рис. 1.31. Формирование КД.

После выделения нажимаем на правую кнопку мыши, выбираем Создать, потом Ключевой диск. В следующем окне подтвердим желание создать Ключевой диск для абонента Лялина. После этого мы увидим Сведения о запросе на сертификат (Рис. 1.32). Более подробную информацию о полях на закладках Субъект, Срок действия, Открытый ключ и Статус можно найти в документации. Все эти настройки оставляем без изменений. В случае необходимости следует обратиться к документации пользователя по программе Ключевой Центр. Нажимаем кнопку Ok и переходим к следующему шагу.

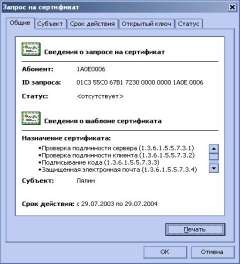


Рис. 1.32. Запрос на сертификат.

Далее, вводим каталог расклейки КД Главного абонента, то есть тот каталог, куда будут помещены файлы с ключами, образующие КД абонента. Так как Главным абонентом у нас является Администратор, то каталогом расклейки должен стать подкаталог SS (клиентская часть места Администратора защищенной сети) каталога установки ПО ViPNet. Поэтому в окне запроса каталога указываем «..\SS\» и жмем Принять. Программа выдаст окно с паролем Главного абонента – Администратора VPN. Этот пароль следует запомнить, так как программа в дальнейшем потребует его ввести. Нажимаем Принять, затем Ok.. Если теперь просмотреть содержимое каталога SS, то мы увидим в нем новый подкаталог KEY\_DISK с расклеенной КД Главного абонента.

Осталось лишь нажать кнопку Закрыть и перейти к следующему шагу нашего занятия.

Шаг 11(12)

*Генерация ключевой информации для всех остальных объектов сети*

Вызываем пункт меню Программа  Автоматическое формирование ключей (Рис. 1.33). Вводим пароль Главного абонента (см. сноску к шагу 10).

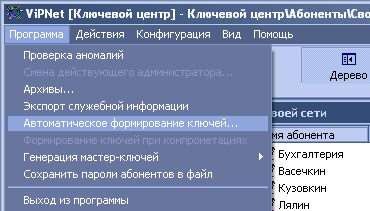


Рис. 1.33 . Пункт меню Автоматическое формирование ключей.

Далее программа сообщит нам, что не смогла найти каталог с ключами Главного абонента, поэтому следует нажать Ввести каталог и в появившемся окошке ввести вручную «..\SS\», либо по кнопке Найти указать соответствующий каталог. Далее, запомнить пароль Администраторов АП – это тот пароль, с которым можно, зная пароль конкретного АП, войти на него с полномочиями администратора. После нажатия кнопки Принять, попадаем в окно автоматической генерации ключевой информации. Жмем Старт и ждем, пока программа сформирует все что необходимо. Для каждого абонента будет открыто окно Запрос на сертификат, в котором этот запрос будет необходимо подтвердить. После окончания всех процедур будет получено окно с информацией о завершении процесса генерации ключевых дискет и наборов. Нажимаем Закрыть.

Вот и все с этим шагом – программа сделала все сама, максимально облегчив нам процедуру формирования ключевой информации.

Шаг 12

*Распределение готовых ключей и справочников*

Ну вот, мы и подошли к заключительному шагу нашего занятия. Нам осталось распределить уже готовую справочно-ключевую информацию между объектами защищенной сети. Проще всего это будет сделать для обычных АП, чуть сложнее для Главного абонента – Администратора VPN. Но обо всем по порядку.

Начнем с Главного абонента. В левой части окна выбираем раздел Ключевой центр  Готовые ключи  Сетевых узлов (Рис. 1.34).

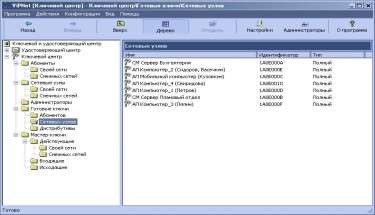


Рис. 1.34. Пункт меню Готовые ключи сетевых узлов

Попадаем в окно со списком готовой ключевой информации (КН) для АП (Рис. 1.35). Большая часть ключей, которые здесь представлены, нам не нужны – это ключи всех АП VPN. Сейчас нас должен интересовать только ключевой набор для АП Главного абонента.

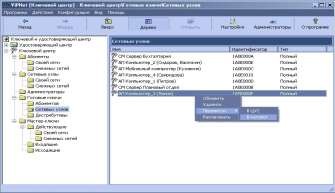


Рис. 1.35. Готовый КН для Администратора.

Его необходимо расклеить вручную, так как программа сама этого делать не будет. Для этого «подсвечиваем» запись «АП Компьютер\_3 (Лялин)» и по нажатию на правую кнопку мыши в выпадающем меню выбираем пункт Перенести - В каталог. В качестве каталога расклейки указываем опять «..\SS\» и жмем Принять. После того, как расклейка будет завершена, и мы нажмем Ok, из записей окна должна исчезнуть запись для вышеозначенного АП. Те ключи, что остались желательно удалить во избежание возможных накладок в дальнейшей работе. Для этого выбираем все остальные КН и удаляем. Если теперь «пойти» в каталог SS, то там, в подкаталоге STATION, можно обнаружить файлы с ключами, составляющими КН данного АП. Ключевые дискеты в разделе Ключевой центр - Готовые ключи – Абонентов нам по отдельности также не нужны, поэтому мы их можем также смело удалять.

Для всех остальных АП существуют дистрибутивы справочно- ключевой информации (файлы \*.dst). Чтобы их найти выбираем пункт меню Ключевой центр  Готовые ключи  Дистрибутивы (Рис. 1.34) и попадаем в окно со списком сформированных дистрибутивов (Рис. 1.36). Заметьте, в этом списке отсутствует дистрибутив для Главного абонента. Далее, нажимаем Выбрать всех и Перенести. В окошке ввода каталога для переноса дистрибутивов указываем какой-нибудь каталог, например, заранее созданный каталог «FULL». Жмем Принять. Исходное окно должно очиститься; нажимаем Закрыть. Теперь в каталоге установки ПО ViPNet в подкаталоге FULL в подкаталогах с именами АП и абонентов лежат требуемые полные дистрибутивы для начальной инсталляции АП и СМ. Их можно переносить на дискеты и раздавать абонентам защищенной сети.

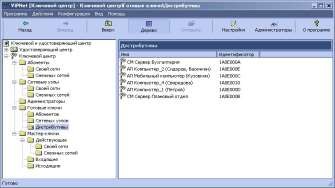


Рис. 1.36. Дистрибутивы для начальной инсталляции.

Последний вопрос по работе УКЦ, который осталось разобрать на этом занятии – это «откуда брать пароли абонентов?». Для ответа на этот вопрос необходимо выбрать раздел Ключевой центр  Абоненты  Своей сети. В этом окне можно просмотреть все пароли отдельно для каждого из абонентов, дважды нажимая на левую кнопку мыши, а можно выбрать пункт меню Программа - Сохранить пароли в файле (Рис. 1.37) и, указав имя файла, сохранить его в выбранном каталоге (рекомендуется ранее созданный FULL). Посмотреть данные о сертификатах каждого из абонентов можно в окне Программа – Удостоверяющий центр – Сертификаты – Абонентов своей сети

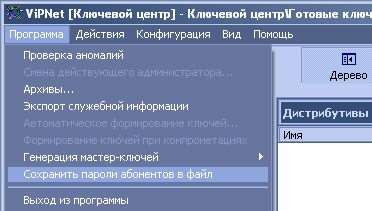


Рис. 1.37. Дистрибутивы для начальной инсталляции.

На этом работу с УКЦ можно считать законченной, поэтому закрываем все окна и саму программу. При закрытии программа спросит, хотим ли мы сохранить рабочие файлы в архиве – необходимо ответить утвердительно.

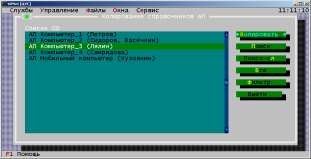


Рис. 1.37. Копирование справочников АП.

Возвращаемся в ЦУС. Здесь мы должны будем скопировать справочники для АП Главного абонента (3-ий, последний этап в создании справочно-ключевой информации для Главного абонента). Для этого вызываем пункт меню Службы Справочники АП Копирование…, в появившемся окне (Рис. 1.37). «Подсвечиваем» запись «АП Компьютер\_3 (Лялин)» и жмем Копировать. В окне запроса каталога для копирования указываем «..\SS\» и нажимаем Принять. Теперь необходимо открыть любой файловый менеджер, зайти в подкаталог SS каталога установки ПО ViPNet и из подкаталога с названием в виде шестнадцатеричного числа перенести все файлы справочников в корень SS. Сам каталог следует удалить.

Закрываем программу ЦУС, при этом также будет создан архив с рабочими файлами программы. Выполнение шага 12 и всего занятия можно считать законченным.

*Подведение итогов занятия:*

В ходе выполнения занятия мы получили полный набор справочно- ключевой информации для развертывания защищенной сети на СУ и целиком установленное место на АП Администратора защищенной сети. Компьютер с этим АП теперь можно перегрузить. Заметьте, что ввод пароля для входа на АП защищенной сети запрашивается до ввода обычного пароля для входа в систему (WinNT,Win2k) или «сетевого» пароля (Win9x). Это позволяет удовлетворить те или иные требования по защите от НСД не только для входа в защищенную сеть, но и для загрузки самой операционной системы, усиливая тем самым ее стандартные средства подобного рода.

Установка АП абонентов VPN производится очень просто: достаточно запустить Setup.exe из комплекта ViPNet Клиент, ответить на вопросы программы инсталляции (они во многом аналогичны тем, на которые мы отвечали в ходе выполнения шага 2), не перегружая операционную систему, скопировать файл \*.dst с дистрибутивом справочно- ключевой информации в корень каталога установки (туда, где находятся все файлы ПО ViPNet Клиент); перегрузить систему, ввести пароль данного

абонента VPN и получить загруженный и готовый к работе АП защищенной сети.

В качестве рекомендации к занятию хотелось бы посоветовать еще раз обратиться к шагу 1 и уяснить себе все этапы его прохождения, сверяясь с заданием к занятию. Научившись составлять схемы защищенных сетей, исходя из реальных требований к реальным сетям, вы сможете в дальнейшем, без какого-либо труда, администрировать защищенную сеть.

### Вопросы к лабораторной работе №1

1.Что является единицей разграничения доступа в защищенной сети? 2.Зачем нужны списки рассылки копий?

3.Что нужно сделать в ЦУС, чтобы заново начать генерацию DST файлов?

4.Что должен сделать администратор при смене мастер - ключа?

5.Что содержится в DST файле?

6.Где задаются полномочия (права доступа пользователя)?

7.Для какой программы задаются полномочия?

8.Что происходит при нажатии кнопки «Сформировать все справочники» в

«ЦУС»?

9.Что такое сетевой узел?

10.Главные абоненты – зачем они? 11.Где хранится Мастер Ключ?

12.Что находится на ключевой дискете? 13.Для чего служит ключевой набор?

# Лабораторная работа№2 «Модификация защищенной сети ViPNet»

#### Цель занятия:

Целью данного занятия является получение опыта в модификации защищенных сетей ViPNet по заданной желаемой схеме. Также необходимо научиться четко понимать, что делают ЦУС и КЦ на каждом шаге, какие файловые ресурсы при этом используются. Подобные знания в дальнейшем позволят грамотно и безошибочно осуществлять модификацию защищенной сети ViPNet.

**Содержание занятия:**

Описываются все шаги необходимые для модификации защищенной сети ViPNet, включающие:

Анализ VPN, созданной на Практическом занятии № 1. Изменения в Адресной администрации ЦУСа.

Изменения в Прикладной администрации ЦУСа.

Формирование новых адресных справочников и справочников для КЦ. Формирование новой ключевой информации в КЦ.

Передача сформированной ключевой информации в ЦУС. Рассылка обновлений из ЦУСа.

Проверка прохождения обновлений из ЦУСа.

Настройка транспортного модуля на АП Компьютер\_3 (Лялин).

Обновление адресной и ключевой информации на АП Компьютер\_3 (Лялин). Контроль прохождения обновления

#### Задание на выполнение лабораторной работы

Модифицировать защищенную сеть ViPNet в соответствии с приведёнными ниже требованиями и схемой (см. рис. 1.1, 1.2).

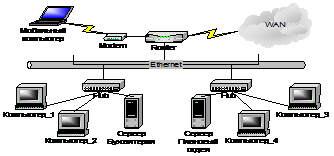


Рис. 1.1. Физическая схема исходной сети.



Рис. 1.2. Физическая схема модифицированной сети.



АП

Мобильный компьютер (Кузовкин)

Межс ерверный канал

АП

Компьютер 1 (Петров)

АП

Компьютер 2 (Сидоров, Вас ечкин)

АП

Компьютер 3 (Лялин)

АП

Компьютер 4 (Свиридова)

СМ

Сервер Плановый отдел

СМ

Сервер Бухгалтерия

Рис. 1.3. Логическая схема исходной защищенной сети.



АП

Мобильный компьютер (Кузовкин)

Межс ерверный канал

АП

Компьютер 5

АП

Компьютер 2 (Сидоров, Вас ечкин)

АП

Компьютер 3 (Лялин)

АП

Компьютер 4 (Свиридова)

СМ

Сервер Плановый отдел

СМ

Сервер Бухгалтерия

Рис. 1.4. Логическая схема модифицированной защищенной сети.

На схемах кружками обозначены абонентские пункты – рабочие станции, на которые будет производиться установка ПО ViPNet Клиент, квадратами – рабочие станции или сервера с установленным на них ПО ViPNet Координатор. Стрелками показаны связи транспортного уровня или – *пути следования транспортных конвертов* (писем Деловой Почты, файлов, отправляемых через защищенный Файловый обмен, служебных файлов системы).

Условия модификации защищённой сети:

Наличие сети (Рис. 1.3.), созданной на занятии №1, в состав которой входят: два СМ (Сервер Бухгалтерия и Сервер Плановый отдел) и пять АП (по два на каждом СМ: Компьютер\_1, Компьютер\_2 и Компьютер\_3, Компьютер\_4, Мобильный компьютер), на одном из АП зарегистрировано 2 абонента: Сидоров и Васечкин (на Компьютере\_2). Более подробное описание сети можно найти в Задании № 1.

*Задание по модификации защищенной сети:*

1.Добавить в структуру сети АП Компьютер\_5 и удалить АП Компьютер\_1.

2.Настроить транспортный модуль MFTP для обновления АП Компьютер\_3 в условиях отсутствия развернутого СМ.

3.Провести обновление АП Компьютер\_3.

Для закрепления полученных навыков требуется модифицировать полученную защищенную сеть в соответствии со своим вариантом. Вариант выбирается согласно последней цифре студенческого билета.

*Вариант 0.*Смена основного мастер ключа. 1.Изменить в УКЦ Основной Мастер-Ключ.

2.Провести обновление и проконтролировать его на АП Компьбтер\_3 (Лялин).

*Вариант 1.Добавление нового ТК с новым пользователем.*

1.Добавить на АП Компьютер\_5 новый ТК Комп\_55 с новым пользователем Селиным.

2.Провести обновление АП Компьбтер\_3 (Лялин).

*Вариант2. Удаление старого ТК без компрометации его пользователя* 1.Удалить на АП Компьютер\_5 старый ТК Компьютер\_5 со старым пользователем.

2.Провести обновление АП компьютер\_3 (Лялин).

*Вариант3.Добавление нового пользователя.*

1.Добавить в ТК Компьютер\_4 нового пользователя Савинова. 2.Провести обновление АП компьютер\_3 (Лялин).

*Вариант4.Удаление пользователя без компрометации.* 1.Удалить на АП Компьютер\_4 пользователя Свиридову. 2.Провести обновление АП компьютер\_3 (Лялин).

*Вариант5.Удаление связей коллективов.*

1.Для ТК компьютер\_3 (Лялин) удалить связь с ТК Компьютер\_5 (Селин). 2.Провести обновление АП компьютер\_3 (Лялин).

*Вариант6.Добавление новых связей коллективов*

1.Для ТК Компьютер\_3 (Лялин) добавить связь с ТК Компьютер\_5. 2.Провести обновление АП компьютер\_3 (Лялин).

*Вариант7.Изменение имени СУ, ТК, Пользователя.*

1.Изменить имя АП Компьютер\_5 на имя АП Селин.

2.Измеить имя ТК Компьютер\_3 (Лялин) на новое имя ТК Лялин. 3.Изменить имя пользователя Свиридова на новое имя Кукушкина. 4.Провести обновление АП компьютер\_3 (Лялин).

*Вариант8.Удаление пользователя с компрометацией.*

1.Удалить на АП Компьютер\_2 пользователя Сидорова с компрометацией. 2.Провести обновление АП компьютер\_3 (Лялин).

*Вариант9.Компрометация пользователя без его удаления*. 1.Скомпроментировать на АП Компьютер\_2 пользователя Васечкина. 2.Провести обновление АП компьютер\_3 (Лялин).

***3.Последовательность выполнения занятия*.**

**Часть 1**

**Шаг 1(10)**

*Анализ VPN, созданной на Практическом занятии № 1*.

Для начала необходимо просмотреть схему существующей защищенной сети, чтобы понять, что мы собираемся модифицировать. Для этого заходим в ЦУС (Рис.2.1.), выбираем пункт меню *Службы*  *Адресная администрация*  *Адреса в сети Инфотекс* (Рис. 2.2) и попадаем в соответствующее окно (Рис. 2.3). Выбираем пункт *Серверы- маршрутизаторы*, перед нами список СМ (Рис. 2.4). В этом же окне в столбце *Сост* (Состояние) можно определить – включен СМ или выключен. Чтобы проверить наличие АП на конкретном СМ, устанавливаем курсор на запись об интересующем нас СМ и нажимаем клавишу «*Enter*», попадаем в окно (Рис. 2.5), содержащее список АП на данном СМ.

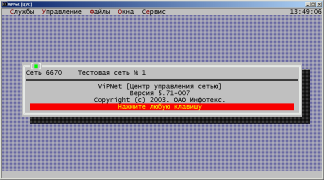


Рис. 2.1. Стартовое окно при запускеЦУСа.



Рис. 2.2. Меню Адресной администрации.

Для проведения анализа связей между ТК в нашей защищенной сети необходимо просмотреть содержимое меню *Прикладная администрация*  *Регистрация типов коллективов* (Рис. 2.7) – в этом меню мы сможем просмотреть связи между ТК и сделать соответствующие выводы в отношении их пересмотра.

Шаг 2(10)

*Изменения в Адресной администрации ЦУСа.*

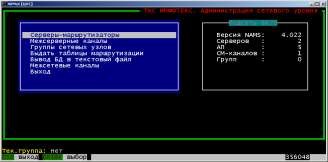


Рис. 2.3. Меню «Адреса в сети Инфотекс...».

В адресной администрации удаляем АП Компьютер\_1 (Петров), ранее заведенный на СМ Сервер Бухгалтерия. Для этого устанавливаем курсор на запись *АП Компьютер\_1 (Петров)* и нажимаем комбинацию клавиш «*Alt+d*», на вопрос отвечаем «*Да*»*.*



Рис. 2.4. Список существующих в защищенной сети СМ.

После этого, на этом же СМ, заводим новый АП Компьютер\_5 с помощью комбинации клавиш «*Alt+i*»*.* В результате – получим окно, представленное на рис. 2.6.

Затем два раза нажимаем клавишу «Esc», выбираем пункт «Выдать таблицы маршрутизации» (Рис. 2.3) и «Выход».

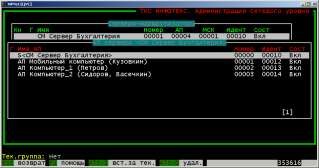


Рис. 2.5. Список АП, заведенных на СМ Сервер Бухгалтерия.

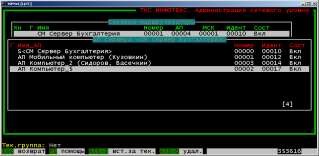


Рис. 2.6. Новый список АП на СМ Сервер Бухгалтерия.

Шаг 3(10)

*Изменения в Прикладной администрации ЦУСа*.

В прикладной администрации необходимо вручную удалить абонента Петрова (ЦУС не делает этого автоматически, поскольку абонент может входить в другие ТК, определенные на других АП или СМ). Для этого выбираем пункт «*Регистрация абонентов...*» (Рис. 2.7), устанавливаем курсор на записи *Петров* и нажимаем кнопку «*Удалить*», на вопрос отвечаем «*Да*».



Рис. 2.7. Меню Прикладной администрации.

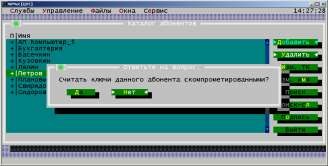


Рис. 2.8. Вопрос о компрометации ключей при удалении абонента.

ЦУС спросит о необходимости компрометации ключей данного абонента (Рис. 2.8), на этот вопрос отвечаем «*Нет*», поскольку мы просто удаляем абонента, а не вводим в действие процедуру Компрометации.

После этого, как и в первом занятии, изменяем имя вновь заведенного абонента на *Компьютер\_5*. Для этого устанавливаем курсор на записи *АП Компьютер\_5* и нажимаем кнопку «*Изм. имя*» (Рис. 2.9). Нажав на кнопку

«*Изм. ТК*», можно посмотреть в какой именно ТК входит новый абонент – ТК должен быть *АП Компьютер\_5*. Новый список абонентов будет выглядеть как на Рис. 2.9.

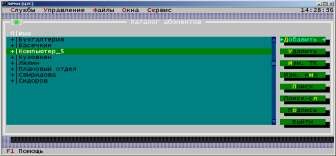


Рис. 2.9. Список зарегистрированных абонентов.

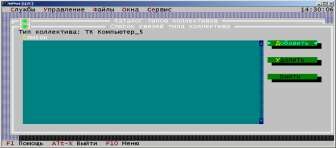


Рис. 2.10. Пустой список связей нового ТК .

Затем переходим в меню «*Регистрация типов*

*коллективов...*» (Рис. 2.7) и изменяем имя нового ТК с *АП Компьютер\_5* на *ТК компьютер\_5* (кнопка «*Изм. имя*»). Нам необходимо проверить связи нового ТК – нажимаем кнопку «*Связи*» и, в случае пустого или не полного списка ТК (Рис. 2.10), нажимаем кнопку «*Добавить*». Программа отобразит список ТК, с которыми на данный момент связи не заданы

выбираем все (кнопка «*Все*», затем кнопка «*Принять*»).

Осталось выйти в основное меню ЦУСа (два раза нажать клавишу «*Esc*») и сформировать необходимые справочники для КЦ, на основе которых будет сформирована новая ключевая информация.

Шаг 4(10)

*Формирование новых адресных справочников и справочников для КЦ.*

*Справочники можно сформировать двумя способами:*

* 1. Способ (простой):в меню *Службы* выбрать пункт *Сформировать все справочники* и программа сама сформирует все необходимые справочники в соответствии с последними изменениями в Адресной и Прикладной администрациях (*рекомендуется*);
  2. Способ (сложный):при модификации защищенной сети изменяются адресные справочники АП или СМ и ключевые наборы (меню *Службы*) ( *ключевые дискеты НЕ ИЗМЕНЯЮТСЯ!!!, т.к. не содержат ключей*

*шифрования, а только индивидуальную для абонента информацию*). Соответственно, необходимо сформировать:

*Справочники АП (СМ...);*

*Справочники КЦ*  *Справочники связей сетевых узлов...*

В обоих случаях выбираются те СУ, для которых необходимо сформировать новую адресную и ключевую информацию и нажимается кнопка «*Копировать*», копируем в каталог по умолчанию, который предложит ЦУС.

*Справочники КЦ*  *Дистрибутивы*  *Полный объем...*  кнопка

«*Копировать*»  каталог по умолчанию *– только для новых СУ!!!*

Внимание! Формировать справочники следует только при отсутствии

аномальных ситуаций!!! Если они есть – необходимо сначала их устранить.

**Часть 2**

Шаг 5(10)

*Формирование новой ключевой информации в КЦ.*

Загружаем программу Ключевой Центр. После ввода пароля КЦ, программа выдаст сообщение о наличии незарегистрированных в ЦУСе абонентах (Рис. 2.11). Это свидетельствует о том, что в КЦ (меню *Программы*

 *Просмотр*  *Список абонентов*) пока еще присутствуют абоненты,

которых мы уже удалили в ЦУСе и информации о них нет в справочниках. Этих абонентов необходимо удалить (кнопка «*Удалить всех*»). Программа попросит ввести пароль главного абонента и после удаления выдаст соответствующее сообщение (Рис. 2.12).



Рис. 2.11. Окно удаления незарегистрированных в ЦУСе абонентов.



Рис. 2.12. Окно подтверждения успешного удаления.

Теперь можно сформировать новую ключевую информацию согласно произведенным в ЦУСе изменениям. Выбираем меню *Действия*  *Автоматическое формирование ключей* (Рис. 2.13). КЦ загрузит подпрограмму *Электронная рулетка* и выдаст приглашение для начала генерации ключевой информации. Нажимаем кнопку «*Создать*», программа формирует ключевую информацию.

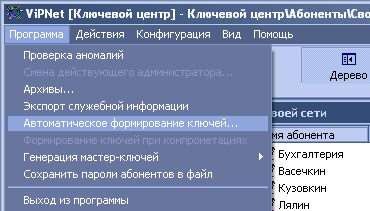


Рис. 2.13. Автоматическое формирование ключей.

Шаг 6(10)

*Передача сформированной ключевой информации в ЦУС.*

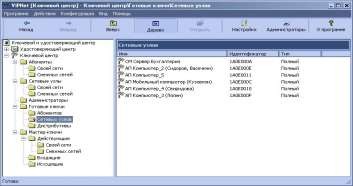


Рис. 2.14. Список готовых КН.

После того как ключи сгенерированы, новые ключевые наборы необходимо перенести в ЦУС и разослать абонентам VPN. Для этого переходим в раздел *Ключевой центр*  *Готовые ключи*  *Сетевых узлов* (Рис. 2.14).

Здесь представлен список готовых КН для всех ранее заведенных и нового СУ. Для нового абонента Компьютер\_5 создан дистрибутив для начальной инсталляции, поэтому его КН отдельно нас не интересуют – мы его удаляем. Все остальные КН переносим в ЦУС, для чего выделяем все СУ и по нажатию правой кнопки мыши в контекстном меню выбираем пункт *Перенести - в ЦУС*. КД нового абонента, также как и КН его СУ отдельно нам не нужен, поэтому его можно удалить из раздела *Ключевой центр*  *Готовые ключи*  *Абонентов*.

Если мы не будем завершать процедуры формирования ключей переносом их в ЦУС, расклеивания или удаления, то рано или поздно в соответствующих разделах *Ключевой центр*  *Готовые ключи* может быть накоплено большое количество готовых ключей. Поэтому логически правильно завершать работу с УКЦ одной перечисленных выше функций переноса/удаления.

Дистрибутив для начальной инсталляции нового абонента необходимо сохранить на жесткий диск (например, в каталог.. \FULL\). Для этого выбираем меню *Ключевой центр*  *Готовые ключи*  *Дистрибутивы*, в контекстном меню выбираем пункт *Перенести – В каталог* и указываем путь ..\FULL\.

После этого можно перезаписать файл с паролями абонентов – меню

*Программа*  *Сохранить пароли абонентов в файл* (Рис. 2.15).

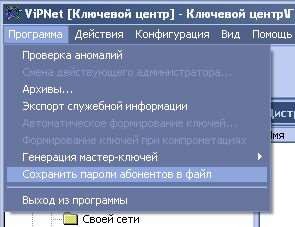


Рис. 2.15. Список абонентов.

Шаг 7(10)

*Рассылка обновлений из ЦУСа.*

Всё что осталось сделать для завершения модификации сети - разослать обновления. Для этого возвращаемся в ЦУС и выбираем меню *Управление*  *Отправить измененные файлы* (Рис. 2.16).

Для всех ранее заведенных и функционирующих СУ разослать обновления можно сразу. Чтобы это сделать – поочередно заходим в пункты меню *Справочники АП и СМ...* и *Ключевые наборы для СУ...*, выбираем функционирующие СУ с помощью кнопки «*Все*» или клавиши «*Insert*» (в меню *Справочники АП и СМ...* помимо функционирующих СУ будет присутствовать и новый СУ – *АП Компьютер\_5* – для него выслать обновление не получиться, т.к. *АП Компьютер\_3 (Лялин)* **пока еще о нем ничего не знает!!!** Отправить справочники для вновь заведенного СУ можно только после обновления самого *АП Компьютер\_3 (Лялин)*, т.е. после того как он получит новые адресные справочники, в которых будет прописана связь с новым ТК, и новый КН с ключами шифрования для связи с новым

АП) и нажимаем кнопку «*Отправить*» (Рис. 2.17). Перед нами появляется диалоговое окно, в котором необходимо установить дату и время проведения обновления (по умолчанию устанавливается задержка на 24 часа). Чтобы обновление произвести «немедленно», необходимо установить время проведения обновления «задним числом». Нажимаем кнопку «*Принять*».

Внимание! Таким образом отправить необходимо и адресные справочники (меню *Управление*  *Справочники АП и СМ...*) и ключевые наборы (меню

*Управление*  *Ключевые наборы для СУ...*).

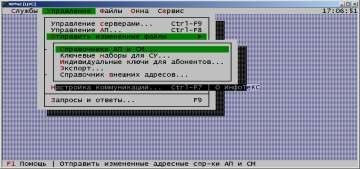


Рис. 2.16. Меню *Управление* ЦУСа.

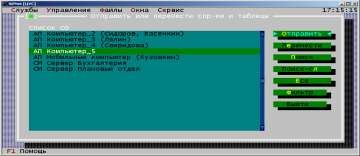


Рис. 2.17. Список готовых к отправке справочников и таблиц.

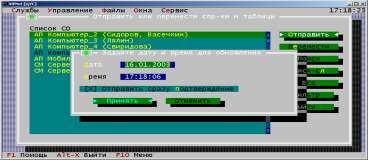


Рис. 2.18. Установка даты и времени проведения обновления на СУ.

Шаг 8(10)

*Проверка прохождение обновления из ЦУСа.*

После рассылки обновлений, в качестве контроля над процессом, необходимо проверить прошло ли оно, для этого можно воспользоваться Журналом Запросов и Ответов в ЦУСе. Для этого необходимо выбрать меню *Управление*  *Запросы и ответы...* или просто нажать клавишу F9. В появившемся окне (Рис. 2.19) можно задать необходимые параметры для

поиска и потом нажать кнопку «*Принять*». По кнопке F1 можно вызвать подсказку по работе с журналом.

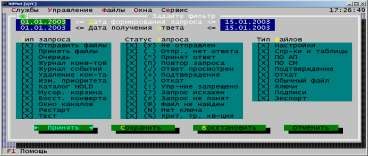


Рис. 2.19. Настройка журнала запросов и ответов.

В появившемся журнале (Рис. 2.20) можно проконтролировать отправку обновлений, получение подтверждений и, в том случае, когда обновление отправлено с временной задержкой, можно выслать квитанцию (при необходимости), которая отменит высланное с задержкой обновление – для этого необходимо выбрать обновление, которое Вы хотите отменить и нажать кнопку «*Откат*» (Рис. 2.20).

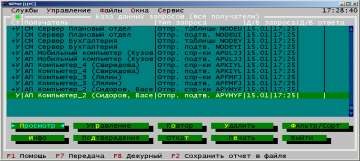


Рис. 2.20. Журнал запросов и ответов.

Шаг 9(10)

*Настройка транспортного модуля на АП Компьютер\_3 (Лялин).*

Чтобы убедиться в правильности произведенной модификации защищенной сети, перенастроим транспортный модуль MFTP *АП Компьютер\_3 (Лялин)* и посмотрим, как проходит процесс обновления на СУ. Для этого необходимо загрузить программу *Монитор* – в окне *Защищенная сеть* можно увидеть список СУ согласно заданию на Практическое занятие

№ 1 (Рис. 2.21).

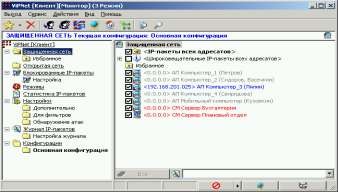


Рис. 2.21. Окно *Монитора* не модифицированной защищенной сети.

Модифицированную структуру защищенной сети (без *АП Компьютер\_1 (Петров)*, но с *АП Компьютер\_5*) мы сможем увидеть только после проведения обновления. В правом нижнем углу окна Монитора есть три кнопки (Рис. 2.21) – нас интересует самая правая – кнопка запуска транспортного модуля MFTP. Нажимаем ее. В трее появляется иконка транспортного модуля. Нажимаем на нее левой клавишей мышки и перед нами появляется окно транспортного модуля MFTP (Рис. 2.22).

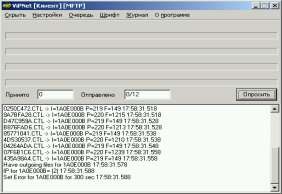


Рис. 2.22. Транспортный модуль MFTP.

Нажимаем меню *Настройки.* В появившемся окне (Рис. 2.23) два раза кликаем левой клавишей мышки на записи для *АП Компьютер\_3 (Лялин)*. Перед нами появляется новое окно (Рис. 2.24), в котором необходимо выбрать:

* установить *Тип канала –* MFTP;
* установить *Период опроса* – 10..15 секунд;
* включить *Вызывать узел по нажатию кнопки «Опросить»*;
* включить *Вызывать узел при наличии конвертов для него*;
* указать IP-адрес *АП Компьютер\_3 (Лялин)* (его можно посмотреть в окне *Защищенная сеть* в Мониторе [при необходимости нужно снять галочку с пункта меню *Инструменты* *Не отображать IP-адрес в списке*

*<Защищенная сеть>*] – запись выделена синим цветом).

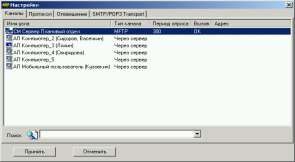


Рис. 2.23. Окно *Настройки* транспортного модуля MFTP.

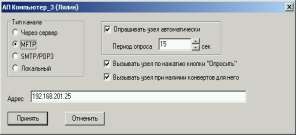


Рис. 2.24. Окно настроек канала работы СУ *АП Компьютер\_3 (Лялин)*.

После этого нажимаем кнопку «*Принять*», перед нами появиться окно *Настройки* транспортного модуля, содержимое которого немного измениться (Рис. 2.25). Еще раз нажимаем кнопку «*Принять*» - теперь транспортный модуль MFTP *АП Компьютер\_3 (Лялин)* настроен для выполнения нашей задачи.

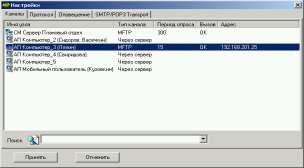


Рис. 2.25. Изменения в окне *Настройки* транспортного модуля MFTP.

Шаг 10(10)

*Обновление адресной и ключевой информации на АП Компьютер\_3 (Лялин).Контроль прохождения обновления.*

Если в Мониторе в разделе Настройки – Дополнительно в подразделе Передача сообщений и конференция поставлена отметка «Автоматически проводить полученной из ЦУСа обновление при отсутствии сеансов передачи сообщений или конференции», то обновление будет произведено автоматически, в противном же случае на экране появится окно с сообщением о принятом обновлении (Рис. 2.26).

Не торопитесь!!!

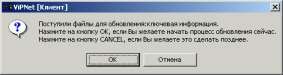


Рис. 2.26. Сообщение о принятом обновлении.

В процессе работы немедленное проведение обновления (программы *Монитор* и *Деловая Почта* закрываются) может быть нежелательным, для этого предусмотрена кнопка «*Отмена*» (Рис. 2.26).

В каталоге установки клиентской части модуля ViPNet Администратор ..\Program Files\Infotecs\ViPNet [Администратор]\SS\ (по умолчанию) есть служебный подкаталог \ССС\ (Рис. 2.27 – левая панель), в который складываются файлы пришедшего обновления – новая информация для СУ (адресные справочники или ключевая информация) содержится в архиве \*.lzh и три файла квитанций \*.c\* (Рис. 2.27 – правая панель).

Найдите этот каталог у себя на компьютере и убедитесь в том, что там находятся 4 файла.

*Внимание!!! Если обновление не проходит по какой-либо причине (например,*

*нарушена целость файлов обновления при передаче по плохим каналам*

*передачи данных), необходимо удалить эти файлы с компьютера*

*пользователя, а затем сформировать и выслать новое обновление! Удалять*

*следует только файлы в каталоге ..\ССС\, не трогая подкаталоги!!!*

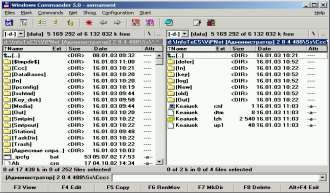


Рис.2.27. Каталог ..\ССС\ с принятыми обновлениями.

После чего загрузится программа *Монитор*, в окне *Защищенная сеть* которой будет отображен новый список сетевых узлов (не будет *АП Компьютер\_1 (Петров)* и появится *АП Компьютер\_5*) в соответствии с произведенной Вами модификацией (Рис. 2.30).



Рис. 2.30. Окно программы Монитор после обновления.

*Убедитесь в том, что после успешного обновления, в каталоге ..\ССС\ не*

*останется файлов обновления!*

### 4.Содержание отчета

*Отчет должен содержать:*

1.Формулировку цели работы.

2.Описание сценария лабораторной работы. 3.Выводы.

### Вопросы к лабораторной работе №2

1.Что будет, если сгенерировать заново (поменять) КД для главного абонента?

2.При смене имени пользователя в КЦ все пункты, отвечающие за генерацию ключей, отклонены. Почему?

3.Вы – администратор. Что делать, если посланное обновление не прошло? 4.Что делать, если пароль на вход в КЦ не проходит?

5.Что нужно сделать в ЦУС, чтобы заново начать генерацию DST-файлов? 6.Что такое «откат» в журнале запросов и ответов?

7.Что должен сделать администратор при смене мастер-ключа?

8.Что происходит при нажатии кнопки «Сформировать все справочники» в ЦУС?

# Лабораторная работа№3 «Межсетевое взаимодействие защищенных сетей ViPNet. Часть первая – СММК»

#### Цель работы

Целью работы является получение опыта организации межсетевого взаимодействия защищенных сетей ViPNet, а также необходимо научиться четко понимать, что администраторы каждой из сетей должны сделать для организации такого взаимодействия, и какие файловые ресурсы при этом используются.

#### Теоретические сведения и основные понятия межсетевого взаимодействия

* 1. ***Виды межсетевых мастер-ключей (ММК)***

***Межсетевые мастер-ключи*** — мастер-ключи, используемые для генерации классических симметричных ключей обмена для межсетевых связей (для связи коллективов, находящихся в разных сетях).

Межсетевые мастер-ключи делятся на три типа:

***Индивидуальный межсетевой мастер-ключ*** — мастер-ключ, уникальный для данной пары сетей. Вырабатывается по договоренности администратором КЦ одной из сетей и доставляется администратору КЦ другой сети средствами, исключающими их компрометацию (с нарочным).

***Универсальный межсетевой мастер-ключ*** — мастер-ключ, общий для всех сетей. Используется по договоренности между администраторами КЦ сетей. Доставляется из сети, в которой он уже имеется, в сеть, в которой его еще нет, средствами, исключающими его компрометацию.

***Межсетевой мастер-ключ Диффи-Хелмана*** — используемый в качестве мастер-ключа симметричный ключ Диффи-Хелмана. Соответствующие асимметричные ключи Диффи-Хелмана называются асимметричными мастер—ключами. Эти последние ключи создаются администраторами КЦ сетей. Асимметричные мастер-ключи могут быть использованы только для создания межсетевых мастер-ключей Диффи- Хелмана.

Пользователи должны отдавать себе отчет в том, что универсальный межсетевой мастер-ключ становится известным администраторам сразу нескольких сетей, поэтому его компрометация в одной из сетей приведет к компрометации ключей обмена коллективов всех остальных сетей, использующих данный универсальный мастер-ключ. По этой причине в

Ключевом центре принят следующий порядок выбора межсетевых мастер- ключей: при наличии нескольких межсетевых мастер-ключей приоритет отдается индивидуальному ключу, при его отсутствии - мастер-ключу Диффи-Хелмана, и только при отсутствии первых двух ключей используется универсальный межсетевой мастер-ключ.

#### Формирование экспорта и импорта данных для межсетевого взаимодействия

Для организации взаимодействия между различными независимыми сетями ViPNet предусмотрены процедуры обмена данными Экспорта между ЦУСами этих сетей, которые импортируются в соответствующую сеть. Одновременно Ключевые центры должны обменяться некоторой общей ключевой информацией для формирования межсетевых мастер-ключей, на базе которых будут выработаны индивидуальные ключи для взаимодействия АП разных сетей. После установления администратором сети связей с импортированными типами коллективов из других сетей ViPNet, формирования и рассылки для своих АП и СМ справочников и таблиц, новой ключевой информации, выработанной в своем Ключевом центре, абоненты данной сети получают возможность взаимодействовать с абонентами других сетей.

При экспорте формируется ряд файлов, содержащих данные об экспортированных Вами АП, коллективах и абонентах: AN<I>.TXT, NG<I>.TXT, NN<I>.TXT, UL<I>.TXT, UN<I>.TXT и другие, и файл

GT<I>.WAY, содержащий данные об СМ Вашей сети, через который будет осуществляться взаимодействие с другой сетью, где <I> - десятичный номер Вашей сети. Кроме того, ключевым центром формируются и передаются в ЦУС для экспорта файлы с образцами открытых ключей подписей главных абонентов Вашей сети, со списками выведенных из действия подписей абонентов сети.

Эти файлы необходимо передать в ЦУС другой сети. Если уже установлено межсетевое взаимодействие, то эти файлы передаются по каналам связи сети ViPNet.

*Рассмотрим действия администраторов двух сетей в ЦУСе и в УКЦ:*

1. Администраторы двух ЦУСов выполняют процедуру экспорта из своей сети информации об объектах, которые должны взаимодействовать с объектами другой сети. Экспортируется также по одному из координаторов каждой сети, через которые или с использованием которых будет осуществляться такое взаимодействие. Каким-либо защищенным способом производится обмен этой информацией и ее импорт в свой ЦУС.
2. Администраторам УКЦ необходимо создать один из

межсетевых мастер-ключей. Следует заметить, что симметричные межсетевые мастер-ключи создаются только в одной сети, а в другую передаются, а асимметричный - в обеих сетях, и Администраторы двух сетей обмениваются открытыми частями своего ключа. Поэтому Администраторам двух сетей предварительно нужно договориться, какие межсетевые мастер-ключи будут использоваться для связи между сетями. Предпочтительно использовать для связи двух сетей симметричный индивидуальный мастер-ключ, так как в этом случае безопасность хранения выше (об этом ключе знают Администраторы только двух сетей, а при использовании универсального ключа - Администраторы всех сетей, в которые он экспортирован). Стойкость же асимметричного ключа ниже (симметричного индивидуального и симметричного универсального ключа).

1. Администраторы двух УКЦ производят обмен межсетевыми мастер- ключами по симметричной или асимметричной схеме. Одновременно выполняется обмен справочниками сертификатов ЭЦП Главных абонентов каждой сети и справочниками отозванных сертификатов ЭЦП абонентов каждой сети (даже если этот справочник пустой, т.е. сертификаты ЭЦП в сети ни разу не отзывались).
2. В каждом из УКЦ производится импорт и заверение справочника сертификата Главных абонентов другой сети подписью своего Главного абонента и импорт справочника отозванных сертификатов ЭЦП абонентов другой сети.
3. На основании информации, полученной из ЦУСа каждой сети, в УКЦ каждой сети необходимо сформировать новые ключевые наборы. На этом этапе будет сформирована новая ключевая информация только для своего ЦУСа и Координатора, так как информация о связях других объектов пока неизвестна. После обновления этой информации будет возможно установление соединения между ЦУСами двух сетей.
4. Администраторы каждого из ЦУСов устанавливают необходимые связи импортированных коллективов со своими экспортированными коллективами. Обмениваются уже автоматически через установленное соединение вновь сформированными экспортными данными и отправляют информацию о новых связях своих объектов в свои УКЦ.
5. На основании полученных данных, в УКЦ необходимо сформировать новые ключевые наборы для АП, которых затронули изменения (в ключевых дискетах абонентов в этой ситуации изменений быть не может). Эти ключевые наборы обычным образом отправляются в свой ЦУС для рассылки по своей сети и автоматического обновления.

#### Методические указания по выполнению лабораторной работы

Шаги, необходимые для межсетевого взаимодействия защищенных сетей ViPNet, включающие:

* + теоретическую проработку схемы объединения защищенных сетей;
  + инсталляцию рабочих мест Администраторов двух защищенных сетей;
  + первоначальное развертывание двух защищенных сетей;
  + формирование начального экспорта в одной из защищенных сетей;
  + передача начального экспорта во вторую защищенную сеть;
  + прием начального экспорта и формирование ответного экспорта во второй защищенной сети;
  + генерация новой ключевой информации и рассылка ее всем СУ второй защищенной сети;
  + передача ответного экспорта в первую защищенную сеть;
  + прием ответного экспорта в первой защищенной сети;
  + генерация новой ключевой информации и рассылка ее всем СУ первой защищенной сети;
  + проверка правильности установления межсетевого взаимодействия.

Задание на занятие:

Организовать межсетевое взаимодействие двух ViPNet сетей, исходя из нижеперечисленных условий и приведенной схемы (Рис. 1).

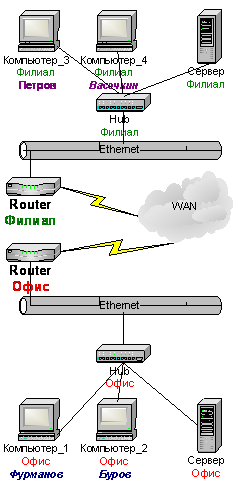


Рис. 1 Схема для организации межсетевого взаимодействия

Условия построения защищенной сети 1 (Офис):

* в защищенную сеть 1 включаются следующие СУ: СМ Сервер Офис, АП Компьютер\_1 (Фурманов), АП Компьютер\_2 (Буров);
* Администратором и Главным абонентом защищенной сети будет Фурманов.

Условия построения защищенной сети 2 (Филиал):

* в защищенную сеть 2 включаются следующие СУ: СМ Сервер Филиал, АП Компьютер\_3 (Петров), АП Компьютер\_4 (Васечкин);
* Администратором и Главным абонентом защищенной сети будет Петров.

Условия межсетевого взаимодействия Филиала и Офиса:

Защищенные сети Офиса и Филиала имеют следующие номера: № 6670 и № 6671. Полная связность – все видят всех. Межсетевое взаимодействие организуется на **Симметричном Межсетевом Мастер- ключе** (СММК), причем на **индивидуальном.**

Последовательность выполнения занятия:

Перед тем как приступить к организации межсетевого взаимодействия, необходимо сформировать две ViPNet сети, исходя из вышеприведенных схем и условий. В качестве справочника можно воспользоваться Лабораторной работой № 1.

Кто из администраторов двух сетей начнет процесс установления межсетевого взаимодействия для нас не важно. Пусть это будет администратор ViPNet сети офиса, т. е. администратор сети № 6670.

*Для установки межсетевого взаимодействия необходимо:*

1. Сформировать начальный экспорт в сети № 6670.
2. Принять экспорт из сети № 6670 в сети № 6671.
3. Сформировать ответный экспорт в сети № 6671 для сети № 6670.
4. Принять ответный экспорт из сети № 6671 в сети № 6670.

*Начальный экспорт* ***для случая СММК*** *содержит* ***3 составляющие:***

1. Экспортные справочники (готовятся в ЦУСе).
2. Межсетевой мастер-ключ (генерируется в КЦ).
3. Сигнатура подписи главного абонента (храниться в ..\KC\PSW\**\*.chf**).

*Ответный экспорт* ***для случая СММК*** *содержит* ***2 составляющие:***

1. Экспортные справочники (готовятся в ЦУСе).
2. Сигнатура подписи главного абонента (храниться в ..\KC\PSW\**\*.chf**).

Отличие двух вариантов симметричных межсетевых мастер-ключей (универсальный и индивидуальный) заключается в том, что УСММК можно передавать в произвольное количество защищенных сетей, а ИСММК создается для конкретной защищенной сети. Оба мастер-ключа защищаются специальными паролями.

**Часть 1**

Шаг 1(25)

*Формирование Экспорта в ЦУСе*

Запускаем ЦУС сети № 6670 и переходим в меню *Службы  Экспорт...* (Рис. 2). Перед нами появляется окно формирования экспорта, нажимаем кнопку *Добавить* и, в появившемся окне, вводим номер сети для которой готовим экспорт, т.е. **6671** (Рис. 3).

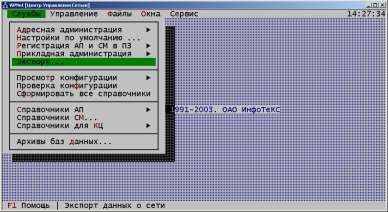


Рис. 2 Меню *Службы* в ЦУСе

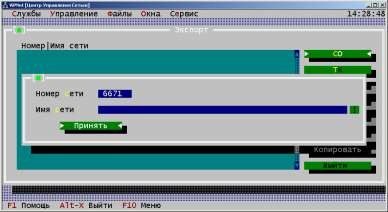


Рис. 3 Задание номера сети для формирования экспорта

В строку *Имя сети* можно внести комментарий о сети, для которой готовим экспорт. Эта строка имеет справочное назначение и никуда не передается.

Для экспорта необходимо предоставить СО и соответствующие им ТК. Это делается для того, чтобы в дальнейшем организовать связи и сформировать ключи шифрования для них. Исходя из задания (полная связность) выбираем ТК на экспорт – нажимаем последовательно, в появляющихся окнах, кнопки *ТК*, *Добавить, Все* и *Принять.* Получаем окно с выбранными на экспорт ТК (Рис. 4).



Рис. 4 Экспортируемые ТК

Нажимаем на кнопку *Выйти* и попадаем в основное окно подготовки экспорта (Рис. 5).

Теперь необходимо проконтролировать, что у нас выбраны СО на экспорт – нажимаем кнопку *СО.* В том случае, когда сначала выбираются ТК, соответствующие им СО выбираются автоматически. Если же сначала выбрать СО, то потом придется выбирать еще и ТК.

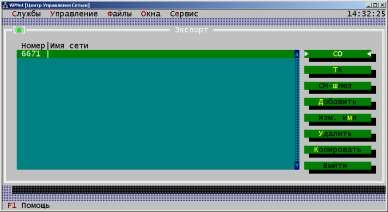


Рис. 5 Окно подготовки экспорта в ЦУСе

Шаг 2(25)

*Задание шлюза*

При установлении межсетевого взаимодействия необходимо в обеих ViPNet сетях определить СМ для организации шлюзов. Шлюзы необходимы

для того, чтобы определить путь прохождения конвертов, формируемых ДП и файлов, пересылаемых по файловому обмену.

Итак, требуется задать шлюз. Делаем это нажатием кнопки *СМ-шлюз*. Перед нами появляется информационное окно, говорящее о том, что шлюз не задан (Рис. 6).



Рис. 6 Сообщение об отсутствии шлюза

Нажимаем на кнопку *Сменить шлюз* и выбираем СМ, который мы хотим использовать в качестве шлюза (в нашем случае сервер один, его и выбираем) (Рис. 7), нажимаем на кнопку *Принять*.

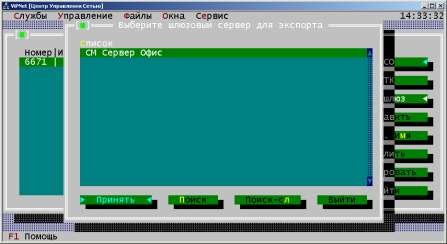


Рис. 7 Окно выбора шлюза

Теперь желательно еще раз убедиться, что мы сделали все правильно:

* проверяем наличие экспортируемых СО;
* проверяем наличие экспортируемых ТК;
* проверяем наличие шлюза.

На этом подготовка экспорта для сети № 6671 в ЦУСе завершается.

Шаг 3(25)

*Копирование экспорта*

Сейчас мы находимся в меню экспорта (Рис. 3.4.). Нажимаем кнопку *Копировать*. Перед нами появляется окно задания пути для копирования экспорта (Рис. 8). Просто **запоминаем этот путь** и нажимаем кнопку *Принять*.



Рис. 8 Задание пути для копирования экспорта

После того, как ЦУС скопирует файлы экспорта, на экране появится информационное окно (Рис. 9). Нажимаем на любую клавишу и выходим из ЦУСа.

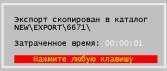


Рис. 9 Экспорт скопирован

Шаг 4(25)

*Генерация индивидуального СММК*

Запускаем КЦ сети № 6670, выбираем пункт меню *Программа  Генерация мастер-ключей  Межсетевые мастер-ключи  Индивидуальный симметричный* (Рис. 10)*.*

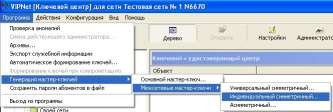


Рис. 10 Меню генерации мастер-ключей в КЦ

Перед нами появится окно (Рис. 11), в котором нам необходимо задать номер внешней сети, для которой этот ИСММК генерируется, т.е. 6671.

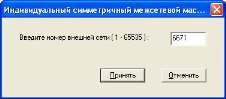


Рис. 11 Задание номера внешней сети

Нажимаем кнопку *Принять*, перед нами появляется информационное окно (Рис. 11), в котором присутствует номер генерируемого мастер-ключа и предупреждающая информация о том, что ключи шифрования, созданные на основе нового мастер-ключа, не смогут стыковаться со старыми ключами шифрования, которые создавались на существующем мастер-ключе (если он уже есть).

Нажимаем кнопку *Создать мастер-ключ* (Рис. 12), отвечаем на вопрос нажатием кнопки *ОК*, «крутим» рулетку и еще раз нажимаем кнопку *ОК.*

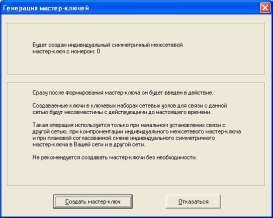


Рис. 12 Окно создания ИСММК

## ИСММК создан.

Шаг 5(25)

*Экспорт сгенерированного ИСММК для сети №6671*

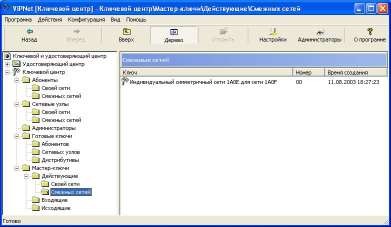


Рис. 13 Экспорт и импорт межсетевых мастер-ключей

Выбираем раздел *Ключевой центр  Мастер-ключи  Действующие  Смежных сетей* (Рис. 1.13)*.* В появившемся окне подсвечиваем запись индивидуального симметричного ключа для сети № 6671 и по контекстному меню выбираем пункт *Экспортировать* (Рис. 14).

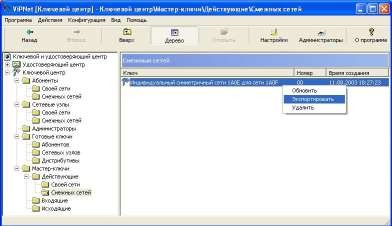


Рис. 14 Экспорт межсетевых мастер-ключей

Если мы **покидали** КЦ, то сначала нам придется крутить рулетку, а затем на экране появится окно (Рис. 3.14.), содержащее сгенерированный

пароль для защиты экспортируемого ИСММК (Рис. 15). **Запомните этот пароль (запишите). В случае его утери, администратор сети № 6671 не сможет импортировать его и использовать для формирования ключевой информации!**

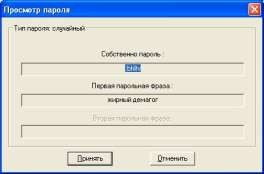


Рис. 15 Пароль для защиты ИСММК

Нажимаем сначала на кнопку П*ринять*, затем *ОК* и *Закрыть*. После этого программу КЦ можно закрыть, все необходимые действия в ней сделаны.

Все, что остается сделать администратору сети № 6670 – это собрать вместе все 3 составляющие начального экспорта и передать их администратору сети № 6671 по надежному каналу передачи данных.

Шаг 6 (25)

*Передача начального экспорта для сети № 6671 ее* ***администратору***

Итак, собираем составляющие начального экспорта в одно место. Для этого на жестком диске создадим папку, например **C:\EXP\_for\_6671\**.

1. Из ЦУСа необходимо взять экспортные адресные справочники. На данный момент они находятся в каталоге **..\NCC\New\Export\6671\** (этот путь был установлен по умолчанию – Шаг №3). Там же находится образец подписи главного абонента - файл, который берется из каталога

..\KC\Psw\**\*.chf**, где под звездочкой скрывается шестнадцатеричный номер сети (**6670 – 1А0Е, 6671 - 1А0F**). Теперь мы копируем **всю папку**

**..\NCC\New\Export\6671\\*.\*** в нашу папку **..\EXP\_for\_6671\**.

1. Из КЦ необходимо взять экспортированный ИСММК для сети № 6671. Он находится в папке ..\КС\Export\**\*.i00**. Копируем его в нашу папку – C:\EXP\_for\_6671\.

Теперь всю папку **C:\EXP\_for\_6671\** необходимо заархивировать и передать администратору сети № 6671 по надежному каналу передачи данных (например, с помощью фельдъегеря).

На этом этапе работа Администратора сети № 6670 закончена.

Шаг 7(25)

*Прием начального экспорта из сети № 6670 администратором сети*

*№ 6671****.***

Администратор сети № 6671 принимает начальный экспорт из сети № 6670 следующим образом:

1. **Содержимое** папки **..\EXP\_for\_6671\6671\\*.\*** (экспортные адресные справочники и образец подписи главного абонента) копируем в ЦУС сети № 6671 в папку ..\NCC\Import\.
2. ИСММК копируем из папки **..\EXP\_for\_6671\\*.i00** в КЦ ..\КС\Import\.

Шаг 8(25)

*Подключение межсетевого канала*

Загружаем ЦУС сети № 6671 и просматриваем сообщения о принятом экспорте. Сначала мы увидим сообщение о принятой подписи главного абонента сети № 6670 (Рис. 16), затем сообщение об изменении в составе шлюзов (Рис. 17). Нажимаем на кнопку *Esc*, затем пробел, видим сообщение об изменениях в импорте (Рис. 18), нажимаем пробел и видим сообщение об изменении в файле шлюзов, с рекомендацией проверить межсетевые каналы (Рис. 19).



Рис. 16 Поступили новые справочники

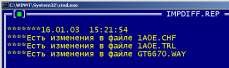


Рис. 17 Сообщение об изменении в составе шлюзов



Рис. 18 Сообщение об изменении в импорте



Рис. 19 Сообщение об изменении в файле шлюзов

Вот с этого и начнем. Дело в том, что шлюз при межсетевом взаимодействии должен быть определен не только на прикладном уровне, но и на адресном, т.е. должен быть сформирован **межсетевой канал.**

Заходим в адресную администрацию – меню *Службы  Адресная администрация  Адреса в сети «Инфотекс»...* Перед нами появляется сообщение об изменении межсетевых каналов (Рис. 20).



Рис. 20 Сообщение адресной администрации

Нажимаем пробел и попадаем в основное меню адресной администрации. Выбираем пункт *Межсетевые каналы.*

Перед нами появляется список межсетевых каналов, в нашем случае он один и выключен (Рис. 21). Как видно, имя чужого СМ-шлюза задано, а своего еще нет (на самом деле нам еще придется производить такие же действия по подключению межсетевого канала в ЦУСе сети № 6670, на данный момент информация о нашем шлюзе взята из файла экспорта **gt\*.way** – ведь на прикладном уровне в ЦУСе сети № 6670 мы его уже задали).

Для того чтобы включить межсетевой канал, нажимаем на кнопку *Enter* два раза – внизу окна появится имя своего сервера (СМ Сервер Филиал), а состояние измениться на *Вкл* (Рис. 22)*.*

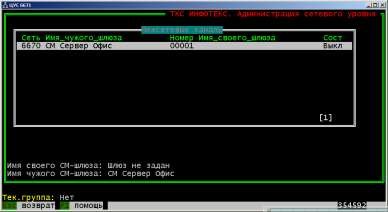


Рис. 21 Межсетевой канал выключен

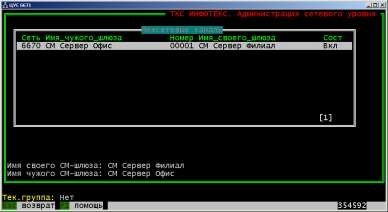


Рис. 22 Межсетевой канал включен

Нажимаем *Esc* и попадаем в основное меню. Выполняем *Выдать таблицы маршрутизации* и выходим из этого меню в главное (нажимаем *Esc*).

Шаг 9(25)

*Образование требуемых связей между ТК сетей №№ 6670 и 6671*

Нам необходимо связать ТК, которые были экспортированы из сети № 6670 с ТК сети № 6671. Для этого выбираем пункт меню *Службы  Прикладная администрация  Регистрация типов коллективов...*

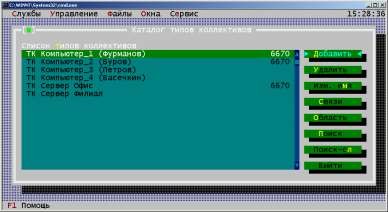


Рис. 23 Новый список ТК

В появившемся списке ТК (Рис. 23) мы видим три новых ТК и справа помечено, что они принадлежат сети № 6670. Выбираем один из этих ТК, например, ТК Компьютер\_1 (Фурманов), и нажимаем кнопку *Связи*. Список связей пока пустой, нажимаем кнопку *Добавить*, потом кнопки *Все* (по заданию – связность полная) и *Принять.* Теперь этот ТК уже связан со всеми ТК из сети № 6671. Нажимаем кнопку *Выйти.*

Повторим вышеописанные действия для двух оставшихся ТК из сети

№ 6670 – ТК Компьютер\_2 (Буров) и ТК Сервер Офис.

Теперь по нажатию кнопки *Связи* для любого из трех ТК сети № 6670 мы увидим список ТК (Рис. 24).

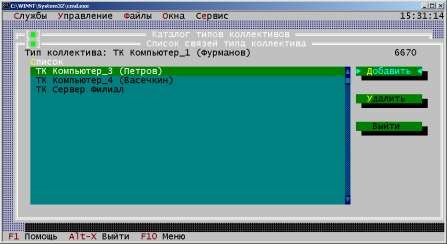


Рис. 24 Список связей экспортированных ТК

Шаг 10(25)

*Формирование экспорта в сеть № 6670*

Итак, ЦУС сети № 6671 принял экспорт из сети № 6670. Теперь необходимо сформировать свой экспорт в сеть № 6670. Как и ранее (Шаг 1) выбираем пункт меню *Службы  Экспорт...* и попадаем в меню подготовки экспорта (Рис. 25). Как видим, здесь уже присутствует запись для сети № 6670 (поскольку ЦУС сети № 6671 принял экспорт из сети № 6670). Нам необходимо выставить на экспорт СО и ТК сети № 6671, что мы и сделаем. Подсвечиваем запись *6670* и нажимаем кнопку ТК, затем в появляющихся окнах последовательно нажимаем кнопки *Добавить, Все* и *Принять.* Получаем окно с выбранными на экспорт ТК (Рис. 26).

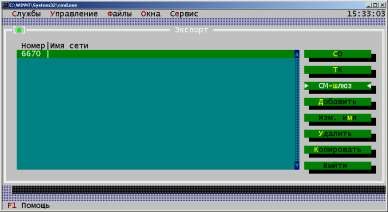


Рис. 25 Окно экспорта

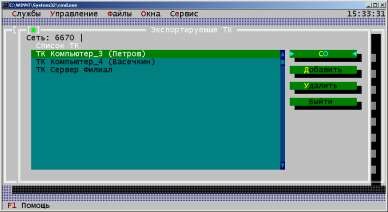


Рис. 26 Список экспортируемых ТК

Нажимаем на кнопку <Esc>, потом нажимаем на кнопку СО и проверяем, что СО тоже выбраны, если же список пуст, то нажимаем на кнопки *Добавить, Все, Принять* и *Выйти.*

Шаг 11(25)

*Задание шлюза и копирование экспорта*

Находясь в окне экспорта (Рис. 25), нажимаем на кнопку *СМ-шлюз,* затем кнопку *Сменить шлюз* (Рис. 6), перед нами появляется окно выбора шлюзов (Рис. 7) в котором присутствует единственный СМ сети № 6671 – СМ Сервер Филиал. Подсвечиваем его, нажимаем кнопку *Принять* и снова попадаем в окно экспорта.

Все, что осталось сделать – это скопировать экспорт в каталог по умолчанию и выйти в основное меню ЦУСа. Для этого нажимаем кнопку *Копировать,* затем *Принять*, нажимаем на любую клавишу и потом на кнопку <Esc>.

Шаг 12(25)

*Формирование всех справочников*

Поскольку мы задали новые связи, необходимо теперь сформировать ключевую и адресную информацию. Соответственно необходимо сформировать справочники. Для этого выбираем пункт меню *Службы  Сформировать все справочники.* ЦУС сформирует все необходимые справочники и выдаст окно отчета. Нажимаем кнопку *Принять* и выходим из ЦУСа (сочетание клавиш <Alt+X>). На вопрос ЦУСа о создании архива ответим утвердительно.

Шаг 13(25)

*Регистрация сертификата ЭЦП главного абонента сети № 6670 в КЦ сети № 6671*

Загружаем КЦ сети № 6671, перед нами появляется предложение КЦ о создании экспорта с вариантами сетевых узлов для смежных сетей (Рис. 3.27). Нужно это для обеспечения нормальной работы при активизации процедуры компрометации в одной из сетей, поэтому на вопрос ответим утвердительно.

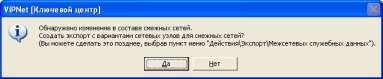


Рис. 27 Предложение КЦ создать импорт с вариантами АП

Ключевой Центр сообщит об успешности проведенной операции и далее выдаст сообщение *«Обнаружен справочник сертификатов ЭЦП главных абонентов из смежной сети»* и спросит, желаете ли Вы импортировать его немедленно или сделаете это позднее. Отвечайте *«Да»*.

После этого перед нами появится окно со списком справочников ЭЦП главных абонентов из других сетей (Рис. 1.29).



Рис. 28 Импорт сертификатов ЭЦП главных абонентов

Выделяем первую из записей *Сеть <6670>* и нажимаем кнопку *Просмотреть сертификат ЭЦП.* Появится окно (Рис. 1.30), в котором можно посмотреть сам сертификат ЭЦП главного абонента, дату создания и срок окончания действия подписи. Один из сертификатов окажется действительным, а второй – нет, так как в версии 2.8 создаются как новые сертификаты ЭЦП (формата Х.509), так и ЭЦП старого образца.

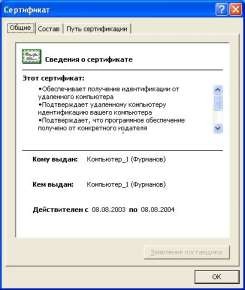


Рис. 29 Просмотр сертификата ЭЦП главного абонента сети № 6670

Нажимаем кнопку *Принять.* Напротив записи *Сеть <6670>* появится галочка. Только после того, как подпись была просмотрена, ее можно импортировать!

Нажимаем на кнопку *Импорт* (Рис. 28)*,* в появившемся окне (Рис. 29) нажимаем кнопку *ОК,* потом еще раз *ОК* и *Выход.* Импорт подписи главного абонента сети № 6670 завершен.

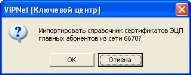


Рис. 30 Подтверждение импорта

**Часть 2**

Шаг 14(25)

*Импорт ИСММК из сети № 6670*

При использовании симметричных межсетевых мастер-ключей, их достаточно сформировать только на одной стороне (обычно на той, которая формирует первоначальный экспорт). В нашем случае ИСММК создан в сети

№ 6670 и формировать СММК в сети № 6671 **не обязательно**, достаточно импортировать ИСММК из сети № 6670 и воспользоваться им для формирования ключевой информации для связи между АП сетей №№ 6670 и 6671.

Выбираем раздел *Ключевой центр  Мастер-ключи  Входящие*

(Рис. 31).

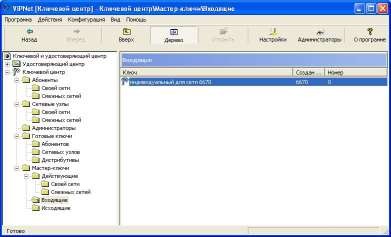


Рис. 31 Импорт межсетевых мастер-ключей

Перед нами появится окно, в котором будет присутствовать запись *Индивидуальный для сети 6670* (Рис. 31). В столбце *Номер* можно посмотреть номер ключа. Нажимаем на кнопку *Импортировать* и в появившемся окне необходимо ввести тот самый пароль, который выдал КЦ сети № 6670 при экспортировании ИСММК. Нажимаем кнопки *ОК* и *Закрыть.*

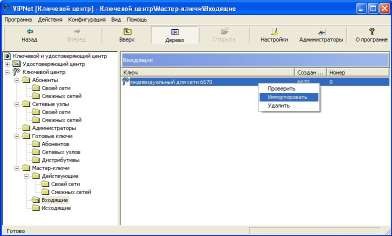


Рис. 32 Список ММК для импорта

Все, что нам осталось сделать в КЦ – сформировать новые КН для СУ сети № 6671 и перенести их в ЦУС для рассылки обновлений.

Шаг 15(25)

*Формирование новых КН и перенос их в ЦУС*

Только после того, как мы импортировали ИСММК можно приступать к формированию новой ключевой информации для СУ сети № 6671, ТК которых связаны с ТК, экспортированными из сети № 6670.

Выбираем разделе *Программа  Автоматическое формирование ключей.* Поскольку это первое, за этот сеанс работы с КЦ, формирование ключей – необходимо «прокрутить» рулетку, после чего, в появившемся окне, нажать на кнопку *Старт*, потом на кнопки *ОК* и *Выход.*

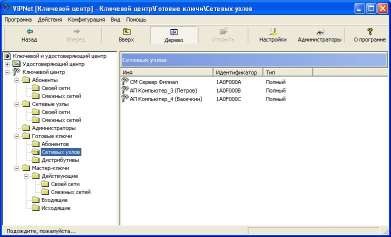


Рис. 33 Готовые КН для СУ сети № 6671.

Новые КН необходимо перенести в ЦУС. Выбираем раздел *Ключевой центр  Готовые ключи  Сетевых узлов*, выделяем все КН и по контекстному меню *Перенести – в ЦУС* отправляем их в ЦУС для рассылки обновлений.

Нажимаем на кнопку *Закрыть* и выходим из КЦ.

Шаг 16(25)

*Рассылка обновлений*

Запускаем ЦУС сети № 6671. Сначала разошлем КН, а потом адресные справочники. Выбираем пункт меню *Управление  Отправить измененные файлы  Ключевые наборы для СУ...*, в появившемся окне (Рис. 34) нажимаем кнопки *Все* и *Отправить*, изменяем дату обновления на «заднее число» и нажимаем кнопку *Принять*, а потом *Выйти.*

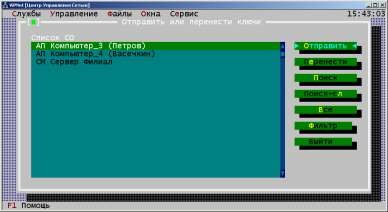


Рис. 34 Список КН для отправки

Теперь отправим адресные справочники. Выбираем пункт меню *Управление  Отправить измененные файлы  Справочники АП и СМ...*, в появившемся окне нажимаем кнопки *Все* и *Отправить*, изменяем дату обновления на «заднее число» и нажимаем кнопку *Принять*, а потом *Выйти.* Выходим из ЦУСа.

Шаг 17(25)

*Передача ответного экспорта для сети № 6670 ее администратору*

Итак, собираем составляющие ответного экспорта в одно место. Для этого на жестком диске создадим папку, например **C:\EXP\_for\_6670\**.

Из ЦУСа необходимо взять экспортные адресные справочники. На данный момент они находятся в каталоге **..\NCC\New\Export\6670\** (этот путь был установлен по умолчанию – Шаг № 11). Там же находится образец подписи главного абонента - файл, который берется из каталога ..\KC\Psw\**\*.chf**, где под звездочкой скрывается шестнадцатеричный номер сети (**6670 – 1А0Е, 6671 - 1А0F**). Теперь мы копируем **всю папку ..\6670\\*.\*** в нашу папку

..\EXP\_for\_6670\.

Теперь всю папку **C:\EXP\_for\_6670\** необходимо заархивировать и передать администратору сети № 6670 по надежному каналу передачи данных (например, с помощью фельдъегеря).

На этом работа Администратора сети № 6671 закончена.

**Часть 3**

Шаг 18(25)

*Прием ответного экспорта из сети № 6671 администратором сети № 6670*

Администратор сети № 6670 принимает ответный экспорт из сети № 6671 следующим образом:

**Содержимое** папки **..\EXP\_for\_6670\6670\\*.\*** (экспортные адресные справочники и образец подписи главного абонента) копируем в ЦУС сети № 6670 в папку ..\NCC\Import\.

Шаг 19(25)

*Подключение межсетевого канала*

Загружаем ЦУС сети № 6670, вводим пароль администратора сети (у нас администратор и главный абонент – одно и то же лицо), перед нами появляется первое информационное сообщение (Рис. 35).



Рис. 35 Поступили новые справочники

Нажимаем любую клавишу и перед нами появляются новые окна (Рис. 1.18 – 1.20) с напоминанием о необходимости включить межсетевой канал.

Межсетевой канал включается в адресной администрации. Выбираем пункт меню *Службы  Адресная администрация  Адреса в сети*

*«Инфотекс»...* Перед нами появляется сообщение об изменении межсетевых каналов (Рис. 3.21). Нажимаем пробел и попадаем в основное меню адресной администрации. Выбираем пункт *Межсетевые каналы.*

Перед нами появляется список межсетевых каналов, в нашем случае он один и пока выключен (Рис. 36). Как видно, имя чужого СМ-шлюза задано, а своего еще нет.

Для того чтобы включить межсетевой канал, нажимаем на кнопку *Enter* два раза – внизу окна появится имя своего сервера (СМ Сервер Офис), а состояние измениться на *Вкл* (Рис. 37)*.*

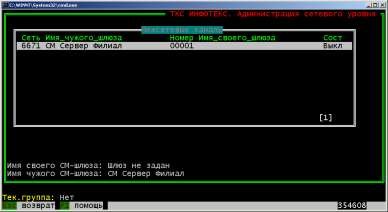


Рис. 36 Межсетевой канал выключен

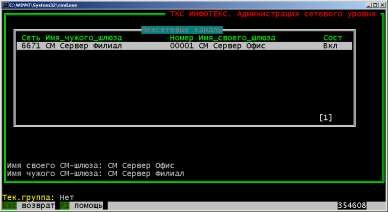


Рис. 37 Межсетевой канал включен

Нажимаем *Esc* и попадаем в основное меню. Выполняем *Выдать таблицы маршрутизации* и выходим из этого меню в главное (нажимаем *Esc*).

Шаг 20(25)

*Проверка наличия связей между ТК сетей №№ 6670 и 6671*

В справочниках связей ответного экспорта уже содержится информация о тех связях между ТК двух сетей, которые установил администратор сети № 6671. Поэтому устанавливать эти связи в ЦУСе сети

№ 6670 не требуется. Мы просто проверим, что все сделали правильно и что связи между ТК сетей №№ 6670 и 6671 установлены. Выбираем пункт меню *Службы  Прикладная администрация  Регистрация типов коллективов...* В появившемся списке ТК есть и ТК из сети № 6671 (Рис. 38).

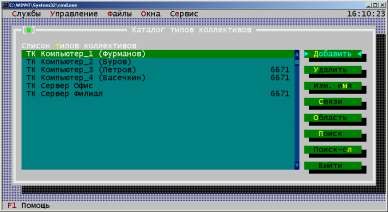


Рис. 38 Список ТК после приема экспорта

Для контроля установленных связей поочередно просмотрим связи ТК сети № 6670 (или сети № 6671), например, для Фурманова список связей будет выглядеть как на рис. 39.

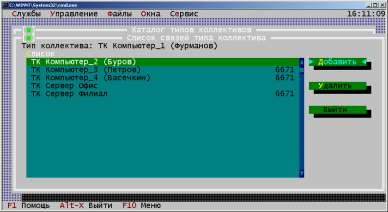


Рис. 39 Список связей ТК Компьютер\_1 (Фурманов)

**Часть 4**

Шаг 21(25)

*Формирование всех справочников*

Для того, чтобы сформировать новые КН и адресные справочники выбираем пункт меню *Службы  Сформировать все справочники.* ЦУС сформирует все необходимые справочники и выдаст статистику по

произведенным действиям. Нажимаем кнопку *Принять* и выходим из ЦУСа, на вопрос о необходимости формировать архив ответим утвердительно.

Шаг 22(25)

*Регистрация сертификата ЭЦП главного абонента сети № 6671 в КЦ сети*

*№ 6670*

Загружаем КЦ сети № 6670. Как и в КЦ сети № 6671, перед нами появляется предложение о создании импорта с вариантами АП для смежных сетей (Рис. 27). Нажимаем на кнопку *Yes*. Перед нами появится окно со списком новых справочников ЭЦП главных абонентов из других сетей (Рис. 40). Выделяем по очереди обе записи *Сеть <6671>* и нажимаем кнопку *Просмотреть сертификат ЭЦП.* Появится окно (Рис. 41), в котором нажимаем кнопку *ОК.*

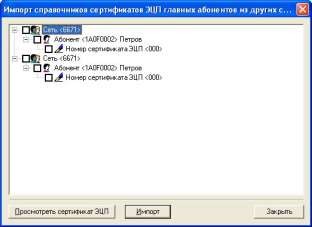


Рис. 40 Импорт ЭЦП главных абонентов

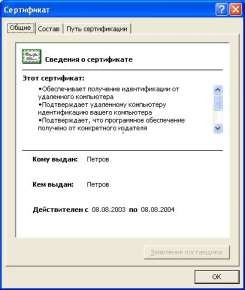


Рис. 41 Просмотр сертификата ЭЦП главного абонента сети № 6671

Напротив записи *Сеть <6671>* появится галочка. **Только после того, как подпись была просмотрена, ее можно импортировать!**

Нажимаем на кнопку *Импорт* (Рис. 40)*,* в появившемся окне (Рис. 42) нажимаем кнопку *ОК,* потом еще раз *ОК* и *Выход.* Импорт подписи главного абонента сети № 6671 завершен.

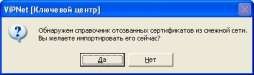


Рис. 42 Подтверждение импорта

Шаг 23(25)

*Импорт отозванных сертификатов ЭЦП*

После того, как мы импортировали ЭЦП главного абонента сети № 6671 м нам нужно импортировать отозванные сертификаты.

В открывшемся окне (Рис. 43) мы должны нажать ДА, а затем в следующем окне (Рис. 44) импортировать нужные справочники

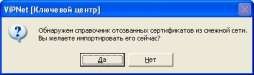


Рис. 43 Обнаружен справочник отозванных сертификатов

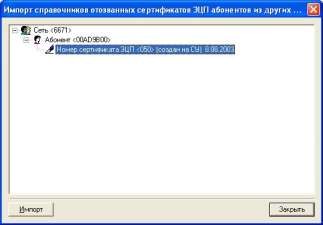


Рис. 44 Импорт справочников отозванных сертификатов ЭЦП

Шаг 23(25)

*Формирование новых КН и перенос их в ЦУС*

После того, как мы зарегистрировали ЭЦП главного абонента сети № 6671 можно приступать к формированию новой ключевой информации для СУ сети № 6670, ТК которых связаны с ТК, экспортированными из сети № 6671.

Выбираем пункт меню *Программа  Автоматическое формирование ключей.* «Крутим» электронную рулетку, затем, в появившемся окне, нажимаем на кнопку *Старт*, потом на кнопки *ОК* и *Выход.*

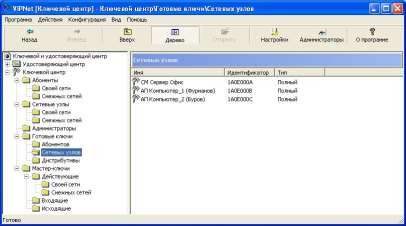


Рис. 45 Готовые КН для СУ сети № 6671

Новые КН необходимо перенести в ЦУС. Выбираем раздел *Ключевой центр  Готовые ключи  Сетевых узлов*, выделяем все КН и по контекстному меню *Перенести - в ЦУС* отправляем КН в ЦУС для рассылки обновлений

Нажимаем на кнопку *Закрыть* и выходим из КЦ.

Шаг 24(25)

*Рассылка обновлений*

Запускаем ЦУС сети № 6670. Сначала разошлем КН, а потом адресные справочники. Выбираем пункт меню *Управление  Отправить измененные файлы  Ключевые набора для СУ...*, в появившемся окне (Рис. 46) нажимаем кнопки *Все* и *Отправить*, изменяем дату обновления на «заднее число» и нажимаем кнопку *Принять*, а потом *Выйти.*

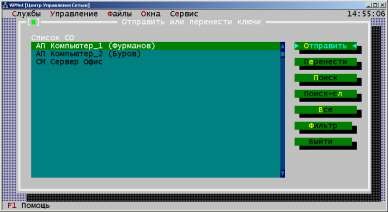


Рис. 46 Список КН для отправки

Теперь отправим адресные справочники. Выбираем пункт меню *Управление  Отправить измененные файлы  Справочники АП и СМ...*, в появившемся окне нажимаем кнопки *Все* и *Отправить*, изменяем дату обновления на «заднее число» и нажимаем кнопку *Принять*, а потом *Выйти.* Выходим из ЦУСа.

Шаг 25(25)

*Проверка правильности выполненной процедуры установления межсетевого взаимодействия*

Загружаем Монитор сети № 6670 и перенастраиваем транспортный модуль MFTP на работу по одноименному каналу, как мы это делали в Лабораторной работе № 2 .

После перенастройки транспортного модуля проведем обновление АП Компьютер\_1 (Фурманов), как и в Лабораторной работе № 2 .

После перезагрузки Монитора **не должно быть «ругательных» сообщений** типа «...не найдены ключи для таких-то сетевых узлов..», а в меню *Защищенная сеть* появятся новые фильтры для СУ сети № 6671 (Рис. 47).

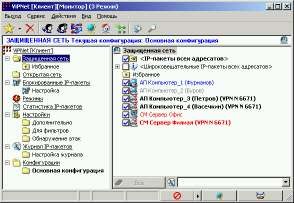


Рис. 47 Окно Монитора после проведенного обновления

Отсутствие ругани и правильный набор фильтров в меню *Защищенная сеть* - показатель того, что Вы все сделали правильно. Закройте Монитор АП Компьютер\_1 (Фурманов) и повторите этот шаг для АП Компьютер\_3 (Петров).

По завершению всех вышеописанных шагов, между двумя защищенными сетями будет установлено межсетевое взаимодействие и теперь данные между сетями будут передаваться в защищенном виде, экспорт можно будет формировать и отсылать в другую сеть по защищенному каналу передачи данных (в ЦУСе меню *Управление  Отправить измененные файлы  Экспорт...*, выбираем экспорт в нужную сеть и нажимаем кнопку *Отправить*).

Итак, на простом примере, мы разобрали установление межсетевого взаимодействия двух VPN-сетей. Однако, на практике, установление межсетевого взаимодействия с использованием СММК применяется достаточно редко из-за необходимости наличия надежного канала передачи данных для обмена начальным и ответным экспортами между Администраторами VPN-сетей. Для тех случаев, когда такой канал отсутствует, предусмотрена асимметричная схема установления межсетевого взаимодействия (схема Диффи-Хэлмана).

1. **Содержание отчета**

Отчет должен содержать:

* 1. Формулировку цели работы;
  2. Описание сценария лабораторной работы;
  3. Выводы о проделанной работе.

### Вопросы к лабораторной работе №3

1. Требуется ли при связывании двух защищенных сетей заново генерировать основной мастер ключ?
2. Зачем необходимо назначение шлюза в защищенной сети?
3. Какого типа может быть межсетевой мастер-ключ?
4. Для чего необходим экспорт ЭЦП главного абонента при установлении межсетевого взаимодействия?

# Лабораторная работа №4 «Межсетевое взаимодействие защищенных сетей ViPNet. Часть вторая – АММК.»

#### Цель работы

Целью работы является получение опыта организации межсетевого взаимодействия защищенных сетей ViPNet, а также необходимо научиться четко понимать, что администраторы каждой из сетей должны сделать для организации такого взаимодействия, и какие файловые ресурсы при этом используются.

#### Теоретические сведения и основные понятия межсетевого взаимодействия

* 1. ***Виды межсетевых мастер-ключей (ММК)***

***Межсетевые мастер-ключи*** — мастер-ключи, используемые для генерации классических симметричных ключей обмена для межсетевых связей (для связи коллективов, находящихся в разных сетях).

Межсетевые мастер-ключи делятся на три типа:

***Индивидуальный межсетевой мастер-ключ*** — мастер-ключ, уникальный для данной пары сетей. Вырабатывается по договоренности администратором КЦ одной из сетей и доставляется администратору КЦ другой сети средствами, исключающими их компрометацию (с нарочным).

***Универсальный межсетевой мастер-ключ*** — мастер-ключ, общий для всех сетей. Используется по договоренности между администраторами КЦ сетей. Доставляется из сети, в которой он уже имеется, в сеть, в которой его еще нет, средствами, исключающими его компрометацию.

***Межсетевой мастер-ключ Диффи-Хелмана*** — используемый в качестве мастер-ключа симметричный ключ Диффи-Хелмана. Соответствующие асимметричные ключи Диффи-Хелмана называются асимметричными мастер—ключами. Эти последние ключи создаются администраторами КЦ сетей. Асимметричные мастер-ключи могут быть использованы только для создания межсетевых мастер-ключей Диффи- Хелмана.

Пользователи должны отдавать себе отчет в том, что универсальный межсетевой мастер-ключ становится известным администраторам сразу нескольких сетей, поэтому его компрометация в одной из сетей приведет к компрометации ключей обмена коллективов всех остальных сетей, использующих данный универсальный мастер-ключ. По этой причине в

Ключевом центре принят следующий порядок выбора межсетевых мастер- ключей: при наличии нескольких межсетевых мастер-ключей приоритет отдается индивидуальному ключу, при его отсутствии - мастер-ключу Диффи-Хелмана, и только при отсутствии первых двух ключей используется универсальный межсетевой мастер-ключ.

#### Формирование экспорта и импорта данных для межсетевого взаимодействия

Для организации взаимодействия между различными независимыми сетями ViPNet предусмотрены процедуры обмена данными Экспорта между ЦУСами этих сетей, которые импортируются в соответствующую сеть. Одновременно Ключевые центры должны обменяться некоторой общей ключевой информацией для формирования межсетевых мастер-ключей, на базе которых будут выработаны индивидуальные ключи для взаимодействия АП разных сетей. После установления администратором сети связей с импортированными типами коллективов из других сетей ViPNet, формирования и рассылки для своих АП и СМ справочников и таблиц, новой ключевой информации, выработанной в своем Ключевом центре, абоненты данной сети получают возможность взаимодействовать с абонентами других сетей.

При экспорте формируется ряд файлов, содержащих данные об экспортированных Вами АП, коллективах и абонентах: AN<I>.TXT, NG<I>.TXT, NN<I>.TXT, UL<I>.TXT, UN<I>.TXT и другие, и файл

GT<I>.WAY, содержащий данные об СМ Вашей сети, через который будет осуществляться взаимодействие с другой сетью, где <I> - десятичный номер Вашей сети. Кроме того, ключевым центром формируются и передаются в ЦУС для экспорта файлы с образцами открытых ключей подписей главных абонентов Вашей сети, со списками выведенных из действия подписей абонентов сети.

Эти файлы необходимо передать в ЦУС другой сети. Если уже установлено межсетевое взаимодействие, то эти файлы передаются по каналам связи сети ViPNet.

Рассмотрим действия администраторов двух сетей в ЦУСе и в УКЦ:

1. Администраторы двух ЦУСов выполняют процедуру экспорта из своей сети информации об объектах, которые должны взаимодействовать с объектами другой сети. Экспортируется также по одному из координаторов каждой сети, через которые или с использованием которых будет осуществляться такое взаимодействие. Каким-либо защищенным способом производится обмен этой информацией и ее импорт в свой ЦУС.
2. Администраторам УКЦ необходимо создать один из

межсетевых мастер-ключей. Следует заметить, что симметричные межсетевые мастер-ключи создаются только в одной сети, а в другую передаются, а асимметричный - в обеих сетях, и Администраторы двух сетей обмениваются открытыми частями своего ключа. Поэтому Администраторам двух сетей предварительно нужно договориться, какие межсетевые мастер-ключи будут использоваться для связи между сетями. Предпочтительно использовать для связи двух сетей симметричный индивидуальный мастер-ключ, так как в этом случае безопасность хранения выше (об этом ключе знают Администраторы только двух сетей, а при использовании универсального ключа - Администраторы всех сетей, в которые он экспортирован). Стойкость же асимметричного ключа ниже (симметричного индивидуального и симметричного универсального ключа).

1. Администраторы двух УКЦ производят обмен межсетевыми мастер- ключами по симметричной или асимметричной схеме. Одновременно выполняется обмен справочниками сертификатов ЭЦП Главных абонентов каждой сети и справочниками отозванных сертификатов ЭЦП абонентов каждой сети (даже если этот справочник пустой, т.е. сертификаты ЭЦП в сети ни разу не отзывались).
2. В каждом из УКЦ производится импорт и заверение справочника сертификата Главных абонентов другой сети подписью своего Главного абонента и импорт справочника отозванных сертификатов ЭЦП абонентов другой сети.
3. На основании информации, полученной из ЦУСа каждой сети, в УКЦ каждой сети необходимо сформировать новые ключевые наборы. На этом этапе будет сформирована новая ключевая информация только для своего ЦУСа и Координатора, так как информация о связях других объектов пока неизвестна. После обновления этой информации будет возможно установление соединения между ЦУСами двух сетей.
4. Администраторы каждого из ЦУСов устанавливают необходимые связи импортированных коллективов со своими экспортированными коллективами. Обмениваются уже автоматически через установленное соединение вновь сформированными экспортными данными и отправляют информацию о новых связях своих объектов в свои УКЦ.
5. На основании полученных данных, в УКЦ необходимо сформировать новые ключевые наборы для АП, которых затронули изменения (в ключевых дискетах абонентов в этой ситуации изменений быть не может). Эти ключевые наборы обычным образом отправляются в свой ЦУС для рассылки по своей сети и автоматического обновления.

#### Методические указания по выполнению лабораторной работы

Шаги, необходимые для межсетевого взаимодействия защищенных сетей ViPNet, включающие:

* теоретическую проработку схемы объединения защищенных сетей;
* инсталляцию рабочих мест Администраторов двух защищенных сетей;
* первоначальное развертывание двух защищенных сетей;
* формирование начального экспорта в одной из защищенных сетей;
* передача начального экспорта во вторую защищенную сеть;
* прием начального экспорта и формирование ответного экспорта во второй защищенной сети;
* генерация новой ключевой информации и рассылка ее всем СУ второй защищенной сети;
* передача ответного экспорта в первую защищенную сеть;
* прием ответного экспорта в первой защищенной сети;
* генерация новой ключевой информации и рассылка ее всем СУ первой защищенной сети;
* проверка правильности установления межсетевого взаимодействия.

###### Задание на занятие:

Организовать межсетевое взаимодействие двух ViPNet сетей, исходя из нижеперечисленных условий и приведенной схемы (Рис. 1).

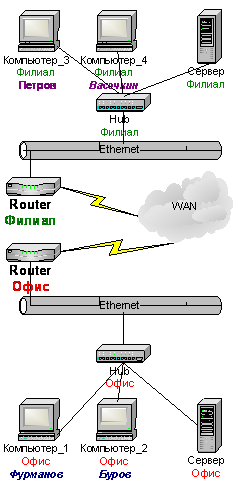


Рис. 1 Схема для организации межсетевого взаимодействия

Условия построения защищенной сети 1 (Офис):

* в защищенную сеть 1 включаются следующие СУ: СМ Сервер Офис, АП Компьютер\_1 (Фурманов), АП Компьютер\_2 (Буров);
* Администратором и Главным абонентом защищенной сети будет Фурманов.

Условия построения защищенной сети 2 (Филиал):

* в защищенную сеть 2 включаются следующие СУ: СМ Сервер Филиал, АП Компьютер\_3 (Петров), АП Компьютер\_4 (Васечкин);
* Администратором и Главным абонентом защищенной сети будет Петров.

Условия межсетевого взаимодействия Филиала и Офиса:

Защищенные сети Офиса и Филиала имеют следующие номера: № 6670 и № 6671. Полная связность – все видят всех. Межсетевое взаимодействие организуется на **Ассимметричном Межсетевом Мастер- ключе** (АММК), причем на **индивидуальном.**

Последовательность выполнения занятия:

Перед тем как приступить к организации межсетевого взаимодействия, необходимо сформировать две ViPNet сети, исходя из вышеприведенных схем и условий. В качестве справочника можно воспользоваться Лабораторной работой № 1.

Кто из администраторов двух сетей начнет процесс установления межсетевого взаимодействия для нас не важно. Пусть это будет администратор ViPNet сети офиса, т. е. администратор сети № 6670.

*Для установки межсетевого взаимодействия необходимо:*

1. Сформировать начальный экспорт в сети № 6670.
2. Принять экспорт из сети № 6670 в сети № 6671.
3. Сформировать ответный экспорт в сети № 6671 для сети № 6670.
4. Принять ответный экспорт из сети № 6671 в сети № 6670.

*Начальный экспорт* ***для случая АММК*** *содержит* ***3 составляющие:***

1. Экспортные справочники (готовятся в ЦУСе).
2. Межсетевой мастер-ключ (генерируется в КЦ).
3. Сигнатура подписи главного абонента (храниться в ..\KC\PSW\**\*.chf**).

*Ответный экспорт* ***для случая АММК*** *содержит* ***2 составляющие:***

1. Экспортные справочники (готовятся в ЦУСе).
2. Сигнатура подписи главного абонента (храниться в ..\KC\PSW\**\*.chf**).

В отличие от СММК, АММК формируется в каждой из сетей, после чего администраторы обмениваются открытыми частями (ОЧ) АММК, сохраняя закрытые части (ЗЧ) в тайне. В каждой защищенной сети мы формируем некие ММКлючи, которые состоят из ОЧ своего АММК и ЗЧ АММК другой защищенной сети, причем эти ММК получаются одинаковыми. Таким образом, мы получаем один и тот же ММК в обеих защищенных сетях, не передавая, по открытым каналам передачи данных, секретной информации.

Предварительная подготовка:

Для того чтобы не повторять то, что мы уже делали, т.е. не инсталлировать снова рабочие места двух администраторов и не формировать

«с нуля» две защищенные сети, мы выполним ряд «хитрых» действий. В

результате мы получим две сформированные защищенные сети, но уже без установленного меж ними взаимодействия.

Итак, приступим к нулевому, подготовительному шагу.

**Часть 1**

Шаг 0(15)

*Удаление межсетевого взаимодействия и ИСММК*

Можно, конечно, все сделать вручную – удалить экспорт, межсетевой канал и межсетевые связи, но мы сделаем это быстрее и проще. Если Вы помните, то после того как были завершены все необходимые действия в ЦУСе при первоначальном развертывании сети, мы ЦУС закрывали, а при закрытии - ЦУС предлагал создать архив. В этот архив помещаются все те данные, которые мы сформировали в адресной и прикладной администрациях для того, чтобы можно было их восстановить в случае сбоя с потерей данных. Воспользуемся архивом и восстановим данные, которые были в ЦУСе до установления межсетевого взаимодействия.

Загружаем ЦУС сети № 6670 и выбираем пункт меню *Службы  Архивы баз данных...* Перед нами появится окно (Рис. 2) со списком всех архивов, которые ЦУС формировал. Выберем самый ранний архив и нажмем кнопку *Восстановить.*

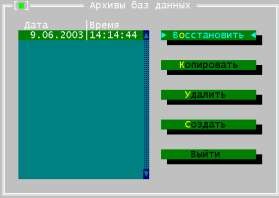


Рис. 2 Архивы баз данных ЦУСа

ЦУС задаст сначала вопрос о восстановлении баз данных из архива, а затем спросит - создавать ли архив текущих баз данных. На оба вопроса отметим утвердительно, нажимая на кнопку *Да.* После чего ЦУС восстановит базы данных из первого архива, а нам останется нажать на кнопку *Выйти* и попасть в основное меню ЦУСа.

Необходимо убедиться, что базы данных восстановлены. Для этого выбираем пункт меню *Прикладная администрация  Регистрация типов коллективов...* В списке ТК не должно быть ТК экспортированных из сети №

6671. Далее нажимаем на кнопку *Выйти* и выбираем пункт меню *Службы  Экспорт...* Запись об экспорте останется (Рис. 9) и поэтому, для избежания аномальных ситуаций при формировании всех справочников, мы ее удалим, нажав на кнопку *Удалить*, на вопрос ответим *Да*, а затем нажмем на кнопку *Выйти*.

Теперь сформируем все справочники, выбрав одноименный пункт меню *Службы.*

Для АП Компьютер\_1 (Фурманов) необходимо выслать обновленные адресные справочники (см. Шаг № 24, Ч1), после чего загрузим Монитор рабочего места администратора сети № 6670 (см. Шаг № 25, Ч1). Транспортный модуль у нас уже настроен, поэтому обновление будет принято сразу, а после перезагрузки Монитора мы увидим, что в списке фильтров для защищенных узлов пропали фильтры для СУ из сети № 6671 (Рис. 3).

Закрываем программу Монитор.

На самом деле мы обновили только адресные справочники, а КН все еще содержит ключи шифрования для СУ из сети № 6671, **но для нас это**

сейчас не важно.

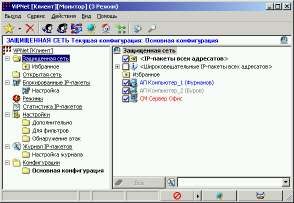


Рис. 3 Окно Монитора АП Компьютер\_1 (Фурманов)

Мы восстановили ЦУС, необходимо еще восстановить КЦ и удалить ненужные файлы. Для этого переходим в каталог установки КЦ сети № 6670 (Рис. 4).

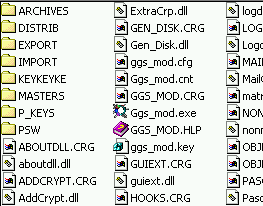


Рис. 4 Структура рабочих каталогов КЦ

* 1. В каталоге **..\KC\ARCHIEVE\** выбираем самый ранний архив и извлекаем из него файл **Interkey.num (MASTERS.LZH)**, который необходимо поместить в каталог **..\Kc\Masters**, перезаписав в нем файл с таким же именем.
  2. В каталогах **..\Kc\Masters** и **..\Kc\Export** удаляем файл с расширением **\*.i00**, т.е. СММК.
  3. В каталоге **..\Kc\Psw** удаляем все файлы, в названии которых присутствуют **1A0F**, в том числе – сертификат ЭЦП главного абонента сети № 6671**. Не перепутайте** - **1A0F, а не 1A0Е.** Удалите также здесь каталог IN.
  4. В каталоге **..\Kc\Export** нужно удалить файл **\*.i00**

После этого загружаем КЦ сети № 6670, по «просьбе» КЦ создаем архив и выбираем пункт меню *Действия  Просмотр  Смежные сети и мастер-ключи.* Перед нами появится окно в котором должна отсутствовать информация о наличии каких-либо ММК (Рис. 5).

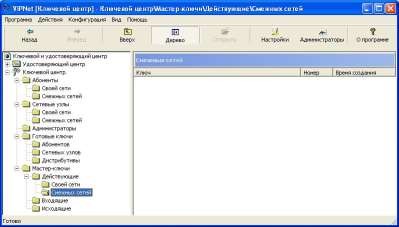


Рис. 5 Смежные сети и мастер-ключи

Нажимаем на кнопку *Выход* и выходим из КЦ.

Все вышеописанные действия надо теперь проделать и для сети № 6671, за исключением того, что в п.3 необходимо удалить уже данные о сети № 6670, т.е. файлы с **1A0Е. Не перепутайте** - **1A0E, а не 1A0F.**

По завершении всех действий Шага № 0 мы должны получить две защищенные сети, как бы только что сформированные и готовые для установления межсетевого взаимодействия, в соответствии с заданием.

Поскольку многие шаги будут такими же, как и в первой части, далее по тексту будут приводиться ссылки на них.

*Начальный экспорт* ***для случая АММК*** *содержит* ***3 составляющие:***

1. Экспортные справочники (готовятся в ЦУСе).
2. ОЧ асимметричного межсетевого мастер-ключа (генерируется в КЦ).
3. Сертификат ЭЦП главного абонента и другие справочники сертификатов (хранятся в ..\KC\PSW\).

*Ответный экспорт* ***для случая АММК*** *содержит* ***3 составляющие*** *(в*

*отличие от случая для СММК)****:***

1. Экспортные справочники (готовятся в ЦУСе).
2. ОЧ асимметричного межсетевого мастер-ключа (генерируется в КЦ).

Сертификат ЭЦП главного абонента и другие справочники сертификатов (хранятся в ..\KC\PSW\).

**Часть 2**

Шаг 1

*Формирование Экспорта в ЦУСе*

Запускаем ЦУС сети № 6670 и переходим в меню *Службы *

*Экспорт...* (Рис. 6). Перед нами появляется окно формирования экспорта,

нажимаем кнопку *Добавить* и, в появившемся окне, вводим номер сети для которой готовим экспорт, т.е. **6671** (Рис. 7).

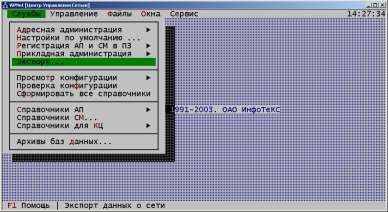


Рис. 6 Меню *Службы* в ЦУСе

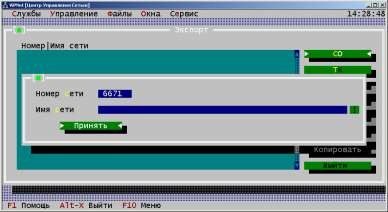


Рис. 7 Задание номера сети для формирования экспорта

В строку *Имя сети* можно внести комментарий о сети, для которой готовим экспорт. Эта строка имеет справочное назначение и никуда не передается.

Для экспорта необходимо предоставить СО и соответствующие им ТК. Это делается для того, чтобы в дальнейшем организовать связи и сформировать ключи шифрования для них. Исходя из задания (полная связность) выбираем ТК на экспорт – нажимаем последовательно, в появляющихся окнах, кнопки *ТК*, *Добавить, Все* и *Принять.* Получаем окно с выбранными на экспорт ТК (Рис. 8).



Рис. 8 Экспортируемые ТК

Нажимаем на кнопку *Выйти* и попадаем в основное окно подготовки экспорта (Рис. 9).

Теперь необходимо проконтролировать, что у нас выбраны СО на экспорт – нажимаем кнопку *СО.* В том случае, когда сначала выбираются ТК,

соответствующие им СО выбираются автоматически. Если же сначала

выбрать СО, то потом придется выбирать еще и ТК.

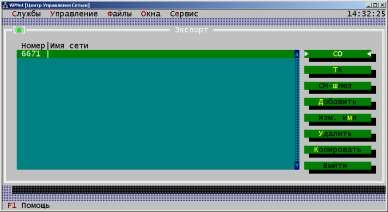


Рис. 9 Окно подготовки экспорта в ЦУСе

Шаг 2

*Задание шлюза*

При установлении межсетевого взаимодействия необходимо в обеих ViPNet сетях определить СМ для организации шлюзов. Шлюзы необходимы для того, чтобы определить путь прохождения конвертов, формируемых ДП и файлов, пересылаемых по файловому обмену.

Итак, требуется задать шлюз. Делаем это нажатием кнопки *СМ-шлюз*. Перед нами появляется информационное окно, говорящее о том, что шлюз не задан (Рис. 10).



Рис. 10 Сообщение об отсутствии шлюза

Нажимаем на кнопку *Сменить шлюз* и выбираем СМ, который мы хотим использовать в качестве шлюза (в нашем случае сервер один, его и выбираем) (Рис. 11), нажимаем на кнопку *Принять*.

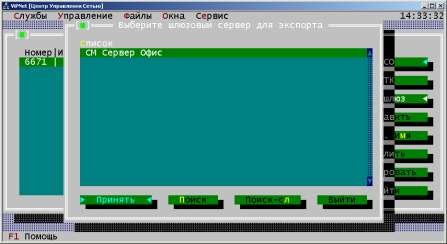


Рис. 11 Окно выбора шлюза

Теперь желательно еще раз убедиться, что мы сделали все правильно:

* проверяем наличие экспортируемых СО;
* проверяем наличие экспортируемых ТК;
* проверяем наличие шлюза.

На этом подготовка экспорта для сети № 6671 в ЦУСе завершается.

Шаг 3

*Копирование экспорта*

Сейчас мы находимся в меню экспорта (Рис. 9). Нажимаем кнопку *Копировать*. Перед нами появляется окно задания пути для копирования экспорта (Рис. 12). Просто **запоминаем этот путь** и нажимаем кнопку *Принять*.



Рис. 12 Задание пути для копирования экспорта

После того, как ЦУС скопирует файлы экспорта, на экране появится информационное окно (Рис. 13). Нажимаем на любую клавишу и выходим из ЦУСа.

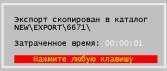


Рис. 13 Экспорт скопирован

Шаг 4

*Генерация асимметричного ММК для сети № 6670*

Отметим, что **АММК**, в отличие от СММК, **генерируется не для удаленной защищенной сети, а для своей** и состоит из двух частей: секретной части АММК - хранится в тайне и открытой части АММК – передается в другую защищенную сеть в составе начального или ответного экспорта.

Именно открытыми частями и должны, в нашем случае, обменяться администраторы сетей №№ 6670 и 6671.

Запускаем КЦ сети № 6670, выбираем пункт меню *Программа  Генерация мастер-ключей  Межсетевые мастер-ключи  Ассиметричный* (Рис. 14)*.*

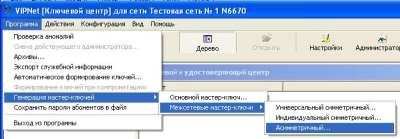


Рис. 14 Меню генерации мастер-ключей в КЦ

Перед нами появляется информационное окно (Рис. 15), в котором присутствует номер генерируемого мастер-ключа и предупреждающая информация о том, что ключи шифрования, созданные на основе нового мастер-ключа, не смогут стыковаться со старыми ключами шифрования, которые создавались на существующем мастер-ключе (если он уже есть).

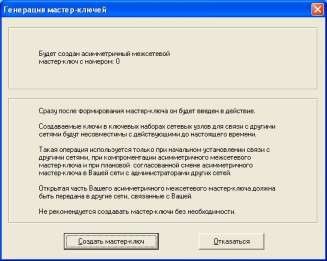


Рис. 15 Окно создания АММК

Нажимаем кнопку *Создать мастер-ключ*, отвечаем на вопрос нажатием кнопки *ОК*, «крутим» рулетку и еще раз нажимаем кнопку *ОК.*

АММК для сети № 6670 создан.

Шаг 5

*Экспорт ОЧ сгенерированного АММК для сети № 6670*

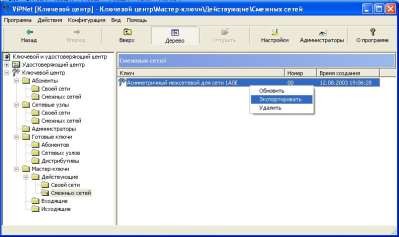


Рис. 16 Экспорт межсетевых мастер-ключей

Выбираем раздел *Ключевой центр  Мастер-ключи  Смежных сетей.* В появившемся окне подсвечиваем запись *Асимметричный для сети 6670* и по контекстному меню выбираем кнопку *Экспортировать* (Рис. 16). В появившемся окне вводим пароль Главного абонента и нажимаем на кнопку *ОК*, затем еще раз *ОК* и *Закрыть*.

После этого программу КЦ можно закрыть, все необходимые действия в ней сделаны.

Все, что остается сделать администратору сети № 6670 – это собрать вместе все 3 составляющие начального экспорта и передать их администратору сети № 6671 любым доступным ему способом.

Шаг 6

*Передача начального экспорта для сети № 6671 ее администратору*

Итак, собираем составляющие начального экспорта в одно место. Для этого на жестком диске создадим папку, например C:\EXP\_for\_6671\.

* 1. Из ЦУСа необходимо взять экспортные адресные справочники. На данный момент они находятся в каталоге

..\NCC\New\Export\6671\ (этот путь был установлен по умолчанию – Шаг №3 Ч1), копируем **всю папку ..\6671\\*.\*** в нашу папку.

* 1. Из КЦ необходимо взять экспортированную ОЧ АММК для сети № 6670. Она находится в папке ..\КС\Export\**\*.p00**. Копируем ее в нашу папку – C:\EXP\_for\_6671\.
  2. Необходимо проконтролировать, что справочники сертификатов ЭЦП *1A0E.CHF, 1A0E.TRL, 1A0E\_REM.CRL, 1A0E\_REM.SGN, 1A0E1A0F.VAR* из КЦ попали в папку **C:\EXP\_for\_6671\6671\**, т.е. в папку с экспортными адресными справочниками из ЦУСа.

Теперь всю папку **C:\EXP\_for\_6671\** необходимо заархивировать и передать администратору сети № 6671 любым доступным способом (например, с помощью e-mail).

На этом этапе работа Администратора сети № 6670 закончена.

Шаг 7

*Прием начального экспорта из сети № 6670 администратором сети*

*№ 6671.*

Администратор сети № 6671 принимает начальный экспорт из сети № 6670 следующим образом:

1. **Содержимое** папки **..\EXP\_for\_6671\6671\\*.\*** (экспортные адресные справочники и образец подписи главного абонента) копируем в ЦУС сети № 6671 в папку ..\NCC\Import\.
2. ОЧ АММК для сети № 6670 копируем из папки **..\EXP\_for\_6671\\*.p00**

в КЦ ..\КС\Import\.

**Часть 3**

Шаг 8

*Подключение межсетевого канала*

Загружаем ЦУС сети № 6671 и просматриваем сообщения о принятом экспорте. Сначала мы увидим сообщение о принятой подписи главного абонента сети № 6670 (Рис. 17), затем сообщение об изменении в составе шлюзов (Рис. 18). Нажимаем на кнопку *Esc*, затем пробел, видим сообщение об изменениях в импорте (Рис. 19), нажимаем пробел и видим сообщение об изменении в файле шлюзов, с **рекомендацией проверить межсетевые**

каналы (Рис. 20).



Рис. 17 Поступили новые справочники

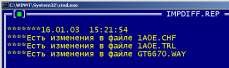


Рис. 18 Сообщение об изменении в составе шлюзов



Рис. 19 Сообщение об изменении в импорте



Рис. 20 Сообщение об изменении в файле шлюзов

Вот с этого и начнем. Дело в том, что шлюз при межсетевом взаимодействии должен быть определен не только на прикладном уровне, но и на адресном, т.е. должен быть сформирован **межсетевой канал.**

Заходим в адресную администрацию – меню *Службы  Адресная администрация  Адреса в сети «Инфотекс»...* Перед нами появляется сообщение об изменении межсетевых каналов (Рис. 21).



Рис. 21 Сообщение адресной администрации

Нажимаем пробел и попадаем в основное меню адресной администрации. Выбираем пункт *Межсетевые каналы.*

Перед нами появляется список межсетевых каналов, в нашем случае он один и выключен (Рис. 22). Как видно, имя чужого СМ-шлюза задано, а своего еще нет (на самом деле нам еще придется производить такие же действия по подключению межсетевого канала в ЦУСе сети № 6670, на данный момент информация о нашем шлюзе взята из файла экспорта **gt\*.way** – ведь на прикладном уровне в ЦУСе сети № 6670 мы его уже задали).

Для того чтобы включить межсетевой канал, нажимаем на кнопку *Enter* два раза – внизу окна появится имя своего сервера (СМ Сервер Филиал), а состояние измениться на *Вкл* (Рис. 23)*.*

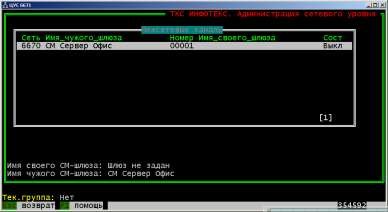


Рис. 22 Межсетевой канал выключен

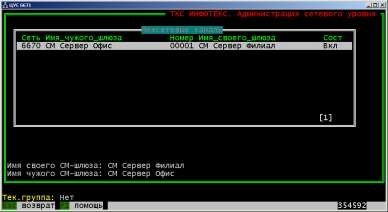


Рис. 23 Межсетевой канал включен

Нажимаем *Esc* и попадаем в основное меню. Выполняем *Выдать таблицы маршрутизации* и выходим из этого меню в главное (нажимаем *Esc*).

Шаг 9

*Образование требуемых связей между ТК сетей №№ 6670 и 6671*

Нам необходимо связать ТК, которые были экспортированы из сети № 6670 с ТК сети № 6671. Для этого выбираем пункт меню *Службы  Прикладная администрация  Регистрация типов коллективов...*

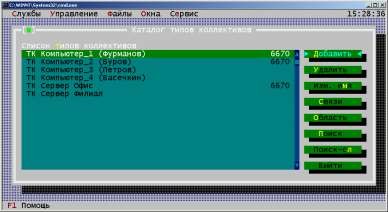


Рис. 24 Новый список ТК

В появившемся списке ТК (Рис. 24) мы видим три новых ТК и справа помечено, что они принадлежат сети № 6670. Выбираем один из этих ТК, например, ТК Компьютер\_1 (Фурманов), и нажимаем кнопку *Связи*. Список связей пока пустой, нажимаем кнопку *Добавить*, потом кнопки *Все* (по заданию – связность полная) и *Принять.* Теперь этот ТК уже связан со всеми ТК из сети № 6671. Нажимаем кнопку *Выйти.*

Повторим вышеописанные действия для двух оставшихся ТК из сети

№ 6670 – ТК Компьютер\_2 (Буров) и ТК Сервер Офис.

Теперь по нажатию кнопки *Связи* для любого из трех ТК сети № 6670 мы увидим список ТК (Рис. 25).

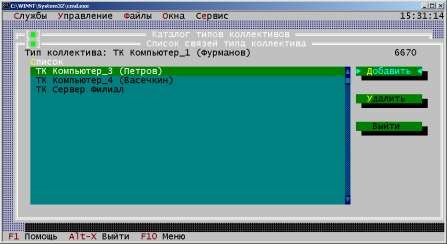


Рис. 25 Список связей экспортированных ТК

Шаг 10

*Формирование экспорта в сеть № 6670*

Итак, ЦУС сети № 6671 принял экспорт из сети № 6670. Теперь необходимо сформировать свой экспорт в сеть № 6670. Как и ранее (Шаг 1) выбираем пункт меню *Службы  Экспорт...* и попадаем в меню подготовки экспорта (Рис. 26). Как видим, здесь уже присутствует запись для сети № 6670 (поскольку ЦУС сети № 6671 принял экспорт из сети № 6670). Нам необходимо выставить на экспорт СО и ТК сети № 6671, что мы и сделаем. Подсвечиваем запись *6670* и нажимаем кнопку ТК, затем в появляющихся окнах последовательно нажимаем кнопки *Добавить, Все* и *Принять.* Получаем окно с выбранными на экспорт ТК (Рис. 27).

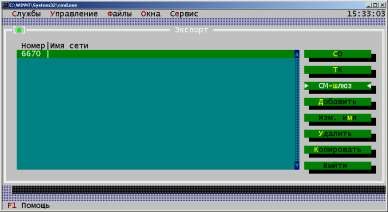


Рис. 26 Окно экспорта

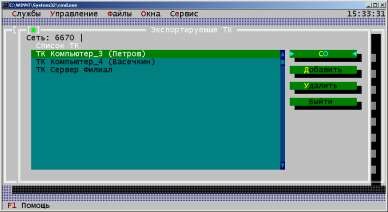


Рис. 27Список экспортируемых ТК

Нажимаем на кнопку <Esc>, потом нажимаем на кнопку СО и проверяем, что СО тоже выбраны, если же список пуст, то нажимаем на кнопки *Добавить, Все, Принять* и *Выйти.*

Шаг 11

*Задание шлюза и копирование экспорта*

Находясь в окне экспорта (Рис. 26), нажимаем на кнопку *СМ-шлюз,* затем кнопку *Сменить шлюз* (Рис. 10), перед нами появляется окно выбора шлюзов (Рис. 11) в котором присутствует единственный СМ сети № 6671 – СМ Сервер Филиал. Подсвечиваем его, нажимаем кнопку *Принять* и снова попадаем в окно экспорта.

Все, что осталось сделать – это скопировать экспорт в каталог по умолчанию и выйти в основное меню ЦУСа. Для этого нажимаем кнопку *Копировать,* затем *Принять*, нажимаем на любую клавишу и потом на кнопку <Esc>.

Шаг 12

*Формирование всех справочников*

Поскольку мы задали новые связи, необходимо теперь сформировать ключевую и адресную информацию. Соответственно необходимо сформировать справочники. Для этого выбираем пункт меню *Службы  Сформировать все справочники.* ЦУС сформирует все необходимые справочники и выдаст окно отчета. Нажимаем кнопку *Принять* и выходим из ЦУСа (сочетание клавиш <Alt+X>). На вопрос ЦУСа о создании архива ответим утвердительно.

**Часть 4**

Шаг 13

*Регистрация сертификата ЭЦП главного абонента сети № 6670 в КЦ сети № 6671*

Загружаем КЦ сети № 6671, перед нами появляется предложение КЦ о создании экспорта с вариантами сетевых узлов для смежных сетей (Рис. 28). Нужно это для обеспечения нормальной работы при активизации процедуры компрометации в одной из сетей, поэтому на вопрос ответим утвердительно.

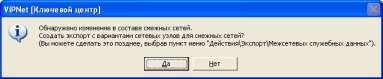


Рис. 28 Предложение КЦ создать импорт с вариантами АП

Ключевой Центр сообщит об успешности проведенной операции и далее выдаст сообщение *«Обнаружен справочник сертификатов ЭЦП главных абонентов из смежной сети»* и спросит, желаете ли Вы импортировать его немедленно или сделаете это позднее. Отвечайте *«Да»*.

После этого перед нами появится окно со списком справочников ЭЦП главных абонентов из других сетей (Рис. 29).



Рис. 29 Импорт сертификатов ЭЦП главных абонентов

Выделяем первую из записей *Сеть <6670>* и нажимаем кнопку *Просмотреть сертификат ЭЦП.* Появится окно (Рис. 30), в котором можно посмотреть сам сертификат ЭЦП главного абонента, дату создания и срок окончания действия подписи. Один из сертификатов окажется действительным, а второй – нет, так как в версии 2.8 создаются как новые сертификаты ЭЦП (формата Х.509), так и ЭЦП старого образца.

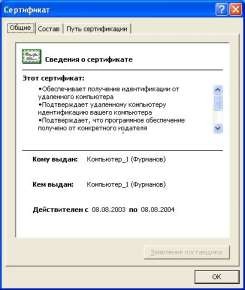


Рис. 30 Просмотр сертификата ЭЦП главного абонента сети № 6670

Нажимаем кнопку *Принять.* Напротив записи *Сеть <6670>* появится галочка. Только после того, как подпись была просмотрена, ее можно

импортировать!

Нажимаем на кнопку *Импорт* (Рис. 29)*,* в появившемся окне (Рис. 31) нажимаем кнопку *ОК,* потом еще раз *ОК* и *Выход.* Импорт подписи главного абонента сети № 6670 завершен.

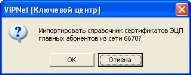


Рис. 31 Подтверждение импорта

Шаг 14

*Импорт ОЧ АММК для сети № 6670 в КЦ сети № 6671*

Выбираем раздел *Ключевой центр  Мастер-ключи  Входящие*. Перед нами появится окно, в котором будет присутствовать запись *Асимметричный* (Рис. 32). В столбце *Номер* можно посмотреть номер ключа. В контекстном меню нажимаем на кнопку *Импортировать*, затем нажимаем кнопки *ОК* и *Закрыть.*

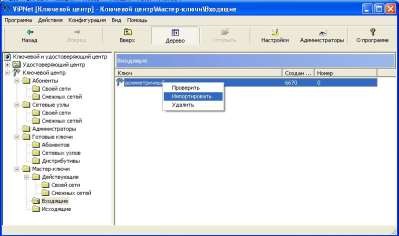
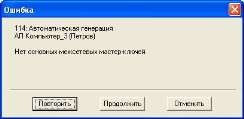


Рис. 32 Список ММК для импорта

Теперь, в свою очередь, администратор сети № 6671 должен сгенерировать свой АММК.

**Внимание!!!** Если Вы забудете это сделать, то при попытке сформировать ключевую информацию для СУ, КЦ будет выдавать сообщение об ошибке (Рис. 33). В этом случае нажимаем поочередно на кнопки *Отменить*, *ОК*, *Выход* и переходим к выполнению следующего шага*.*



**Часть 5**

**Шаг 15**

Рис. 33 Сообщение об ошибке

*Экспорт ОЧ сгенерированного АММК для сети № 6671*

Выбираем раздел *Ключевой центр  Мастер-ключи  Действующие  Смежных сетей.* В появившемся окне подсвечиваем запись *асимметричный для сети 6671* и нажимаем кнопку *Экспорт* (Рис. 34).

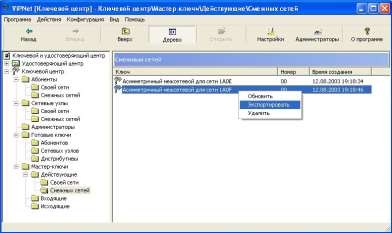


Рис. 34 Экспорт межсетевых мастер-ключей

В появившемся окне вводим пароль Главного абонента и нажимаем на кнопку *ОК*, затем еще раз *ОК* и *Закрыть*.

Шаг 16

*Формирование новых КН и перенос их в ЦУС*

Только после того, как мы импортировали ИСММК можно приступать к формированию новой ключевой информации для СУ сети № 6671, ТК которых связаны с ТК, экспортированными из сети № 6670.

Выбираем разделе *Программа  Автоматическое формирование ключей.* Поскольку это первое, за этот сеанс работы с КЦ, формирование ключей – необходимо «прокрутить» рулетку, после чего, в появившемся окне, нажать на кнопку *Старт*, потом на кнопки *ОК* и *Выход.*

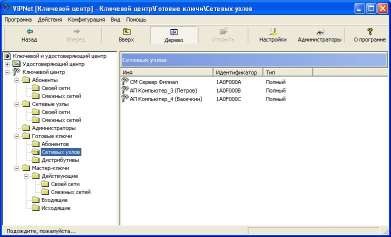


Рис. 35 Готовые КН для СУ сети № 6671.

Новые КН необходимо перенести в ЦУС. Выбираем раздел *Ключевой центр  Готовые ключи  Сетевых узлов*, выделяем все КН и по контекстному меню *Перенести – в ЦУС* отправляем их в ЦУС для рассылки обновлений.

Нажимаем на кнопку *Закрыть* и выходим из КЦ.

Шаг 17

*Рассылка обновлений*

Запускаем ЦУС сети № 6671. Сначала разошлем КН, а потом адресные справочники. Выбираем пункт меню *Управление  Отправить измененные файлы  Ключевые наборы для СУ...*, в появившемся окне (Рис. 36) нажимаем кнопки *Все* и *Отправить*, изменяем дату обновления на «заднее число» и нажимаем кнопку *Принять*, а потом *Выйти.*

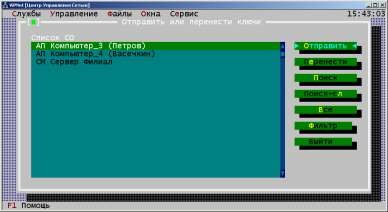


Рис. 36 Список КН для отправки

Теперь отправим адресные справочники. Выбираем пункт меню *Управление  Отправить измененные файлы  Справочники АП и СМ...*, в появившемся окне нажимаем кнопки *Все* и *Отправить*, изменяем дату обновления на «заднее число» и нажимаем кнопку *Принять*, а потом *Выйти.* Выходим из ЦУСа.

Шаг 18

*Передача ответного экспорта для сети № 6670 ее администратору*

Итак, собираем составляющие ответного экспорта в одно место. Для этого на жестком диске создадим папку, например C:\EXP\_for\_6670\.

1. Из ЦУСа необходимо взять экспортные адресные справочники. На данный момент они находятся в каталоге ..\NCC\New\Export\6670\ (этот путь был установлен по умолчанию), копируем **всю папку**

**..\6670\\*.\*** в нашу папку.

1. Из КЦ необходимо взять экспортированную ОЧ АММК для сети № 6671. Она находится в папке ..\КС\Export\**\*.p00**. Копируем ее в нашу папку – C:\EXP\_for\_6670\.
2. Необходимо проконтролировать, что справочники сертификатов ЭЦП *1A0F.CHF, 1A0F.TRL, 1A0F\_REM.CRL, 1A0F\_REM.SGN, 1A0F1A0E.VAR* из КЦ попали в папку **C:\EXP\_for\_6670\6670\**, т.е. в папку с экспортными адресными справочниками из ЦУСа.

Теперь всю папку **C:\EXP\_for\_6670\** необходимо заархивировать и передать администратору сети № 6670 любым доступным способом (например, с помощью e-mail).

На этом работа Администратора сети № 6671 закончена.

Шаг 19

*Прием ответного экспорта из сети № 6671 администратором сети*

*№ 6670*

Администратор сети № 6670 принимает ответный экспорт из сети № 6671 следующим образом:

1. **Содержимое** папки **..\EXP\_for\_6670\6670\\*.\*** (экспортные адресные справочники и образец подписи главного абонента) копируем в ЦУС сети № 6670 в папку ..\NCC\Import\.
2. ОЧ АММК для сети № 6671 копируем из папки **..\EXP\_for\_6671\\*.p00**

в КЦ ..\КС\Import\.

Шаг 20

*Подключение межсетевого канала*

Загружаем ЦУС сети № 6670, вводим пароль администратора сети (у нас администратор и главный абонент – одно и то же лицо), перед нами появляется первое информационное сообщение (Рис. 37).



Рис. 37 Поступили новые справочники

Нажимаем любую клавишу и перед нами появляются новые окна (Рис. 18 – 20) с напоминанием о необходимости включить межсетевой канал.

Межсетевой канал включается в адресной администрации. Выбираем пункт меню *Службы  Адресная администрация  Адреса в сети*

*«Инфотекс»...* Перед нами появляется сообщение об изменении межсетевых каналов (Рис. 21). Нажимаем пробел и попадаем в основное меню адресной администрации. Выбираем пункт *Межсетевые каналы.*

Перед нами появляется список межсетевых каналов, в нашем случае он один и пока выключен (Рис. 38). Как видно, имя чужого СМ-шлюза задано, а своего еще нет.

Для того чтобы включить межсетевой канал, нажимаем на кнопку *Enter* два раза – внизу окна появится имя своего сервера (СМ Сервер Офис), а состояние измениться на *Вкл* (Рис. 39)*.*

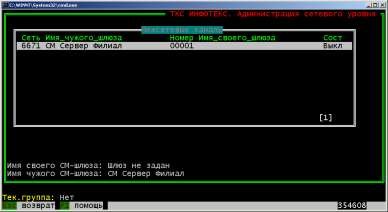


Рис. 38 Межсетевой канал выключен

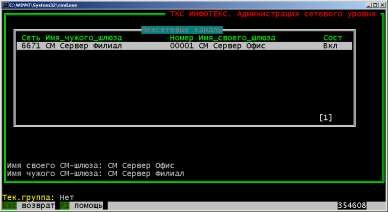


Рис. 39 Межсетевой канал включен

Нажимаем *Esc* и попадаем в основное меню. Выполняем *Выдать таблицы маршрутизации* и выходим из этого меню в главное (нажимаем *Esc*).

Шаг 21

*Проверка наличия связей между ТК сетей №№ 6670 и 6671*

В справочниках связей ответного экспорта уже содержится информация о тех связях между ТК двух сетей, которые установил администратор сети № 6671. Поэтому устанавливать эти связи в ЦУСе сети

№ 6670 не требуется. Мы просто проверим, что все сделали правильно и что связи между ТК сетей №№ 6670 и 6671 установлены. Выбираем пункт меню *Службы  Прикладная администрация  Регистрация типов коллективов...* В появившемся списке ТК есть и ТК из сети № 6671 (Рис. 40).

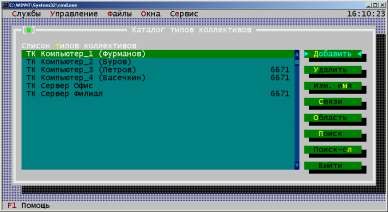


Рис. 40 Список ТК после приема экспорта

Для контроля установленных связей поочередно просмотрим связи ТК сети № 6670 (или сети № 6671), например, для Фурманова список связей будет выглядеть как на рис. 41.

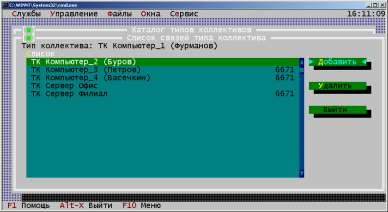


Рис. 41 Список связей ТК Компьютер\_1 (Фурманов)

Шаг 22

*Формирование всех справочников*

Для того, чтобы сформировать новые КН и адресные справочники выбираем пункт меню *Службы  Сформировать все справочники.* ЦУС сформирует все необходимые справочники и выдаст статистику по

произведенным действиям. Нажимаем кнопку *Принять* и выходим из ЦУСа, на вопрос о необходимости формировать архив ответим утвердительно.

Шаг 23

*Регистрация сертификата ЭЦП главного абонента сети № 6671 в КЦ сети*

*№ 6670*

Загружаем КЦ сети № 6670. Как и в КЦ сети № 6671, перед нами появляется предложение о создании импорта с вариантами АП для смежных сетей (Рис. 28). Нажимаем на кнопку *Yes*. Перед нами появится окно со списком новых справочников ЭЦП главных абонентов из других сетей (Рис. 42). Выделяем по очереди обе записи *Сеть <6671>* и нажимаем кнопку *Просмотреть сертификат ЭЦП.* Появится окно (Рис. 43), в котором нажимаем кнопку *ОК.*

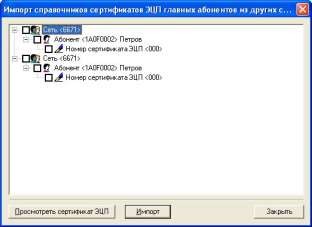


Рис. 42 Импорт ЭЦП главных абонентов

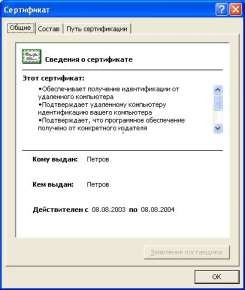


Рис. 43 Просмотр сертификата ЭЦП главного абонента сети № 6671

Напротив записи *Сеть <6671>* появится галочка. **Только после**

того, как подпись была просмотрена, ее можно импортировать!

Нажимаем на кнопку *Импорт* (Рис. 42)*,* в появившемся окне (Рис. 44) нажимаем кнопку *ОК,* потом еще раз *ОК* и *Выход.* Импорт подписи главного абонента сети № 6671 завершен.

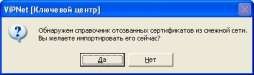


Рис. 44 Подтверждение импорта

Шаг 23

*Импорт отозванных сертификатов ЭЦП*

После того, как мы импортировали ЭЦП главного абонента сети № 6671 м нам нужно импортировать отозванные сертификаты.

В открывшемся окне (Рис. 45) мы должны нажать ДА, а затем в следующем окне (Рис. 46) импортировать нужные справочники

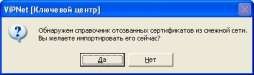


Рис. 45 Обнаружен справочник отозванных сертификатов

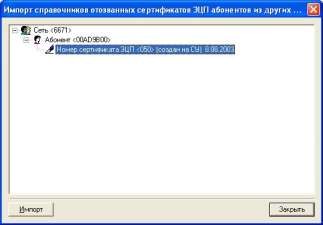


Рис. 46 Импорт справочников отозванных сертификатов ЭЦП

Шаг 24

*Импорт ОЧ АММК для сети № 6671 в КЦ сети № 6670*

Выбираем раздел *Ключевой центр  Мастер-ключи  Входящие*. Перед нами появится окно, в котором будет присутствовать запись *Асимметричный* (Рис. 47). В столбце *Номер* можно посмотреть номер ключа. Нажимаем на кнопку *Импортировать*, затем нажимаем кнопки *ОК* и *Закрыть.*

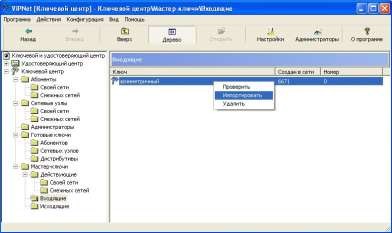


Рис. 47 Список ММК для импорта

Шаг 25

*Формирование новых КН и перенос их в ЦУС*

После того, как мы зарегистрировали ЭЦП главного абонента сети № 6671 можно приступать к формированию новой ключевой информации для СУ сети № 6670, ТК которых связаны с ТК, экспортированными из сети № 6671.

Выбираем пункт меню *Программа  Автоматическое формирование ключей.* «Крутим» электронную рулетку, затем, в появившемся окне, нажимаем на кнопку *Старт*, потом на кнопки *ОК* и *Выход.*

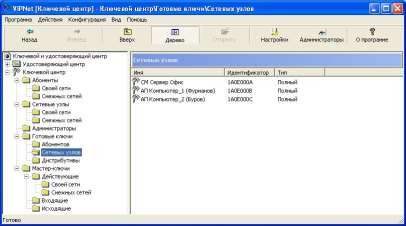


Рис. 48 Готовые КН для СУ сети № 6671

Новые КН необходимо перенести в ЦУС. Выбираем раздел *Ключевой центр*

* Готовые ключи  Сетевых узлов*, выделяем все КН и по контекстному меню *Перенести - в ЦУС* отправляем КН в ЦУС для рассылки обновлений Нажимаем на кнопку *Закрыть* и выходим из КЦ.

Шаг 26

*Рассылка обновлений*

Запускаем ЦУС сети № 6670. Сначала разошлем КН, а потом адресные справочники. Выбираем пункт меню *Управление  Отправить измененные файлы  Ключевые набора для СУ...*, в появившемся окне (Рис. 49) нажимаем кнопки *Все* и *Отправить*, изменяем дату обновления на «заднее число» и нажимаем кнопку *Принять*, а потом *Выйти.*

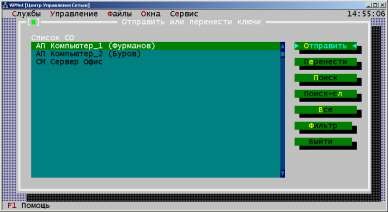


Рис. 49 Список КН для отправки

Теперь отправим адресные справочники. Выбираем пункт меню *Управление  Отправить измененные файлы  Справочники АП и СМ...*, в появившемся окне нажимаем кнопки *Все* и *Отправить*, изменяем дату обновления на «заднее число» и нажимаем кнопку *Принять*, а потом *Выйти.* Выходим из ЦУСа.

Шаг 27

*Проверка правильности выполненной процедуры установления межсетевого взаимодействия*

Загружаем Монитор сети № 6670 и перенастраиваем транспортный модуль MFTP на работу по одноименному каналу.

После перенастройки транспортного модуля проведем обновление АП Компьютер\_1 (Фурманов), как и в Лабораторной работе № 2.

После перезагрузки Монитора **не должно быть «ругательных»**

**сообщений** типа «...не найдены ключи для таких-то сетевых узлов..», а в меню *Защищенная сеть* появятся новые фильтры для СУ сети № 6671 (Рис. 50).

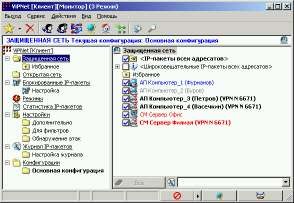


Рис. 50 Окно Монитора после проведенного обновления

Отсутствие ругани и правильный набор фильтров в меню *Защищенная сеть* - показатель того, что Вы все сделали правильно. Закройте Монитор АП Компьютер\_1 (Фурманов) и повторите этот шаг для АП Компьютер\_3

(Петров).

По завершению всех вышеописанных шагов, между двумя защищенными сетями будет установлено межсетевое взаимодействие и теперь данные между сетями будут передаваться в защищенном виде, экспорт можно будет формировать и отсылать в другую сеть по защищенному каналу передачи данных (в ЦУСе меню *Управление  Отправить измененные файлы  Экспорт...*, выбираем экспорт в нужную сеть и нажимаем кнопку *Отправить*).

Итак, на простом примере, мы разобрали установление межсетевого взаимодействия двух VPN-сетей.

### 4 Содержание отчета

Отчет должен содержать:

* 1. Формулировку цели работы;
  2. Описание сценария лабораторной работы;
  3. Выводы о проделанной работе.

### Вопросы к лабораторной работе №4

1. Требуется ли при связывании двух защищенных сетей заново генерировать основной мастер ключ?
2. Требуется ли генерация симметричного индивидуального ключа при связывании двух защищенных сетей асимметричным ключем?
3. Зачем необходимо назначение шлюза в защищенной сети ?
4. Что должен сделать администратор при смене асимметричного мастер - ключа?
5. Какого типа может быть межсетевой мастер-ключ?
6. Где хранится ассимметричный Мастер Ключ?
7. Для чего необходим экспорт ЭЦП главного абонента при установлении межсетевого взаимодействия?

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

#### Цель работы

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

#### 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.);
  1. 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 СОМ 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;
  1. 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;

* 1. 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 СОМ интерфейс для вызова криптофункций и их совместного использования

с Web приложениями.

#### 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 ко торым анализируется трафик.

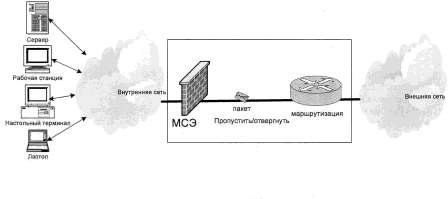


Рисунок 3.1 – Межсетевой экран

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).

* 1. 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.

* 1. 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:

* cистема 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).

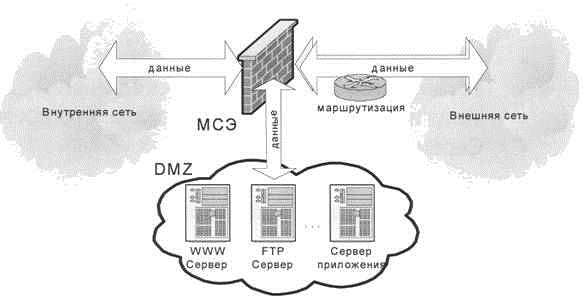


Рисунок 3.2 – Демилитаризованная зона (ДМЗ)

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

#### 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].

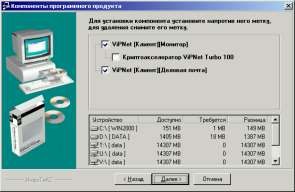


Рисунок 4.1 – Выбор типа установки

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***.**

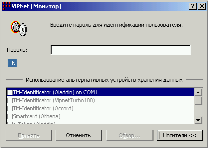


Рисунок 4.2 – Окно ввода пароля

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).

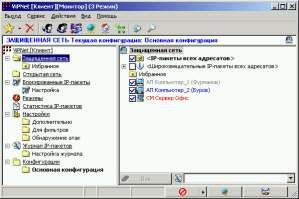


Рисунок 4.3 – Окно программы Монитор

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.

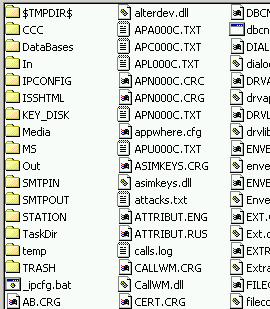


Рисунок 4.4 – Структура каталога установки.

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 . Поработать в каждом из режимов (Рисунок 4.5), понять, чем они отличаются и разобраться в возможностях, предоставляемых каждым режимом.

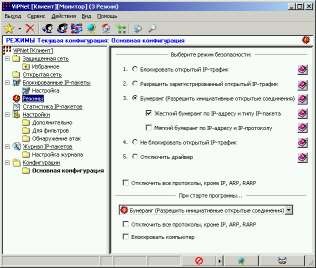


Рисунок 4.5 – Режимы безопасности

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.

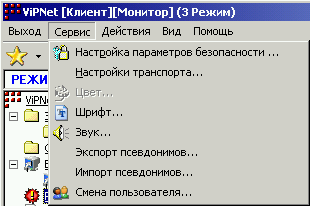


Рисунок 4.6 – Меню *Сервис*

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)*.*

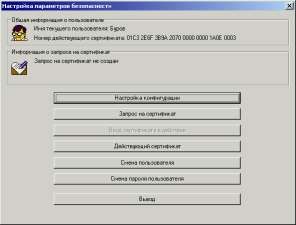


Рисунок 4.7 – Настройка параметров безопасности

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.

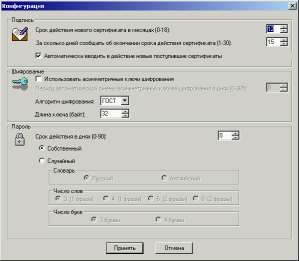


Рисунок 4.8 – Окно *Конфигурация*

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).

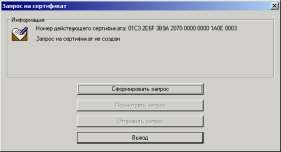


Рисунок 4.9 – Работа с подписью

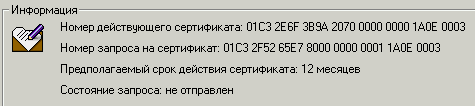


Рисунок 4.10 – Поле Информация

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

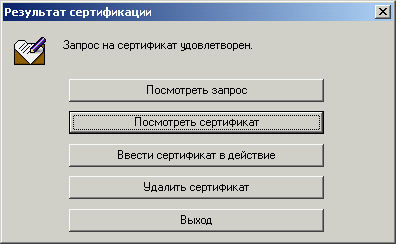


Рисунок 4.11 – Результат сертификации

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

.сертификат или удалить его.

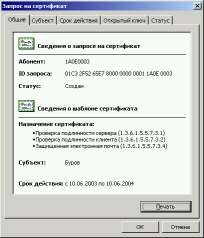


Рисунок 4.11 – ОЧ новой подписи

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.

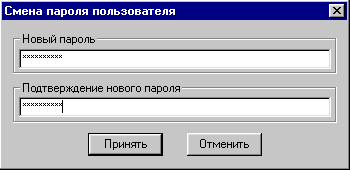


Рисунок 4.12 – Смена собственного пароля

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).

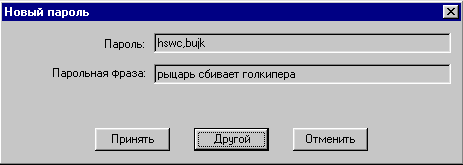


Рисунок 4.13 Пароль и парольная фраза

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).

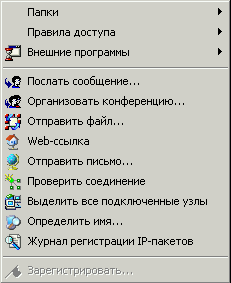


Рисунок 4.14 – Сервисное меню



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).

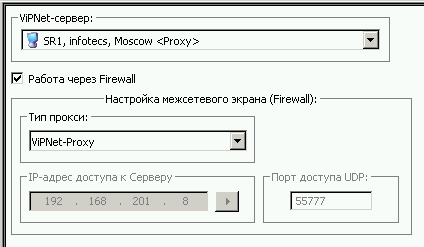


Рисунок 4.16 – Настройки АП

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*).

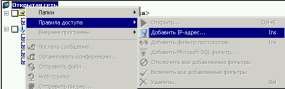


Рисунок 4.17 – Добавление адреса в открытой сети

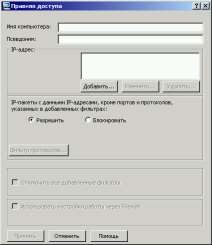


Рисунок 4.18 – Настройка фильтра

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.

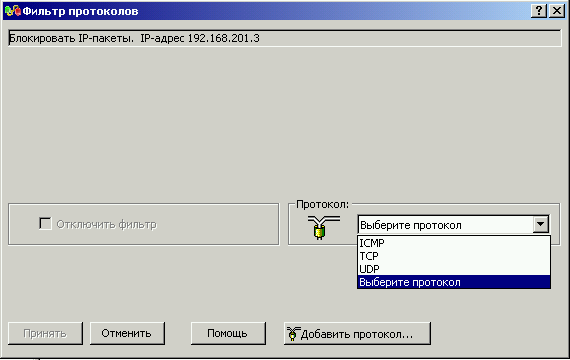


Рисунок 4.19 – Добавление фильтра

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

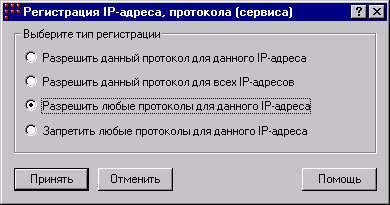


Рисунок 4.21 – Регистрация блокированного пакета

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.

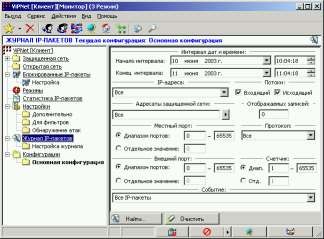


Рисунок 4.22 – Журнал IP-пакетов

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.*

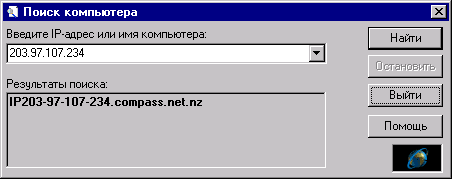


Рисунок 4.23 – Поиск компьютера

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.).

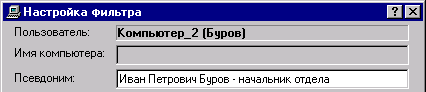
Псевдонимы задаются локально на каждом СУ, для этого выберите СУ в списке *Защищенная сеть* и два раза кликнете на нем левой клавишей мыши (или по правой клавише мыши выберите пункт *Изменить*). В появившемся

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: @@@@@xхххxxххх, где ххххххххх – 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).

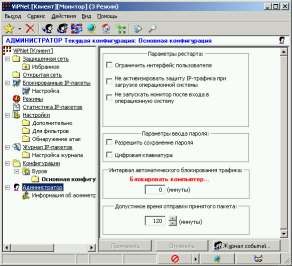


Рисунок 4.25 – Окно *Администратор*

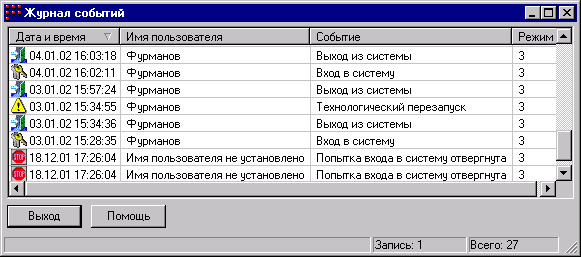


Рисунок 4.26 – Журнал событий

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).

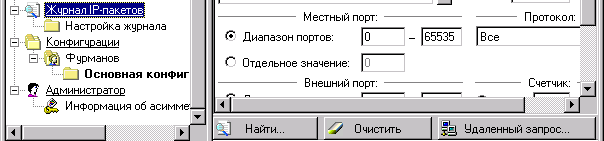


Рисунок 4.27 – Журнал IP-пакетов в режиме администратора

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.

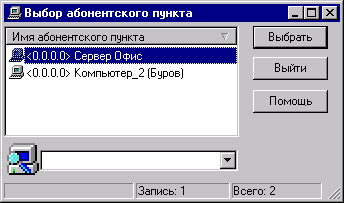


Рисунок 4.28 – Выбор АП для удаленного запроса журнала

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).

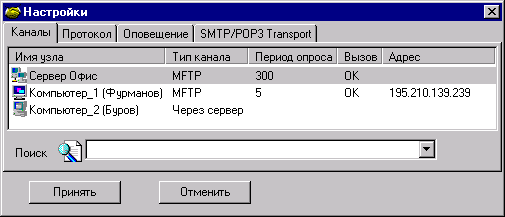


Рисунок 4.29 – Окно *Настройки*

По умолчанию, все АП работают через свой СМ для обеспечения

гарантированной доставки передаваемой информации.

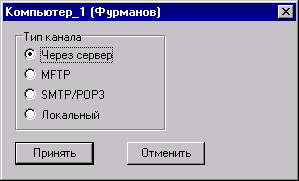


Рисунок 4.30 – Выбор типа канала

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.

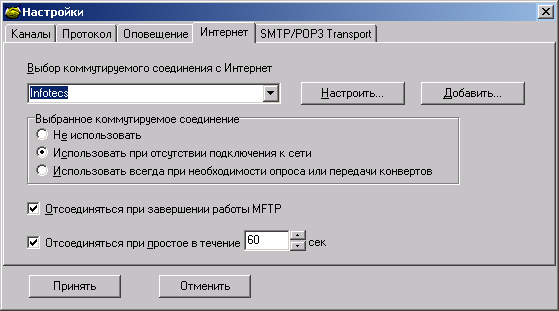


Рисунок 4.31 – Настройка вкладки *Интернет*

**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).

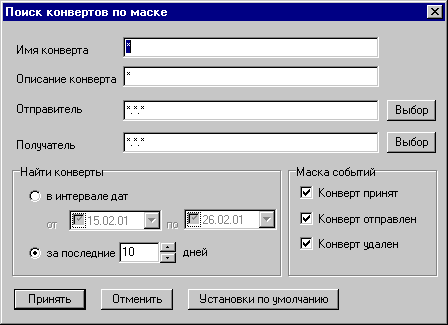


Рисунок 4.32 – Настройка журнала

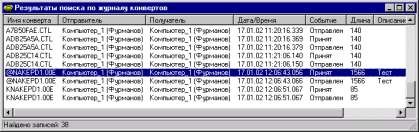


Рисунок 4.33 – Журнал MFTP

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.

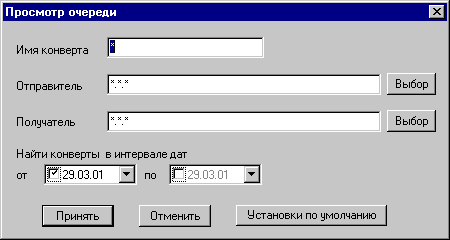


Рисунок 4.34 – Настройка очереди

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) добавьте вложение  (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

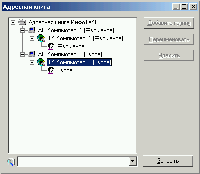


Рисунок 4.36 – Адресная книга

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).

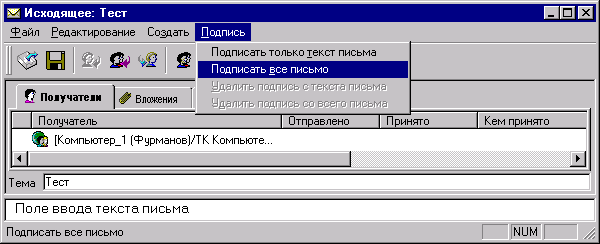


Рисунок 4.37 – Меню *Подпись*

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

Шаг 22(28)

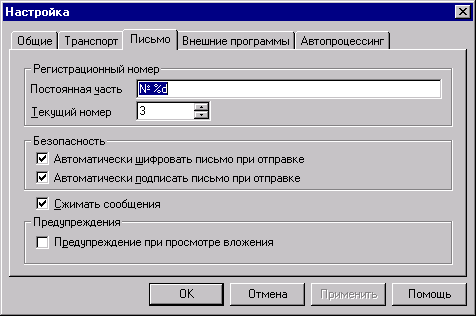
*Использование прикладного шифрования писем*

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.

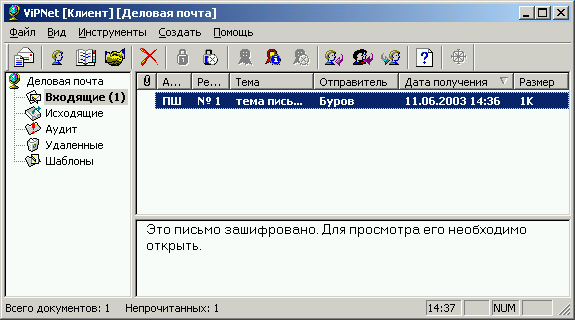


Рисунок 4.39 – Основное окно ДП

**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).

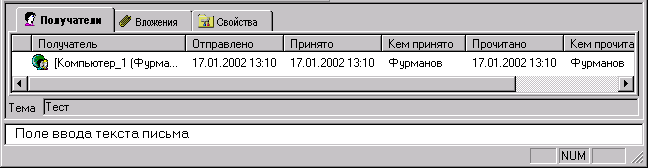


Рисунок 4.40 – Вкладка *Получатели*

Шаг 25(28)

*Запуск внешних программ в ДП*

Запуск внешних программ настраивается на вкладке *Внешние программы*

в меню ДП *Инструменты  Настройка*... (Рисунок 4.41).

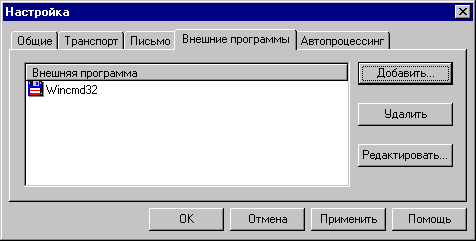


Рисунок 4.41 – *Внешние программы*

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.

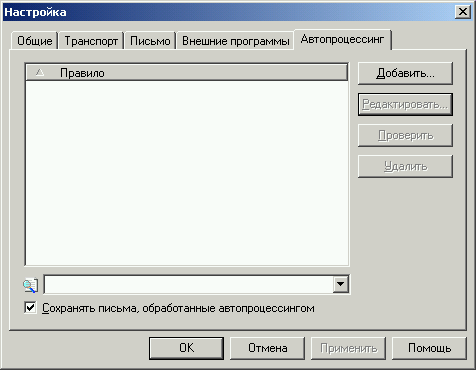


Рисунок 4.42 – Настройка автопроцессинга

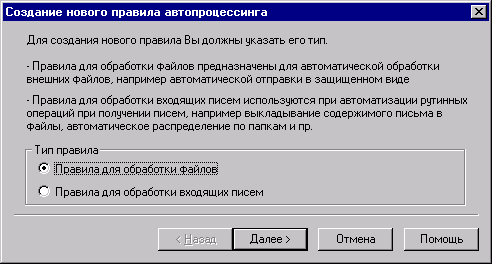


Рисунок 4.43 – Окно выбора правил

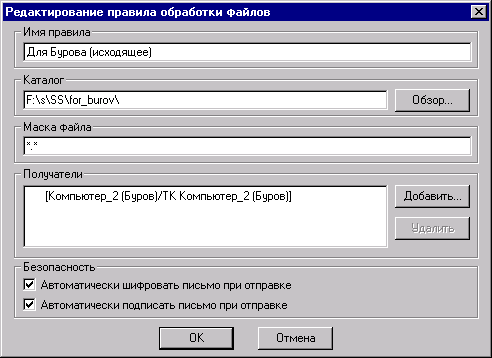


Рисунок 4.44 – Настройка исходящего правила

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.

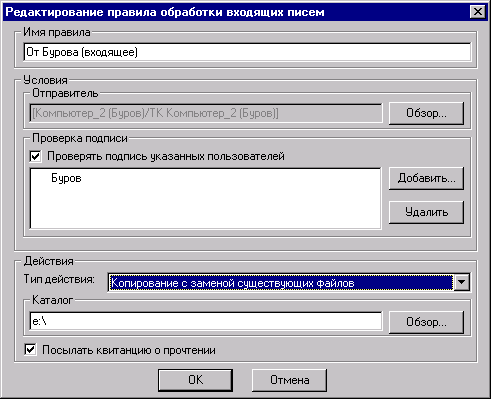


Рисунок 4.45 – Настройка входящего правила

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.

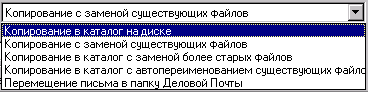


Рисунок 4.46 – Возможные типы действий

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 к лабораторной работе №5

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 CУ 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?