Защита информации, Межсетевые экраны, VPN-построители

АМИКОН

WWW.AMICON.RU

г. Москва, Варшавское шоссе, д. 125, стр. 1, тел.: 797-6412, 797-6413
E-mail: info@amicon.ru

Программно-аппаратный комплекс ФПСУ-IP

ФПСУ-IP: Фильтр Пакетов Сетевого Уровня IP протокола

Средство криптографической защиты информации от несанкционированного доступа

VPN-построитель и межсетевой экран с централизованным управлением для распределенных сетей

Программа лекции

- - Введение
- - Общие сведения о комплексе «ФПСУ-IP»
- - Обзор лабораторной работы

- Комплект учебных материалов:
  - Практикум по ПАК «ФПСУ-IP»
  - Документация

ООО «АМИКОН». Немного истории

- · 1994-1995 годы – первый отечественный проходной шифратор X.25
- · 1997 год – ФПСУ-X.25
- · 1998 год – ФПСУ-IP
- · 2002 год – ФПСУ-IP/Клиент
- · 2005 год – ФПСУ-IP – 2
- · 2009 год – ФПСУ-IP – 2.50
- · 2014 год – ФПСУ-IP – 3

- На настоящий момент комплексы эксплуатируются в крупнейших информационных системах таких организаций как: Банк России, «Сбербанк России», «ЛУКОЙЛ», «Альфа-Банк» и в ряде других
- Общее количество внедрений – более 430 000 комплексов «ФПСУ-IP/Клиент» и «ФПСУ-IP»

Состав программно-аппаратного комплекса «ФПСУ-IP»

- Программно-аппаратный комплекс межсетевой экран «ФПСУ-IP»

  VPN-построитель и основной компонент

- Программно-аппаратный комплекс «ФПСУ-IP/Клиент»

  VPN-клиент для мобильных пользователей

- Программно-аппаратный комплекс «Удаленный администратор ФПСУ-IP»

  средство централизованного управления группой межсетевых экранов «ФПСУ-IP» и «ФПСУ-IP/Клиентов»

Состав программно-аппаратного комплекса «ФПСУ-IP»

Управление ключевой информацией

- Специальное программное обеспечение «Центр выработки ключей»

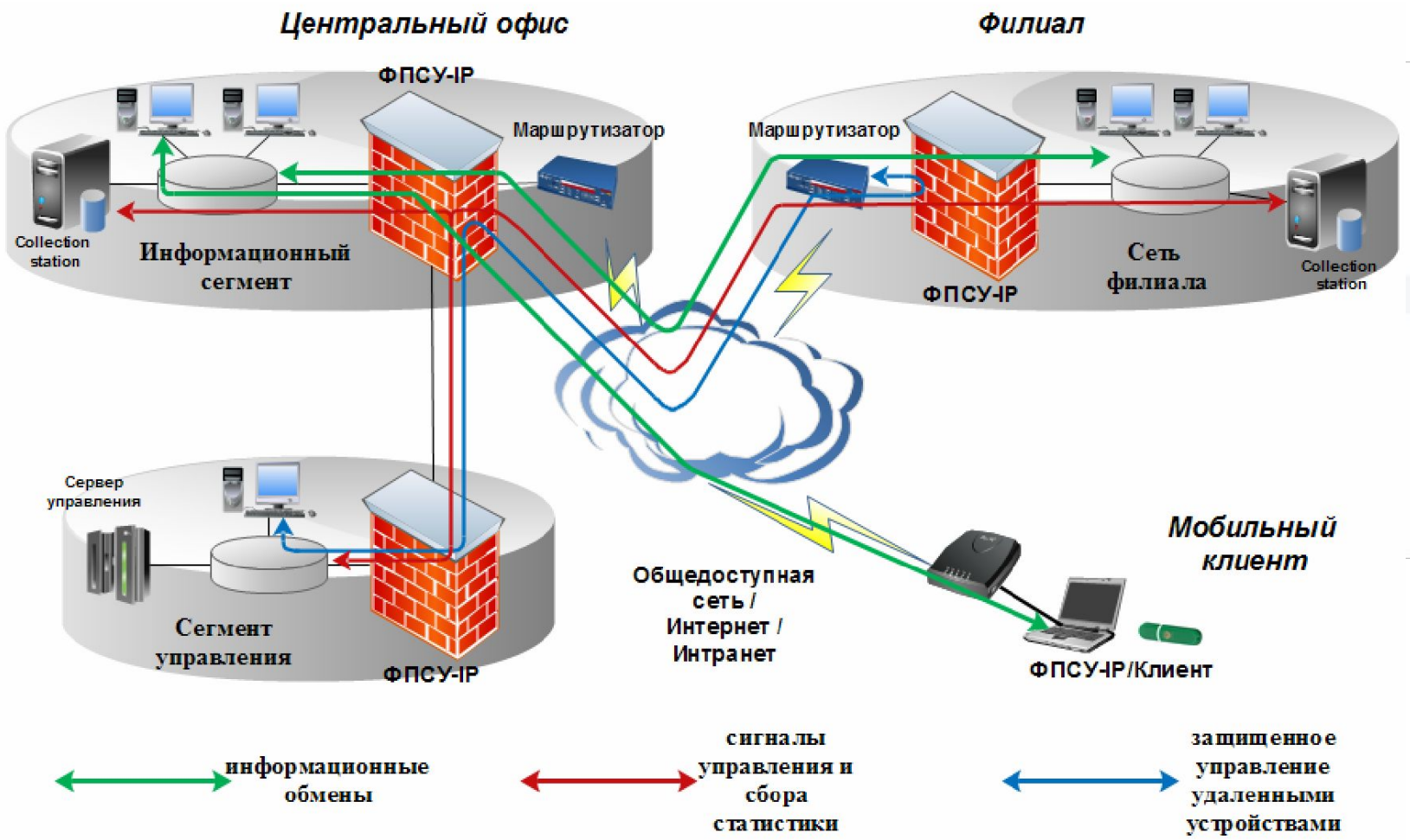
  создание криптографических ключей для взаимной двусторонней идентификации и аутентификации между межсетевыми экранами «ФПСУ-IP» и построения VPN-соединений поверх глобальных сетей

- Специальное программное обеспечение «Центр генерации ключей Клиентов»

  создание криптографических ключей для

  - *аутентификации и идентификации между «ФПСУ-IP/Клиентами» и межсетевыми экранами «ФПСУ-IP»*
  - *построения защищенного VPN-соединения между рабочей станцией и межсетевым экраном «ФПСУ-IP»*

Общая схема применения



Основной компонент: ПАК МЭ ФПСУ-IP

- Межсетевой экран программно-аппаратного комплекса «ФПСУ-IP» является программно-аппаратным средством защиты от несанкционированного доступа к информации.
- МЭ позволяет выделять в открытой сети защищенные области с ограниченным доступом, а также обеспечивать защищенную передачу данных между защищенными областями.
- МЭ «ФПСУ-IP» работает по стеку протоколов TCP/IP и использует формат фрейма Ethernet II

Основные функции ПАК МЭ ФПСУ-IP

- ***VPN-построитель: установка защищенных туннелей с другими ПАК МЭ «ФПСУ-IP»*** для организации безопасной передачи данных через сети, которым нет доверия (До 1024 туннелей)
- ***VPN-шлюз:*** установка защищенных туннелей с клиентской частью комплекса – ПАК ФПСУ-IP/Клиент (до 128 000 клиентов)
- ***Межсетевой экран:*** фильтрация передаваемых данных на сетевом, транспортном (и, выборочно, на сеансовом и прикладном) уровня (с регистрацией результатов фильтрации)

Аппаратные платформы ПАК МЭ «ФПСУ-IP»

На 2014 год существует пять основных вариантов исполнения ПАК «ФПСУ-IP», отличающихся аппаратными платформами и производительностью при включенном режиме шифрования

- ПА  СУ-IP» STD – **2U платформа, 130 Мбит/с**
- ПА  СУ-IP» EXT – **2U платформа, до 750 Мбит/с**
- П  У-IP» SRV – **1U платформа, до 800 Мбит/с**
- П  У-IP» ULT – **1U платформа, до 3 Гб/с**
- ПА  СУ-IP» MINI – **компактный корпус, до 10 Мбит/с**

Краткая спецификация ПАК ФПСУ-IP	
Производитель	ООО АМИКОН
Сертификаты	Сертификаты ФСТЭК, Сертификаты ФСБ России на применяемое СКЗИ "Туннель 2.0"
Соответствие требованиям федерального закона №152-ФЗ «О персональных данных»	Может применяться в ИСПДн класса К1
ОС / стек протоколов	На базе LINUX / собственный
Количество интерфейсов и тип	2; 100/1000/10G Ethernet (UTP, Optic), 3-й интерфейс для комплексов по схеме "горячий резерв"
Алгоритм шифрования	ГОСТ 28147-89
VPN-протокол / избыточность	Собственный / не более 26 байт на пакет
Ключевая система / распределение ключей	Симметричная / централизованное
Обрабатываемые уровни ЭМВОС	Сетевой, транспортный. Выборочно – сеансовый и прикладной
Управление и мониторинг	Локальное и удаленное, с механизмами "отката" при сбоях. До 2048 комплексов на один АРМ удаленного администрирования. Поддержка SNMP-протокола и Syslog

Краткая спецификация ПАК ФПСУ-IP	
Протокол удаленного управления	Собственный туннельный протокол со строгой двухсторонней аутентификацией согласно X.509
Собственная безопасность	Полный аудит событий и действий персонала, разграничение доступа с помощью iButton и USB-Key
Дополнительные защитные функции	Сокрытие топологии, NAT, сокрытие факта присутствия комплекса, VPN-проксирование протоколов управления
Дополнительные сетевые функции	ARP-proxy, VLAN 802.1q, пропуск MPLS-фреймов, сохранение поля TOS в туннельном заголовке
Удаленный клиент	Для Windows XP, XP Embedded, Vista, 7, 2003 Server, 2008 Server, Linux, MacOS
Производительность "ФПСУ-IP" ("ФПСУ-IP/Клиент") при включенном режиме шифрования	До 3 (0,25) Гб/сек
Число абонентов/подсетей на порту	До 8000
Число VPN-туннелей с ФПСУ	До 1024
Число поддерживаемых «ФПСУ-IP/Клиент»	До 128000

Легитимность применения

- ПАК «ФПСУ-IP» является сертифицированным ФСБ средством криптографической защиты информации «Туннель 2.0», что позволяет осуществлять шифрование передаваемой информации в соответствии с ГОСТ 28147-89.
- СКЗИ «Туннель 2.0» (разработано ООО Фирма «ИнфоКрипт») имеет сертификат ФСБ соответствия уровням КС1 и КС2

Легитимность применения

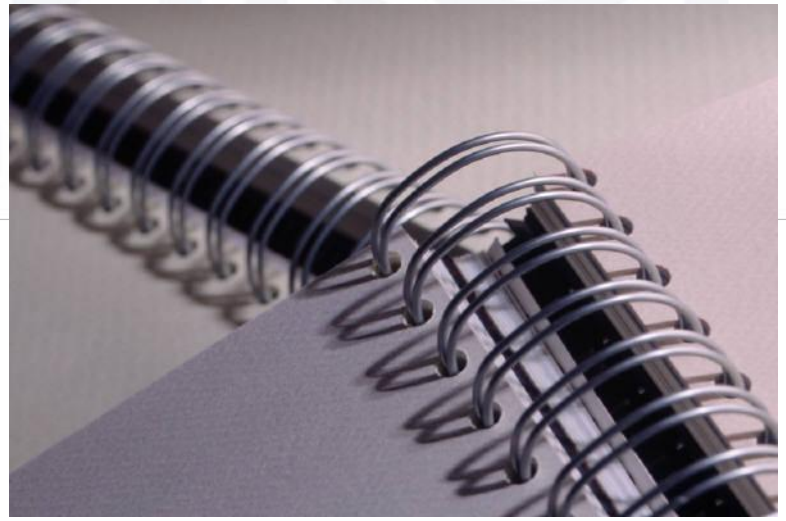
- ПАК «ФПСУ-IP» может применяться для защиты информации:
  - не составляющей государственную тайну
  - в автоматизированных системах до класса защищенности 1Г включительно (Гостехкомиссия)
  - в информационных система персональных данных (ИСПДн) до 1 класса включительно (в соответствии с требованиями федерального закона №152-ФЗ «О персональных данных»)

Легитимность применения

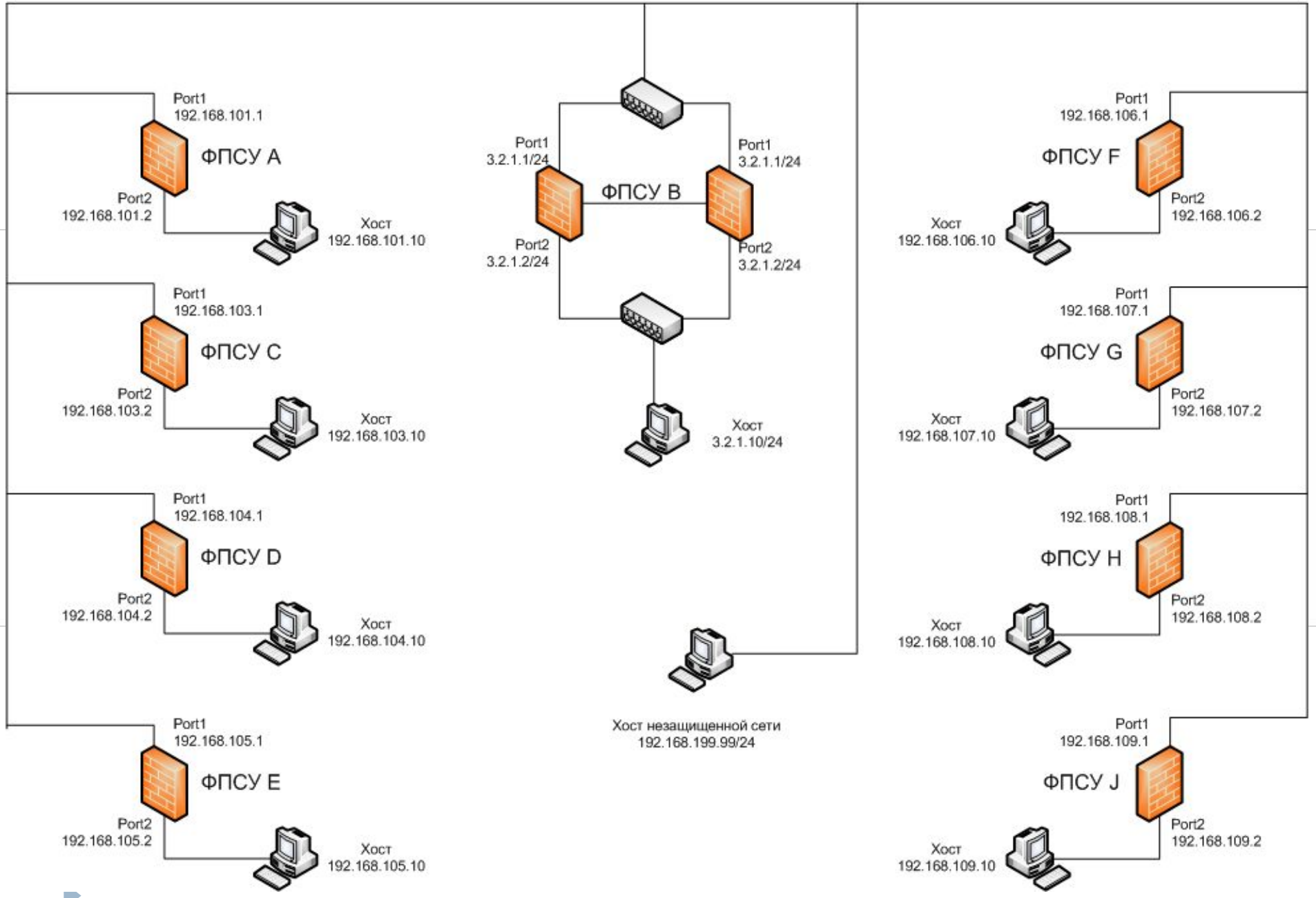
- ПАК МЭ ФПСУ-IP имеет сертификат Мининформсвязи России на соответствие "Правилам применения оборудования коммутации и маршрутизации пакетов информации" при условиях применения на сети связи общего пользования в качестве оборудования коммутации и маршрутизации пакетов информации сетей передачи данных

Задания практикума ФПСУ-IP

- 1. Настройка работы межсетевого экрана ПАК ФПСУ-IP
- 2. Настройка работы VPN-построителя ПАК ФПСУ-IP

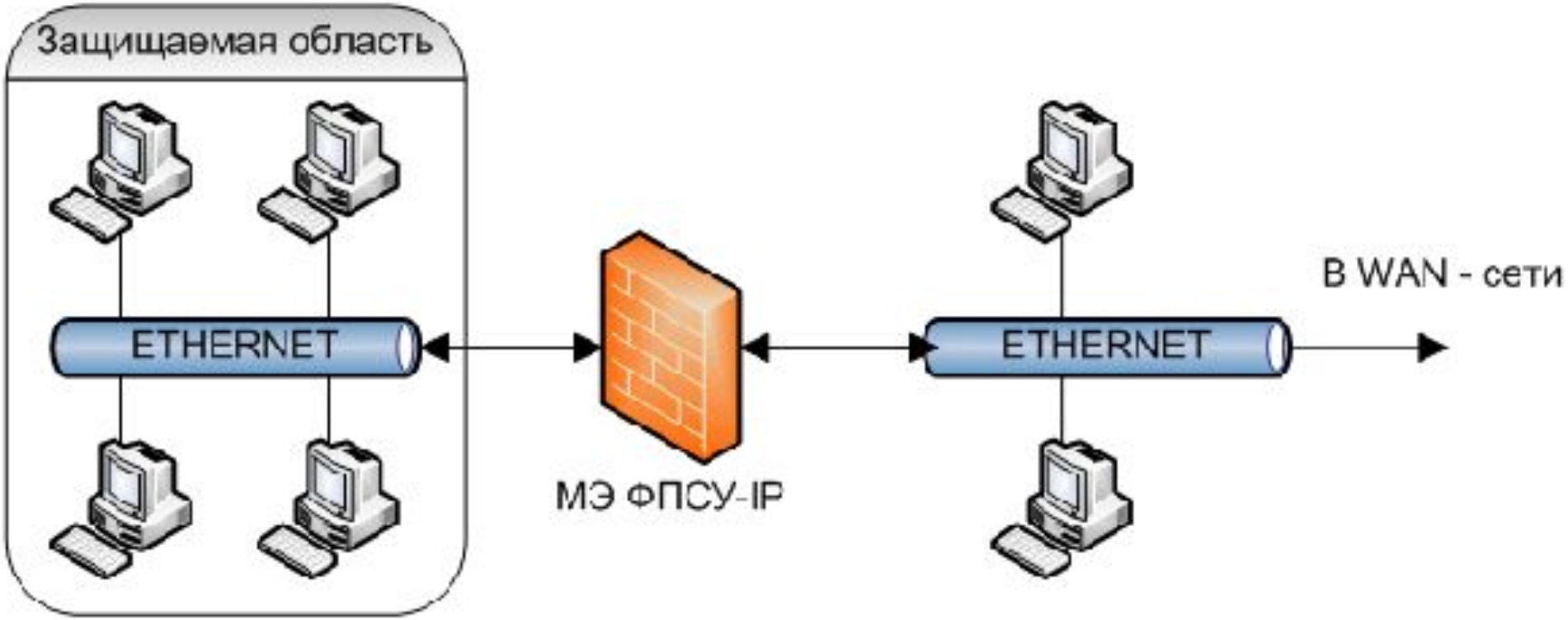


T-205 Схема лабораторной сети ФПСУ-IP



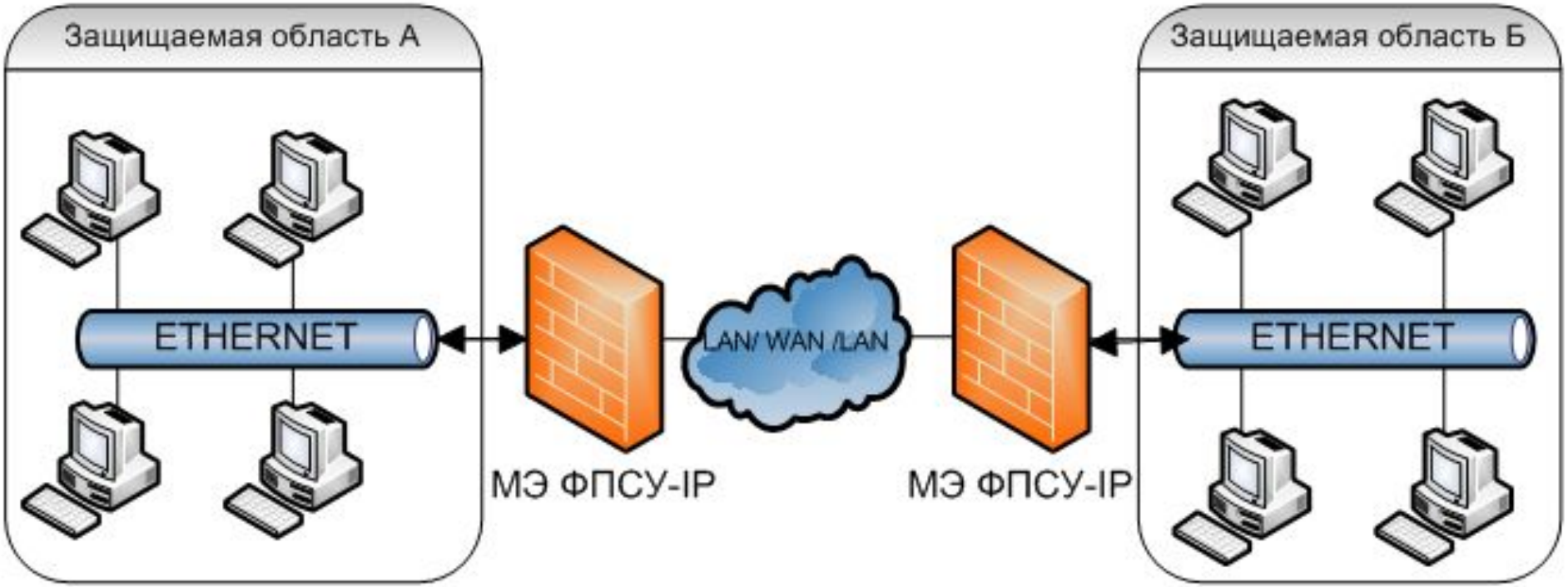
Задания практикума

- Обзор первого задания. Основная задача – научиться конфигурировать маршрутизацию и межсетевой экран «ФПСУ-IP»



Задания практикума

- Обзор второго задания. Основная задача – научиться работать с ключевой информацией и настраивать VPN-соединения между «ФПСУ-IP»



Основные принципы работы с ФПСУ-IP

- Интерфейс
- Аутентификация
- Конфигурирование
- Тестирование конфигурации
- Поиск ошибок

Операционная система ПАК МЭ «ФПСУ-IP»

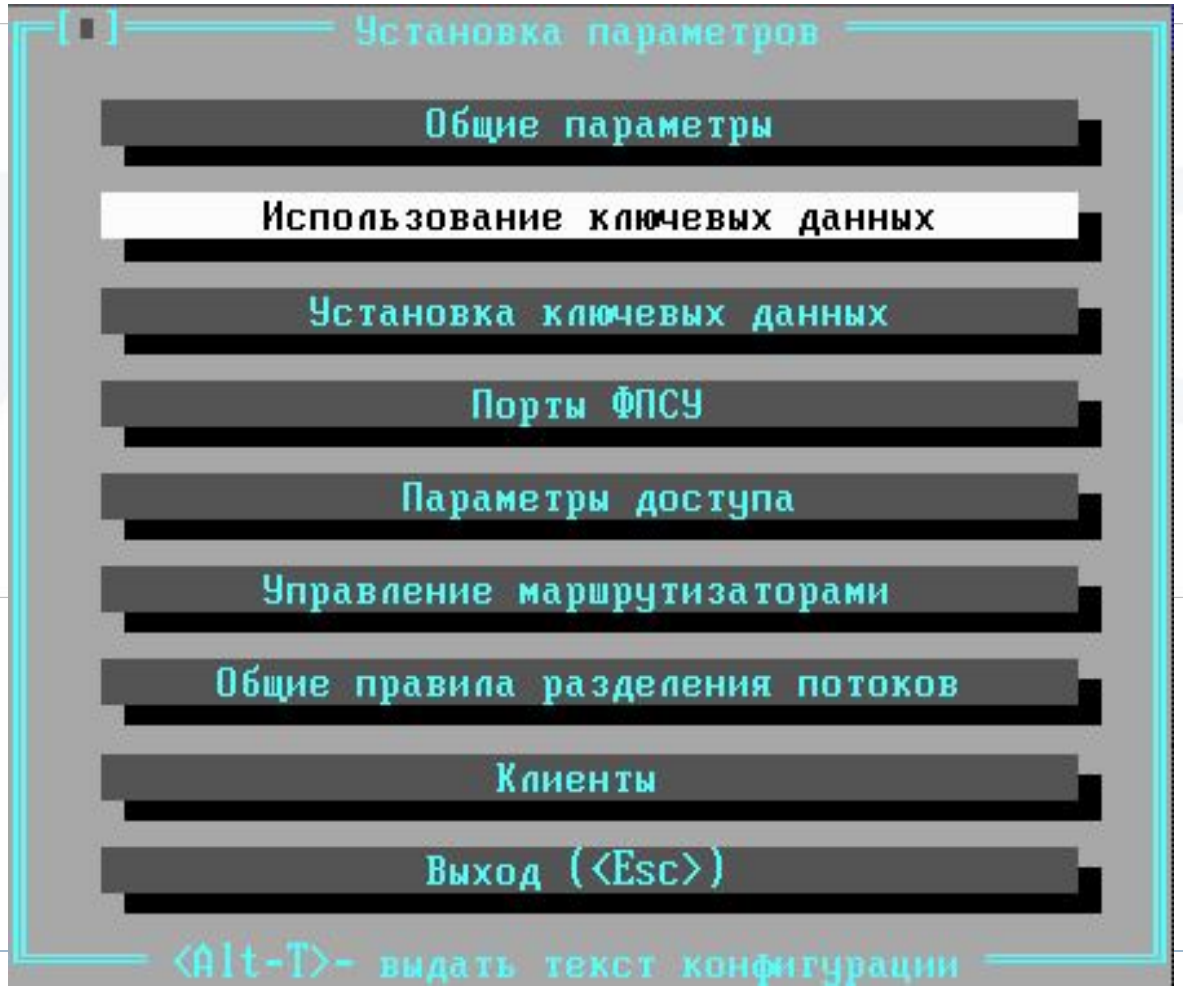
- Функционирование межсетевого экрана происходит под управлением собственной (основанной на Linux), изолированной и функционально замкнутой операционной системой
- Графическая среда при локальном управлении – псевдографика

Идентификация, аутентификация и аудит действия локального администратора

- Любое действие локального администратора на просмотр или изменение конфигурационных настроек МЭ ФПСУ-IP требует обязательной аутентификации с помощью аппаратного ключа, контактной памяти (touch-memory iButton) с данными администратора

Конфигурация ФПСУ-IP

- Принцип белого листа – все что явно не разрешено, то запрещено



Порты ФПСУ

- **Здесь задаются основные правил фильтрации абонентского трафика и способ передачи данных через МЭ “ФПСУ-IP”.**
- **Для каждого рабочего порта МЭ необходимо создать**
  - **список абонентов, которым разрешается подключаться к МЭ со стороны этого порта,**
  - **указать смежные МЭ “ФПСУ-IP”**
  - **указать маршрутизаторы, через которые абоненты будут доступны**
  - **установить правила их работы.**

Порты ФПСУ

N	Адрес порта	Маска подсети	Абонентов	Gateway	ФПСУ
1	190.007.000.044	255.255.000.000	1	1	0
2	190.007.000.044	255.255.000.000	5	1	1

Взаимные идентификация и аутентификация МЭ «ФПСУ-IP»

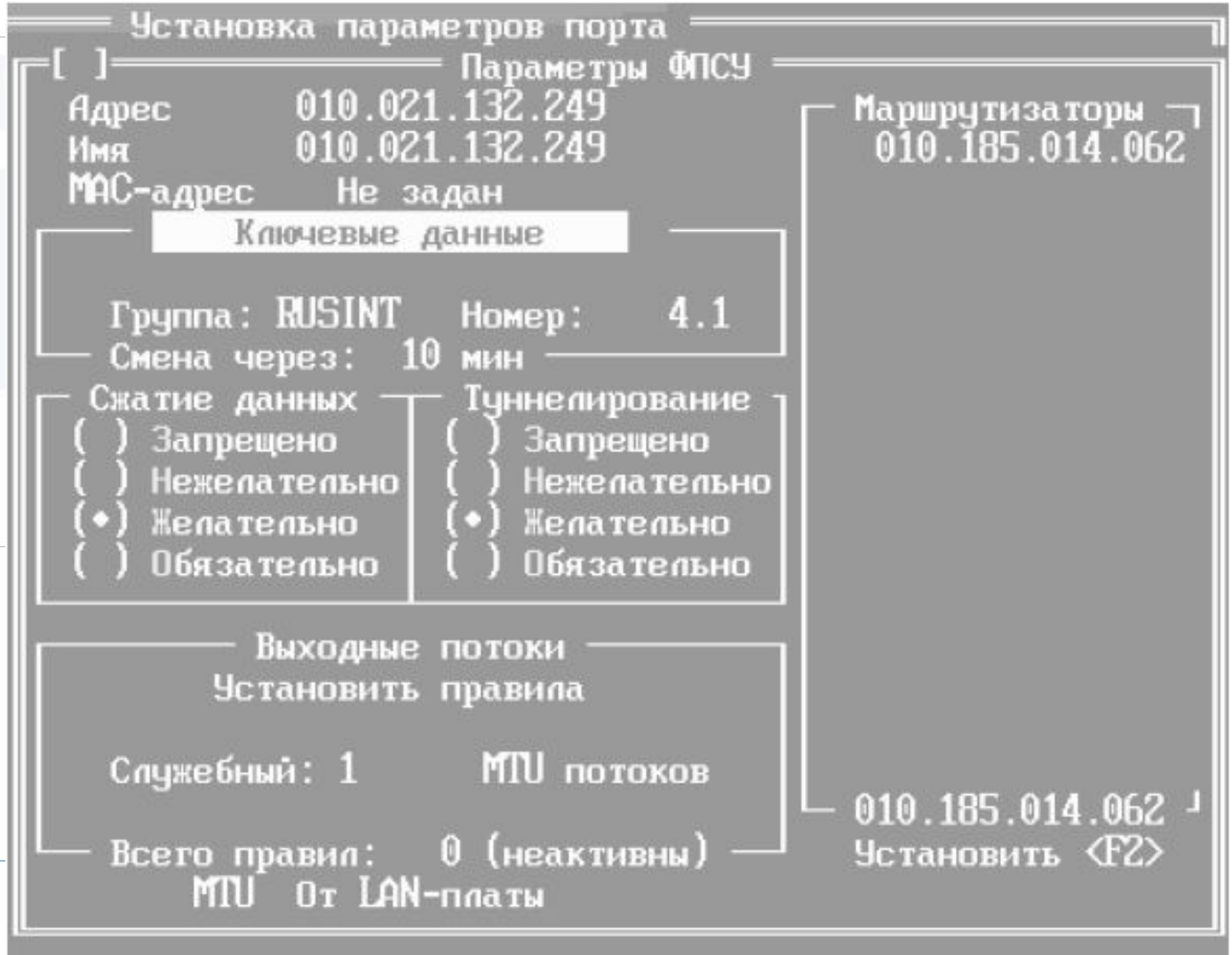
- **Шифрование данных** производится на **сеансовых ключах**
- **аутентификация МЭ** - на **долговременных ключах** парно-выборочной связи.

- **Схема двусторонней аутентификации МЭ “ФПСУ-IP”, работающих в паре и создающих VPN-туннель для передачи IP-пакетов, обеспечивает устойчивость передаваемых данных к пассивному и активному перехвату информации.**

Описание соседних ФПСУ-IP

- В поле ***ФПСУ*** необходимо описать все удалённые МЭ “ФПСУ-IP”, которые будут участвовать в создании VPN-туннелей передачи данных между защищаемыми ими абонентами (сетями) и абонентами конфигурируемого МЭ “ФПСУ-IP”.
- Создать описатель удаленного МЭ “ФПСУ-IP” возможно только в том случае, если соответствующие ключи, полученные от “Центра выработки ключей”, установлены на жёсткий диск и указаны к использованию

Описание соседних ФПСУ-IP

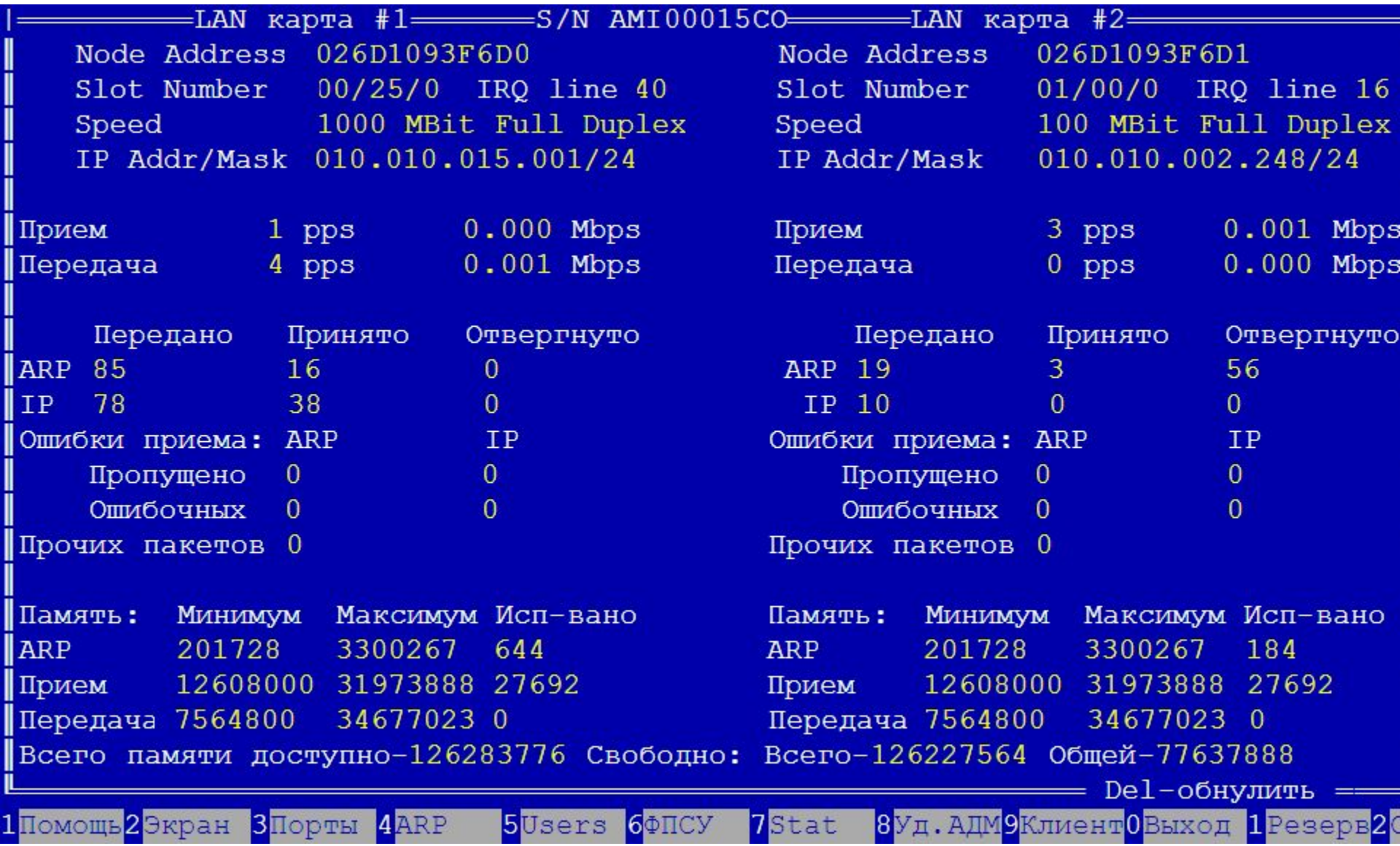


Режимы сжатия и шифрования

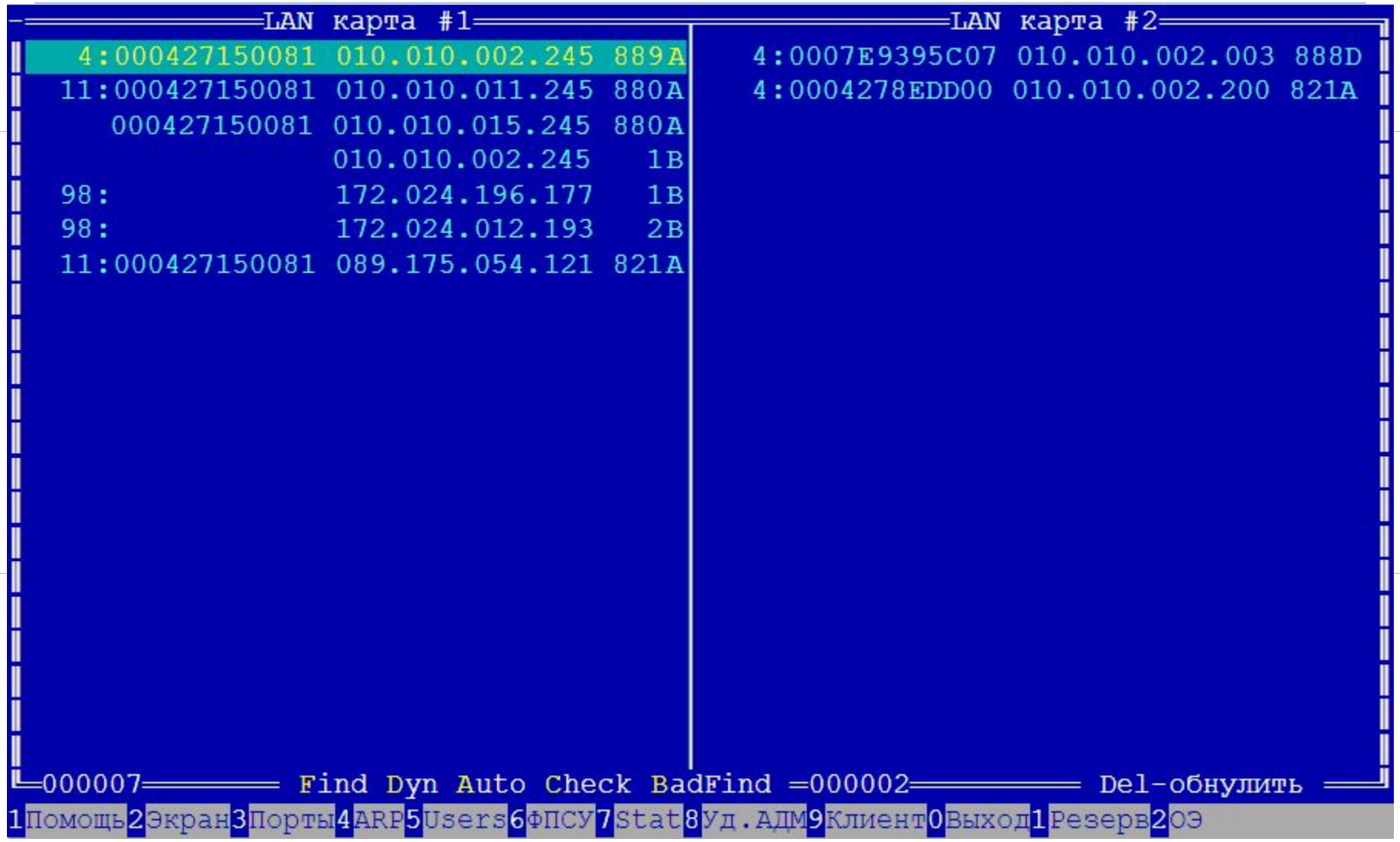
- **Ответственность** за согласование конфигураций двух МЭ “ФПСУ-IP”, через которые осуществляется соединение абонентов, и за соответствие установленных на них режимов **несёт администратор.**

Установленный режим на данном МЭ “ФПСУ-IP”	Установленный режим на удалённом МЭ “ФПСУ-IP”			
	ЗАПРЕЩЕНО	*НЕЖЕЛАТЕЛЬНО*	*ЖЕЛАТЕЛЬНО*	*ОБЯЗАТЕЛЬНО*
ЗАПРЕЩЕНО	не используется	не используется	не используется	соединение не состоится
НЕЖЕЛАТЕЛЬНО	не используется	не используется	используется	используется
ЖЕЛАТЕЛЬНО	не используется	используется	используется	используется
ОБЯЗАТЕЛЬНО	соединение не состоится	используется	используется	используется

Отслеживание ошибок 1: LAN-адаптеры



Отслеживание ошибок 2: ARP



Отслеживание ошибок 3: VPN-туннели

Отслеживание ошибок 4: передачи данных абонентов

Спасибо за внимание!

Вопросы?

Волченков Павел
ООО «АМИКОН»
контакты:
www.amicon.ru
mail to: vpv@amicon.ru