

Подготовка к работе ИС «ЭФРОС-РІХ»

ИС «ЭФРОС-РІХ» функционирует под управлением ОС Microsoft Windows 2000/XP и при инсталляции должна устанавливаться в папку, находящуюся в корневом каталоге любого логического диска.

Для подготовки к работе ИС «ЭФРОС-РІХ» необходимо выполнить следующие действия:

1. Выполнить процедуру инсталляции ИС «ЭФРОС-РІХ».
2. Сформировать базу данных команд Cisco Ріх.
3. Сформировать файлы настроек.

Подготовка к работе ИС «ЭФРОС-РІХ»

Формирование базы данных команд Cisco Pih

База данных команд Cisco Pih в ИС «ЭФРОС-РІХ» реализована в виде совокупности файлов, содержащих варианты цепочек команд режима интерпретатора команд ОС Cisco Pih с указанием номера уровня привилегий команды.

Имя файла в БД совпадает с именем режима интерпретатора команд ОС Cisco Pih.

Подготовка к работе ИС «ЭФРОС-PIХ»

Формирование базы данных команд Cisco Pix

Пример записей файла режима aaa-user БД ИС «ЭФРОС-PIХ»:

```
1 exit
15 group-lock none
15 group-lock value WORD
15 password-storage disable
15 password-storage enable
15 vpn-access-hours none
15 vpn-access-hours value WORD
15 vpn-filter none
15 vpn-filter value WORD
15 vpn-framed-ip-address A.B.C.D A.B.C.D
15 vpn-group-policy WORD
15 vpn-idle-timeout <1-35791394>
15 vpn-idle-timeout none
15 vpn-session-timeout <1-35791394>
15 vpn-session-timeout none
15 vpn-simultaneous-logins <0-2147483647>
15 vpn-tunnel-protocol
```

Подготовка к работе ИС «ЭФРОС-PIХ»

Формирование базы данных команд Cisco Pix

База данных хранится в файлах ***Routers\<Имя МСЭ>\Modes*** и ***Routers\<ИмяМСЭ>\Comments***. Первоначально в ИС «ЭФРОС-PIХ» входит демонстрационная база, которая размещается в файлах ***Routers\Demo\Modes*** и ***Routers\Demo\Comments***

Содержимое файлов, в основном, совпадает, различие в форматах записей файлов — в файлах ***Comments*** хранятся цепочки команд вместе комментариями, которые формирует справочная служба Cisco Pix. Они же используются в справочной подсистеме ИС «ЭФРОС-PIХ».

Для создания базы данных команд Cisco Pix для ИС «ЭФРОС-PIХ» необходимо выполнить следующие действия:

1. В каталоге ***Routers*** создать файлы ***\<Имя МСЭ>\Modes*** и ***<Имя МСЭ>\Comments***.
2. Сформировать файлы режимов команд Cisco Pix.
3. Поместить файлы в ***Routers\<Имя МСЭ>\Modes*** и ***<Имя МСЭ>\Comments***.

Формирование файлов режимов команд Cisco Pix осуществляется с использованием сканера команд «ЭФРОС-сканер», входящего в состав комплекса.

Подготовка к работе ИС «ЭФРОС-РІХ»

Формирование файлов настроек

Перед запуском ИС «ЭФРОС-РІХ» необходимо сформировать файлы настроек и поместить их в каталог **Routers\<Имя МСЭ>**

Сформировать список режимов команд ОС Cisco Pix и установленных для них уровней привилегий по умолчанию — файл настроек **ParserModes.ini**. Для формирования файла необходимо на МСЭ выполнить команду **Show running-config all privilege all** и результаты ее поместить в файл **ParserModes.ini**

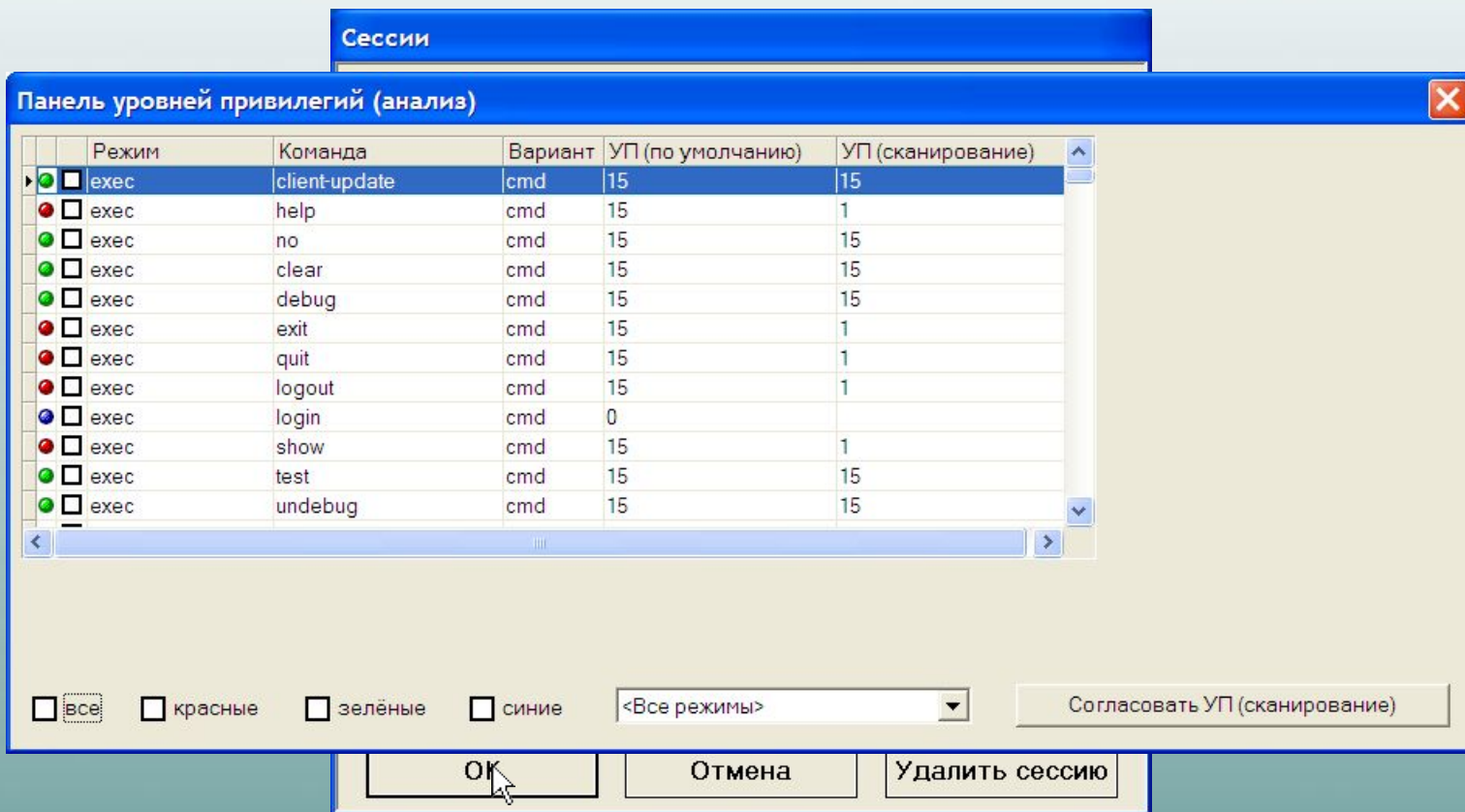
Анализ состава и уровней привилегий команд Cisco Pix

При анализе состава команд и уровней их привилегий по умолчанию в Cisco Pix необходимо выполнить следующие шаги:

- создание новой сессии в режиме анализа;
- формирование отчета по результатам анализа;
- корректировка (при необходимости) базы данных команд, полученной с использованием сканера команд.

Анализ состава и уровней привилегий команд Cisco Pix

Создание новой сессии в режиме анализа



Режим	Команда	Вариант	УП (по умолчанию)	УП (сканирование)
<input checked="" type="checkbox"/>	client-update	cmd	15	15
<input type="checkbox"/>	help	cmd	15	1
<input type="checkbox"/>	no	cmd	15	15
<input type="checkbox"/>	clear	cmd	15	15
<input type="checkbox"/>	debug	cmd	15	15
<input type="checkbox"/>	exit	cmd	15	1
<input type="checkbox"/>	quit	cmd	15	1
<input type="checkbox"/>	logout	cmd	15	1
<input type="checkbox"/>	login	cmd	0	
<input type="checkbox"/>	show	cmd	15	1
<input type="checkbox"/>	test	cmd	15	15
<input type="checkbox"/>	undebug	cmd	15	15

После открытия сессии в основном окне будет активизирована панель уровней привилегий команд.

Анализ состава и уровней привилегий команд Cisco Pix

Создание новой сессии в режиме анализа

Панель уровней привилегий (анализ)

зеленые: уровни привилегий одноименных команд совпадают.

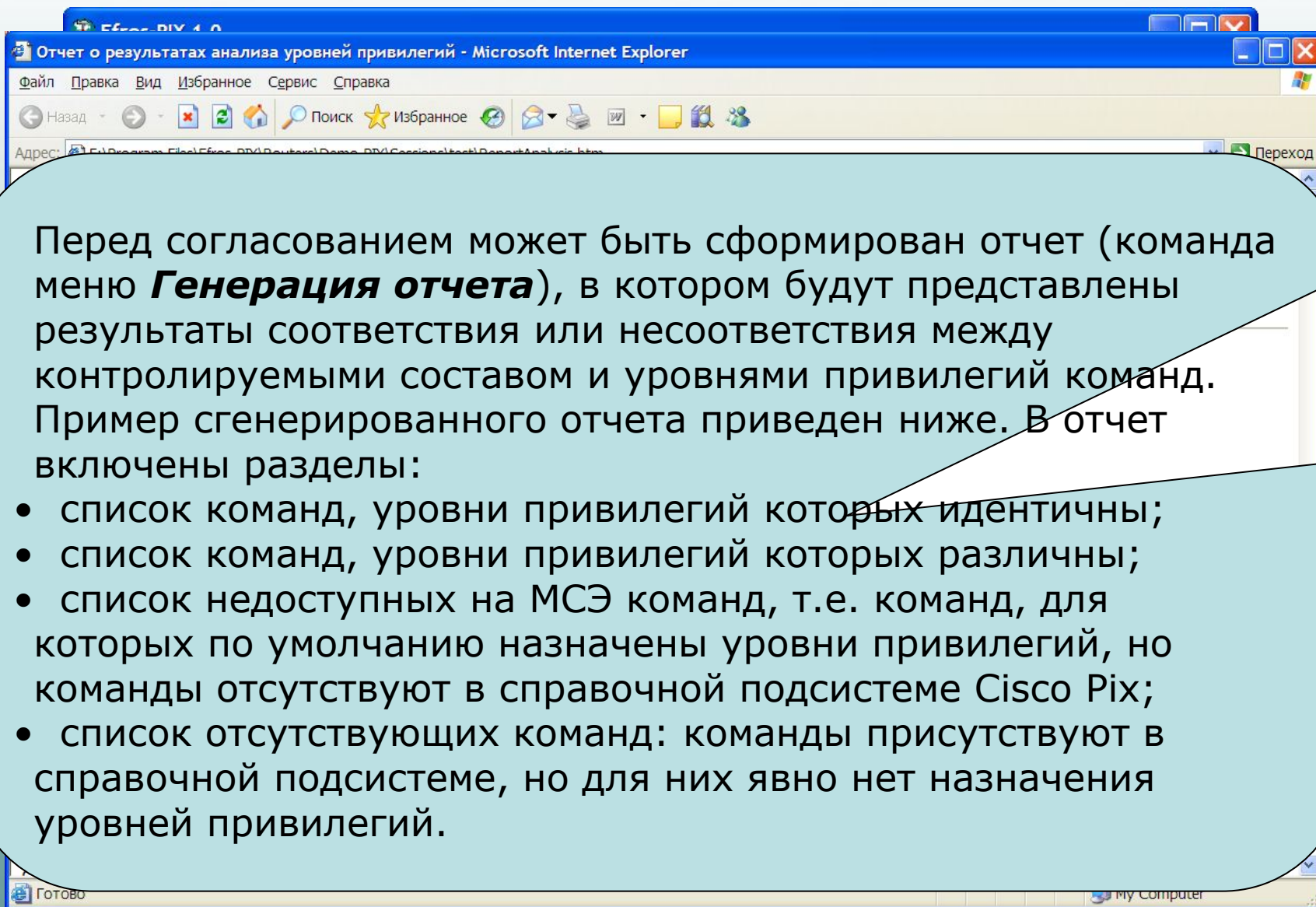
привилегии

<input type="checkbox"/>	exec	show	cmd	15	15
<input checked="" type="checkbox"/>	exec	test	cmd	15	15
<input checked="" type="checkbox"/>	exec	undebug	cmd	15	15

На панели отражаются уровни привилегий команд режимов, заданные по умолчанию в Cisco Pix (столбец УП (по умолчанию)), которые формируются из файла ParserMode.ini и уровни привилегий команд, полученные с использованием сканера команд (столбец УП (сканирование)).

Анализ состава и уровней привилегий команд Cisco Pix

Создание отчета



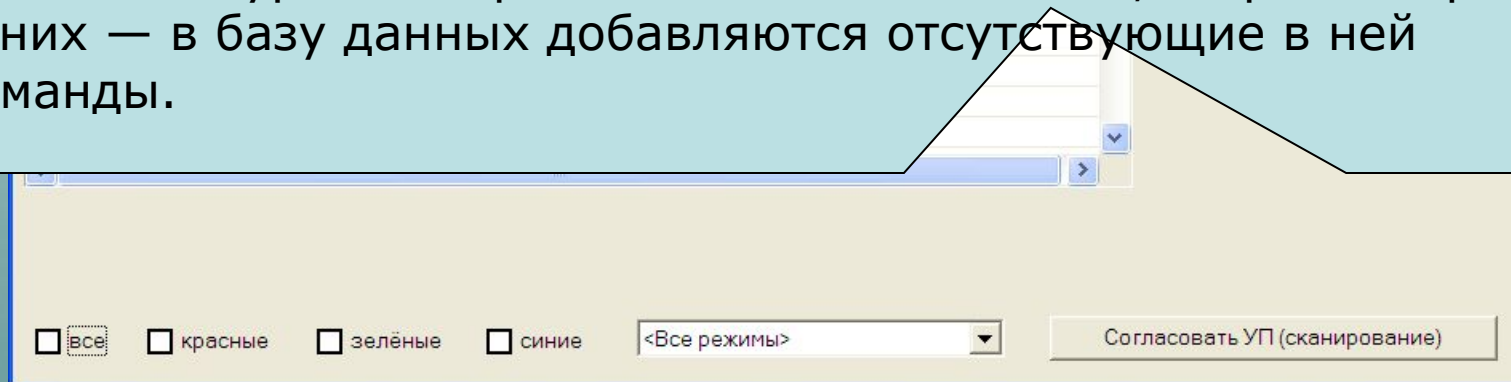
Перед согласованием может быть сформирован отчет (команда меню **Генерация отчета**), в котором будут представлены результаты соответствия или несоответствия между контролируемым составом и уровнями привилегий команд. Пример сгенерированного отчета приведен ниже. В отчет включены разделы:

- список команд, уровни привилегий которых идентичны;
- список команд, уровни привилегий которых различны;
- список недоступных на МСЭ команд, т.е. команд, для которых по умолчанию назначены уровни привилегий, но команды отсутствуют в справочной подсистеме Cisco Pix;
- список отсутствующих команд: команды присутствуют в справочной подсистеме, но для них явно нет назначения уровней привилегий.

Анализ состава и уровней привилегий команд Cisco Pix

Создание новой сессии в режиме анализа

С помощью кнопки **Согласовать УП (сканирование)** можно выполнить согласование составов команд, режимов и их уровней привилегий. Причины рассогласования могут быть различными: некорректная работа справочной подсистемы МСЭ Cisco Pix при отображении команд и их уровней привилегий, либо некорректное (неполное) сканирование МСЭ с помощью сканера команд. При выборе для согласования красных строк изменяется уровень привилегий в базе данных, а при выборе синих — в базу данных добавляются отсутствующие в ней команды.



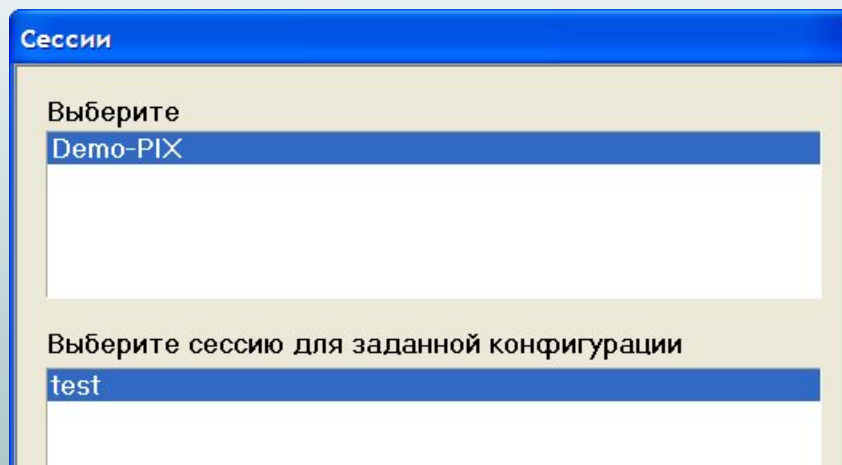
Создание файла конфигурации для МСЭ Cisco Pix

При создании файла конфигурации для разграничения доступа к командам МСЭ Cisco Pix требуется выполнить следующую последовательность шагов:

- создание новой (открытие существующей) сессии в режиме редактирования;
- обработка команд (перенос с одного уровня привилегий на другой) режима exes;
- обработка подчиненных режимов;
- создание файла конфигурации.

Создание файла конфигурации для МСЭ Cisco Pix

Создание новой сессии в режиме редактирования



Сессии

Выберите

Демо-PIX

Выберите сессию для заданной конфигурации

test

Для создания новой сессии необходимо выбрать тип используемого МСЭ из списка, в котором обязательно есть тип, используемый по умолчанию (Demo-Pix). Только после этого можно приступить к созданию новой сессии или использовать существующую. В зависимости от выбранного типа МСЭ список ранее созданных сессий будет различным, т.к. каждая сессия обязательно сопоставляется с определенным типом МСЭ.

Создание файла конфигурации для МСЭ Cisco Pix

Создание новой сессии в режиме редактирования



Режим	Команда	Вариант	УП (текущий)	УП (новый)
<input checked="" type="checkbox"/> exec	client-update	cmd	15	15
<input type="checkbox"/> exec	help	cmd	15	15
<input type="checkbox"/> exec	no	cmd	15	15
<input type="checkbox"/> exec	clear	cmd	15	1
<input type="checkbox"/> exec	debug	cmd	15	15
<input type="checkbox"/> exec	exit	cmd	15	15
<input type="checkbox"/> exec	quit	cmd	15	15
<input type="checkbox"/> exec	logout	cmd	15	15

После открытия сессии в основном окне будет активизирована панель уровней привилегий команд режима редактирования.

Структура панели аналогична панели режима анализа. Но теперь здесь отображаются текущий уровень привилегий команд режимов в рамках сессии и новый, тот, который им будет назначен. Первоначально для согласованных представлений во время анализа они будут совпадать.

Создание файла конфигурации для МСЭ Cisco Pix

Создание новой сессии в режиме редактирования

Панель уровней привилегий (редактирование)

	Режим	Команда	Вариант	УП (текущий)	УП (новый)
<input type="checkbox"/>	еxес	client-update	cmd	15	15
<input type="checkbox"/>	еxес	help	cmd	15	15
<input type="checkbox"/>	еxес	no	cmd	15	15
<input type="checkbox"/>	еxес	clear	cmd	15	1
<input type="checkbox"/>	еxес	debug	cmd	15	15
<input type="checkbox"/>	еxес	exit	cmd	15	15
<input type="checkbox"/>	еxес	quit	cmd	15	15
<input type="checkbox"/>	еxес	logout	cmd	15	15
<input type="checkbox"/>	еxес	login	cmd	0	0
<input type="checkbox"/>	еxес	show	cmd	15	0
<input type="checkbox"/>	еxес	test	cmd	15	1
<input type="checkbox"/>	еxес	undebug	cmd	15	2

все красные зелёные синие <Все режимы>

Изменять уровни привилегий команд можно либо непосредственно на данной панели в столбце **УП(новый)**

Создание файла конфигурации для МСЭ Cisco Pix

Создание новой сессии в режиме редактирования

The screenshot displays a software interface for creating a configuration file. On the left, a table lists various commands and their properties. The 'login' command is selected. On the right, a tree view shows the configuration structure, with a context menu open over the 'enable' node.

Команда	Вариант	Уровень привилег...
enable	cmd	0
login	cmd	0
arp	clear	1
clear	cmd	1
flash:	show	1
show	cmd	1
activation-key	cmd	15
asdm	cmd	15
blocks	cmd	15
capture	cmd	15
cd	cmd	15
changeto	cmd	15
aaa	clear	15
aaa-server	clear	15
access-list	clear	15
asp	clear	15
blocks	clear	15
capture	clear	15
chardrop	clear	15
console-output	clear	15

The tree view on the right shows a hierarchy starting with '<root>'. Underneath, there are nodes for '0' and '1'. The 'enable' node is selected, and a context menu is open with the following options:

- Выбрать ветвь
- Выбрать уровень
- Групповое выделение...
- Переместить выделенные элементы сюда
- Добавить...
- Добавить из файла...
- Удалить

либо в окне документа графического представления структуры команд. Данные панели синхронизированы.

Создание файла конфигурации для МСЭ Cisco Pix

Создание новой сессии в режиме редактирования

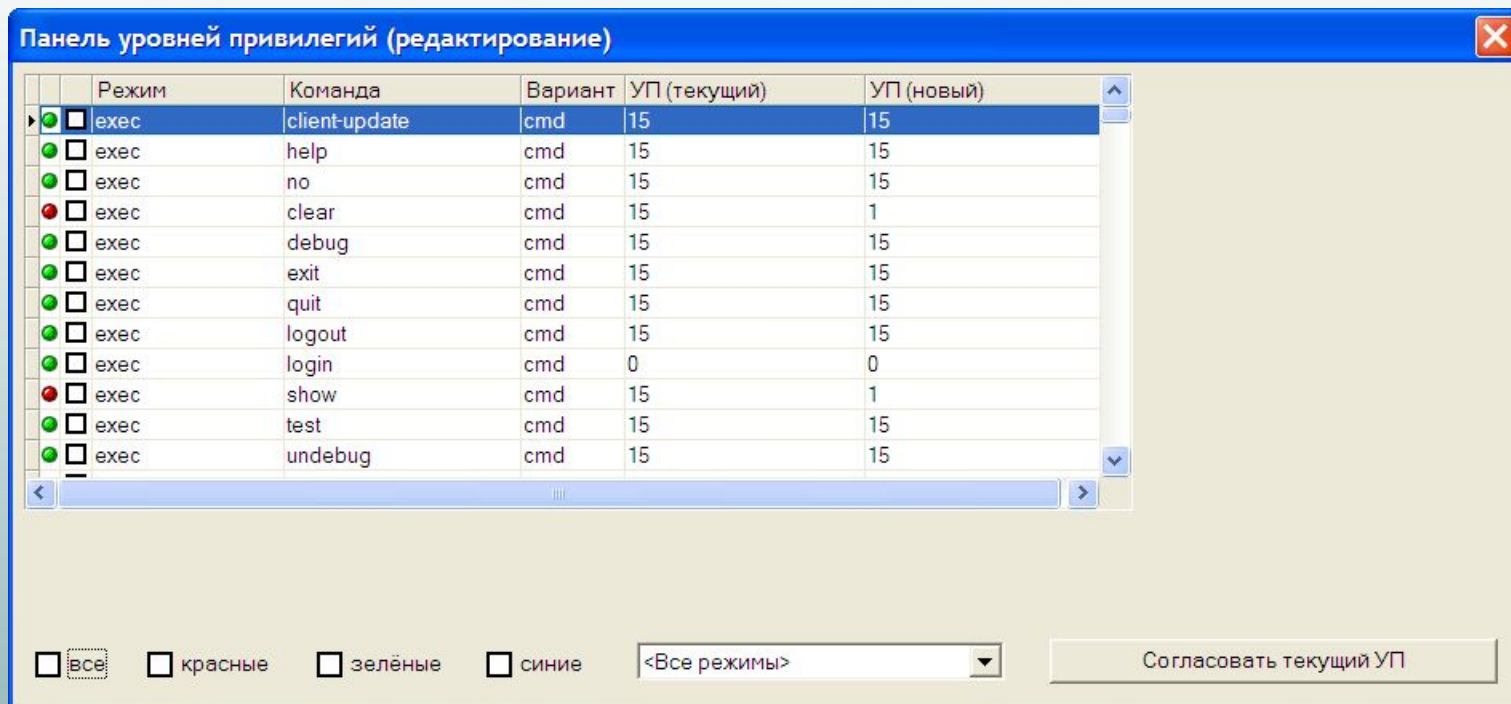
Команда	Вариант	Уровень привилег...
enable	cmd	0
login	cmd	0
arp	clear	1
clear	cmd	1
flash:	show	1
show	cmd	1
activation-key	cmd	15
asdm	cmd	15
blocks	cmd	15
capture	cmd	15
cd	cmd	15
changeto	cmd	15
aaa	clear	15
aaa-server	clear	15
access-list	clear	15
asp	clear	15
blocks	clear	15
capture	clear	15
chardrop	clear	15
console-output	clear	15

Выбрать ветвь
Выбрать уровень
Групповое выделение...
Переместить выделенные элементы сюда
Добавить...
Добавить из файла...
Удалить

либо в окне документа графического представления структуры команд. Данные панели синхронизированы.

Создание файла конфигурации для МСЭ Cisco Pix

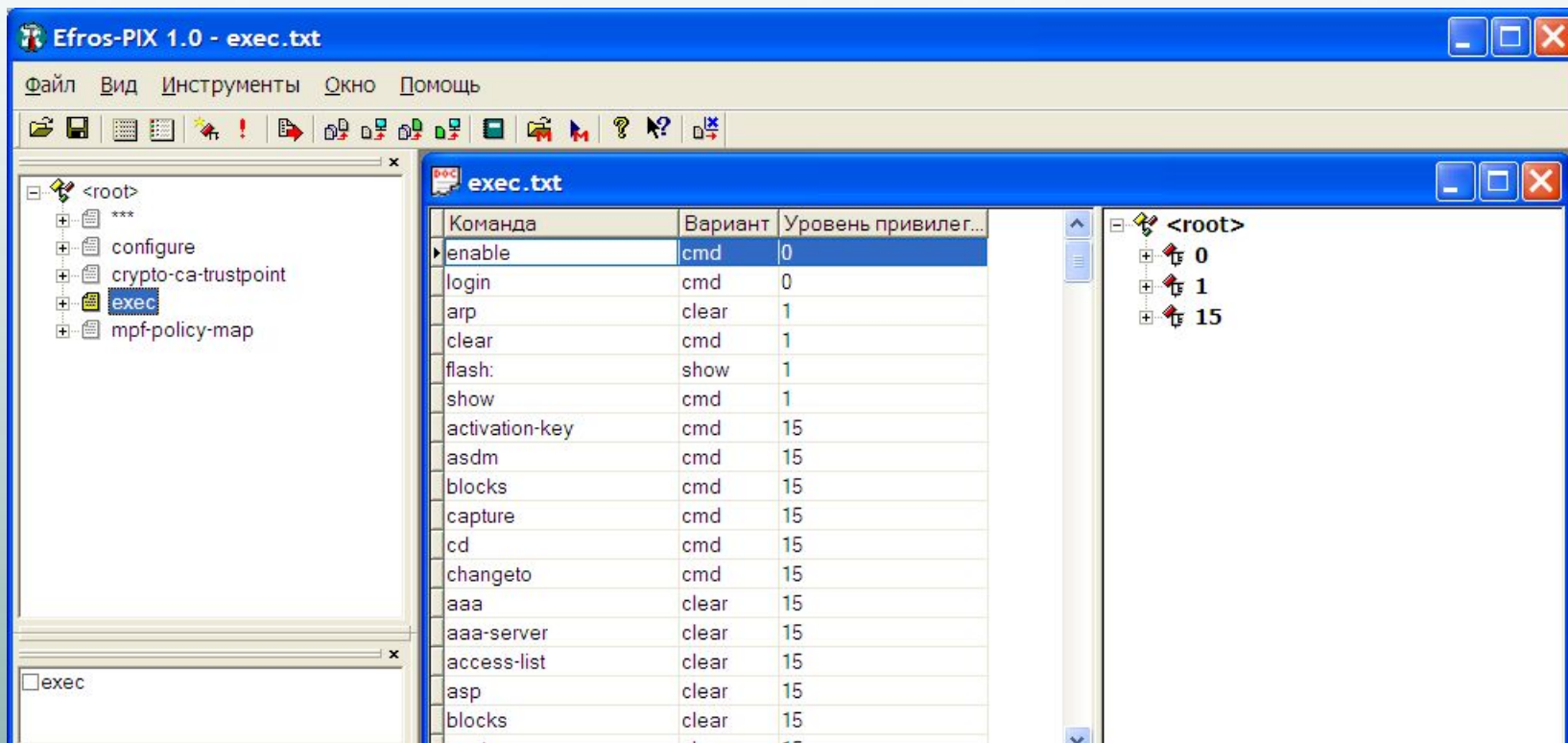
Создание новой сессии в режиме редактирования



После завершения редактирования уровней привилегий необходимо нажать кнопку **Согласовать текущий УП**, результатом будет внесение изменений в файл **ParserModes.ini** и сохранение в каталоге сессии, т.е. в следующем сеансе работы при открытии сессии новые уровни привилегий станут текущими.

Создание файла конфигурации для МСЭ Cisco Pix

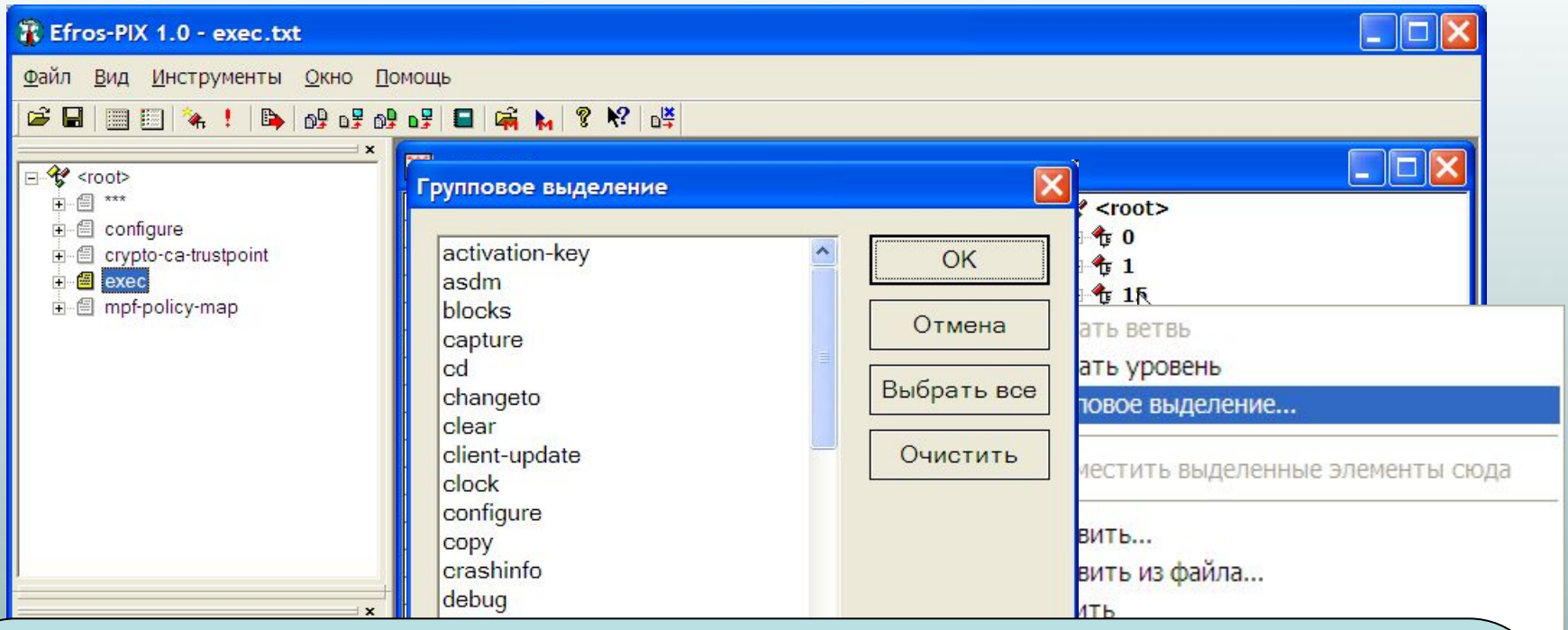
Обработка команд режима (на примере режима exec)



По двойному щелчку левой кнопкой мыши на режиме «exec» в окне панели режимов (или в любой строке режима exec на панели уровней привилегий команд) открывается окно документов режима exec с заданными уровнями привилегий для этого режима.

Создание файла конфигурации для МСЭ Cisco Pix

Обработка команд режима (на примере режима exec)



При выборе группового выделения открывается окно, где при нажатии кнопки «**Выбрать все**» будут отмечены все команды, представленные в окне. Для выбора отдельных команд необходимо нажать и удерживать кнопку «Ctrl» и левой кнопкой мыши выбрать необходимые команды. После выбора команд необходимо нажать кнопку «ОК». Выбранные команды будут помещены в буфер.

Создание файла конфигурации для МСЭ Cisco Pix

Обработка команд режима (на примере режима exec)

The screenshot shows the Efros-PIX 1.0 software interface. The main window displays a list of commands and their privilege levels. The 'exec' mode is selected in the left pane. The table below shows the configuration for the 'exec' mode.

Режим	Команда	Новый режим
exec	configure terminal	configure

Создание нового уровня привелегий

Для получения справки нажмите "F1"

Создание файла конфигурации для МСЭ Cisco Pix

Обработка команд режима (на примере режима exec)

The screenshot shows the Efros-PIX 1.0 software interface. The main window displays a table of commands and their privilege levels. A context menu is open over the table, showing options to move selected elements to a specific level (14).

Команда	Вариант	Уровень привилегий
enable	cmd	0
login	cmd	0
arp	clear	1
clear	cmd	1
flash:	show	1
show	cmd	1
asdm	cmd	14
blocks	cmd	14
capture	cmd	14
cd	cmd	14
changeto	cmd	14
aaa	clear	14
aaa-server	clear	14
access-list	clear	14
asp	clear	14
blocks	clear	14

Context menu options:

- Выбрать ветвь
- Выбрать уровень
- Групповое выделение...
- Переместить выделенные элементы сюда**
- Добавить...
- Добавить из файла...
- Удалить

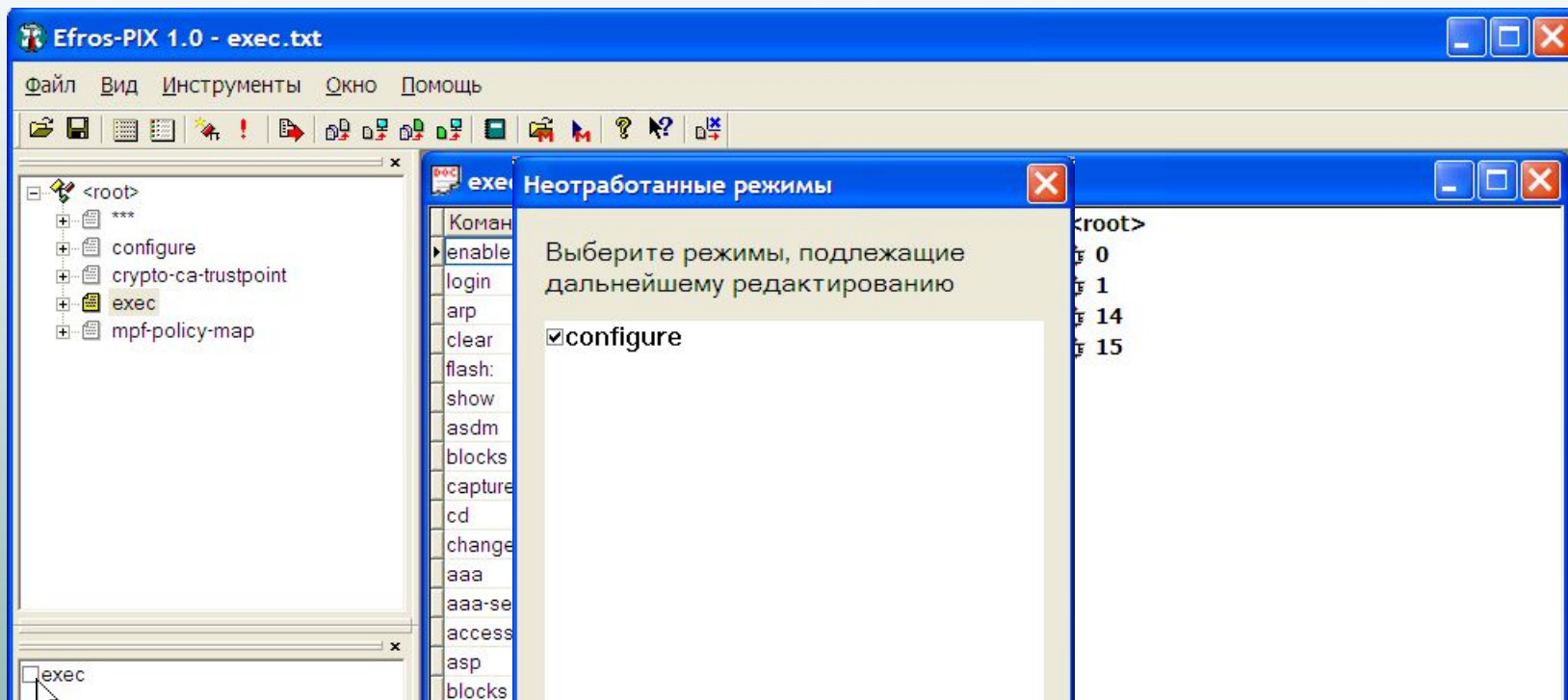
Режим	Команда	Новый режим
exec	configure terminal	configure

Для получения справки нажмите "F1" NUM

Перенос выделенных команд на 14 уровень

Создание файла конфигурации для МСЭ Cisco Pix

Обработка команд режима (на примере режима exec)

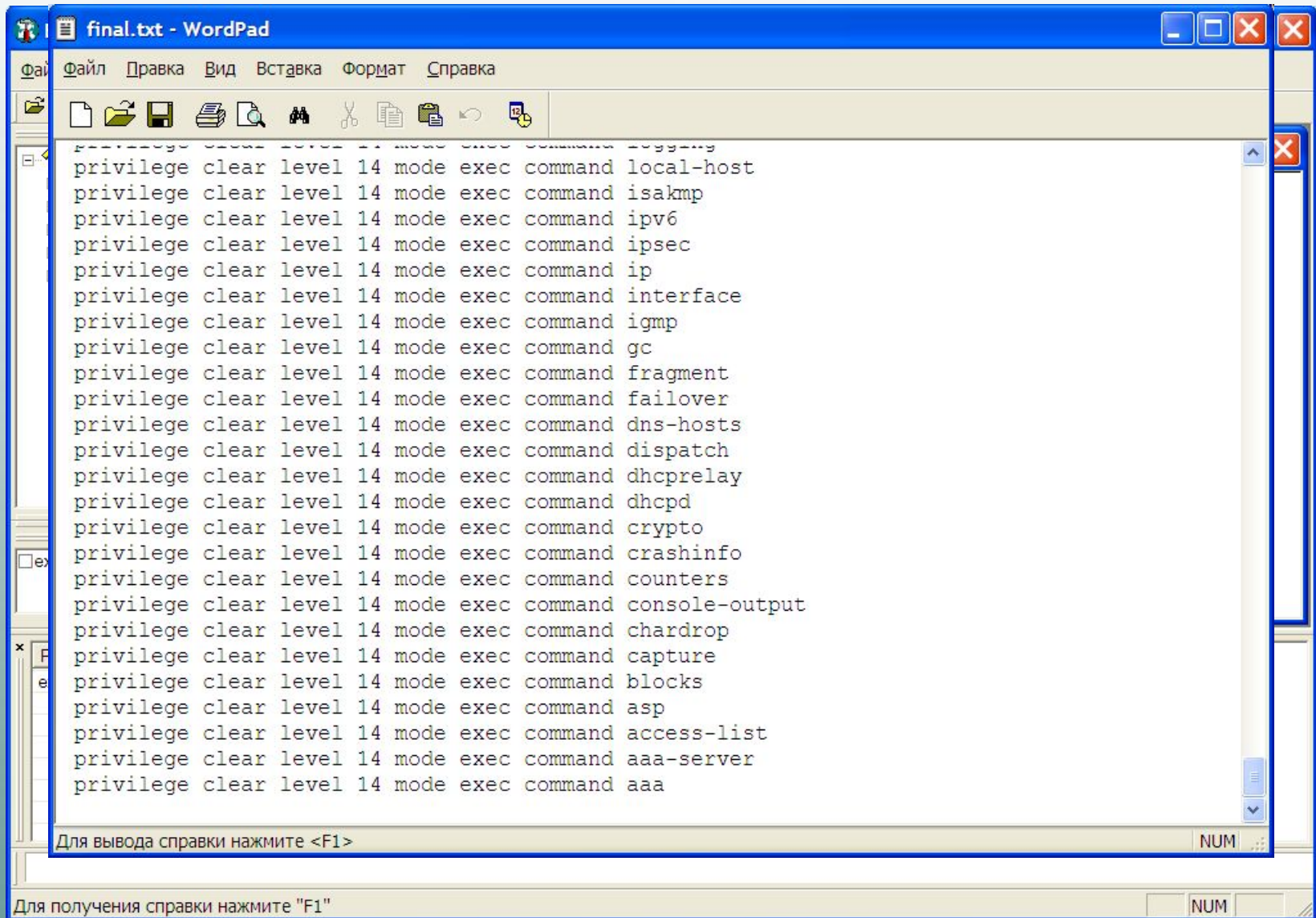


Если при изменении уровней привилегий были задействованы команды, которые переводят интерпретатор команд Cisco Pix в другой режим, после отработки режима появится окно «Неотработанные режимы». В этом окне установить галочки напротив тех режимов, которые требуют дальнейшей обработки.

Обработка подчиненных режимов осуществляется точно таким же образом, как и обработка режима «exec». Все «неотработанные режимы» подсвечены желтым цветом в окне дерева режимов.

Создание файла конфигурации для МСЭ Cisco Pix

Создание файла конфигурации



```
privilege clear level 14 mode exec command logging
privilege clear level 14 mode exec command local-host
privilege clear level 14 mode exec command isakmp
privilege clear level 14 mode exec command ipv6
privilege clear level 14 mode exec command ipsec
privilege clear level 14 mode exec command ip
privilege clear level 14 mode exec command interface
privilege clear level 14 mode exec command igmp
privilege clear level 14 mode exec command gc
privilege clear level 14 mode exec command fragment
privilege clear level 14 mode exec command failover
privilege clear level 14 mode exec command dns-hosts
privilege clear level 14 mode exec command dispatch
privilege clear level 14 mode exec command dhcprelay
privilege clear level 14 mode exec command dhcpd
privilege clear level 14 mode exec command crypto
privilege clear level 14 mode exec command crashinfo
privilege clear level 14 mode exec command counters
privilege clear level 14 mode exec command console-output
privilege clear level 14 mode exec command chardrop
privilege clear level 14 mode exec command capture
privilege clear level 14 mode exec command blocks
privilege clear level 14 mode exec command asp
privilege clear level 14 mode exec command access-list
privilege clear level 14 mode exec command aaa-server
privilege clear level 14 mode exec command aaa
```

Для вывода справки нажмите <F1>

Создание файла конфигурации для сервера TACACS+

Вызов модуля генерации

Основной метод авторизации команд определенного уровня привилегий указывает на то, будут ли команды (и их операнды) нижележащих уровней добавляться в данный результирующий файл конфигурации при его создании. То есть, если для некоторого уровня привилегий был установлен основной метод авторизации команд — «TACACS+», то в этом уровне будут гарантированно присутствовать все команды нижележащих уровней со своими наборами операндов.

зволяет про

возможные уровни привилегии, а также устанавливать

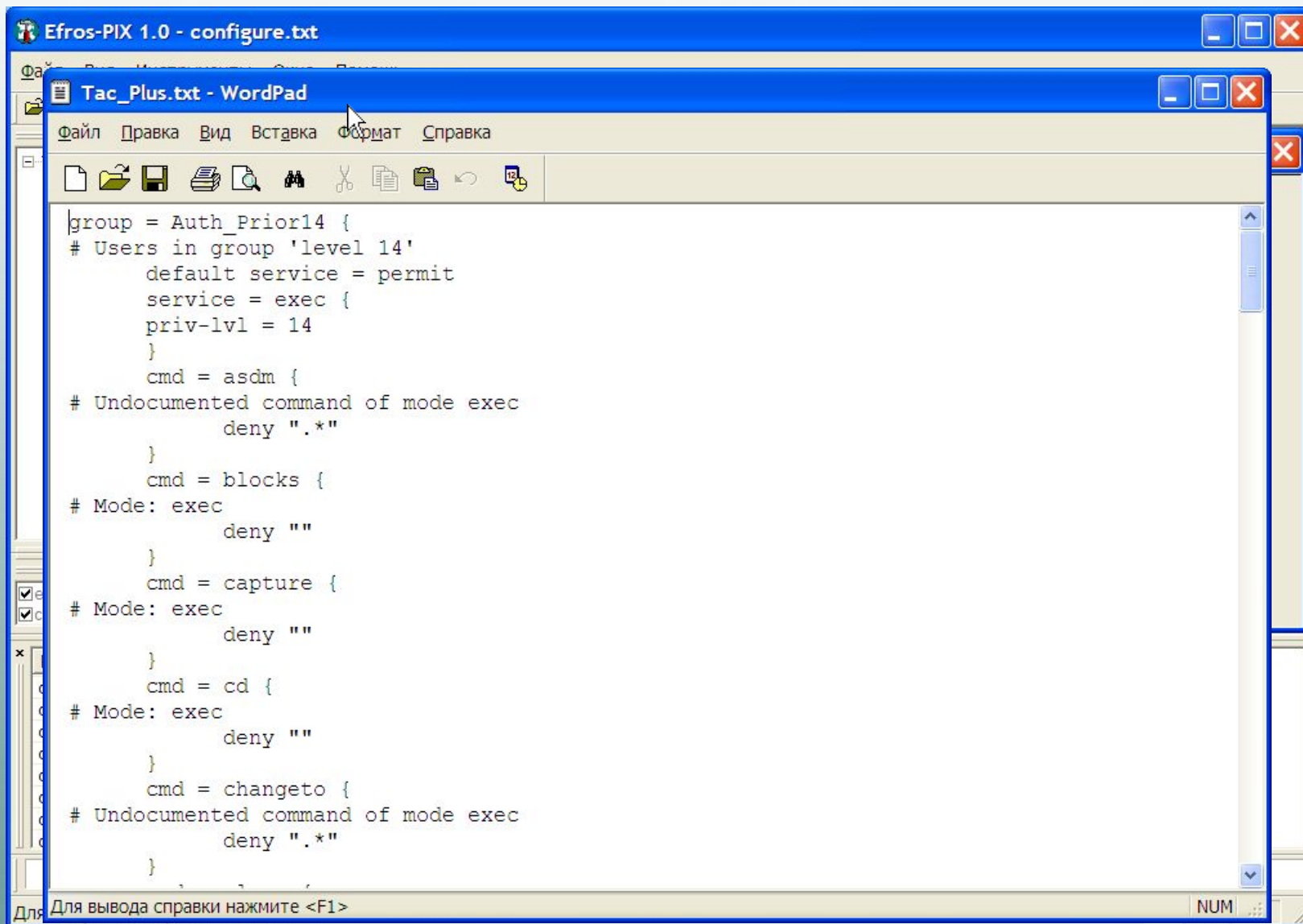
Установка политики разграничения доступа (разрешительная или запретительная) и выбор основного метода авторизации команд (TACACS+ или Другой) выполняются для каждого уровня привилегий команд. При выборе уровня его номер отображается в двух нижележащих заголовках

Для получения справки нажмите "F1"

NUM

Создание файла конфигурации для сервера TACACS+

Просмотр конфигурации



```
group = Auth_Prior14 {
# Users in group 'level 14'
  default service = permit
  service = exec {
    priv-lvl = 14
  }
  cmd = asdm {
# Undocumented command of mode exec
    deny ".*"
  }
  cmd = blocks {
# Mode: exec
    deny ""
  }
  cmd = capture {
# Mode: exec
    deny ""
  }
  cmd = cd {
# Mode: exec
    deny ""
  }
  cmd = changeto {
# Undocumented command of mode exec
    deny ".*"
  }
}
```

Для вывода справки нажмите <F1>