Подготовка к работе ИС «ЭФРОС-PIX»

ИС «ЭФРОС-PIX» 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-PIX» необходимо выполнить следующие действия:

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

Подготовка к работе ИС «ЭФРОС-PIX»

Формирование базы данных команд Cisco Pix

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

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

Подготовка к работе ИС «ЭФРОС-PIX»

Формирование базы данных команд Cisco Pix

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

```
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-PIX»

Формирование базы данных команд Cisco Pix

База данных хранится в файлах ***Routers\<Имя МСЭ>\Modes*** и ***Routers\<ИмяМСЭ>\Comments.*** Первоначально в ИС «ЭФРОС-PIX» 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-PIX».

Для создания базы данных команд Cisco Pix для ИС «ЭФРОС-PIX» 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-PIX»

Формирование файлов настроек

Перед запуском ИС «ЭФРОС-PIX» 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 rumming-config all privilege all*** и результаты ее поместить в файл ***ParserModes.ini***

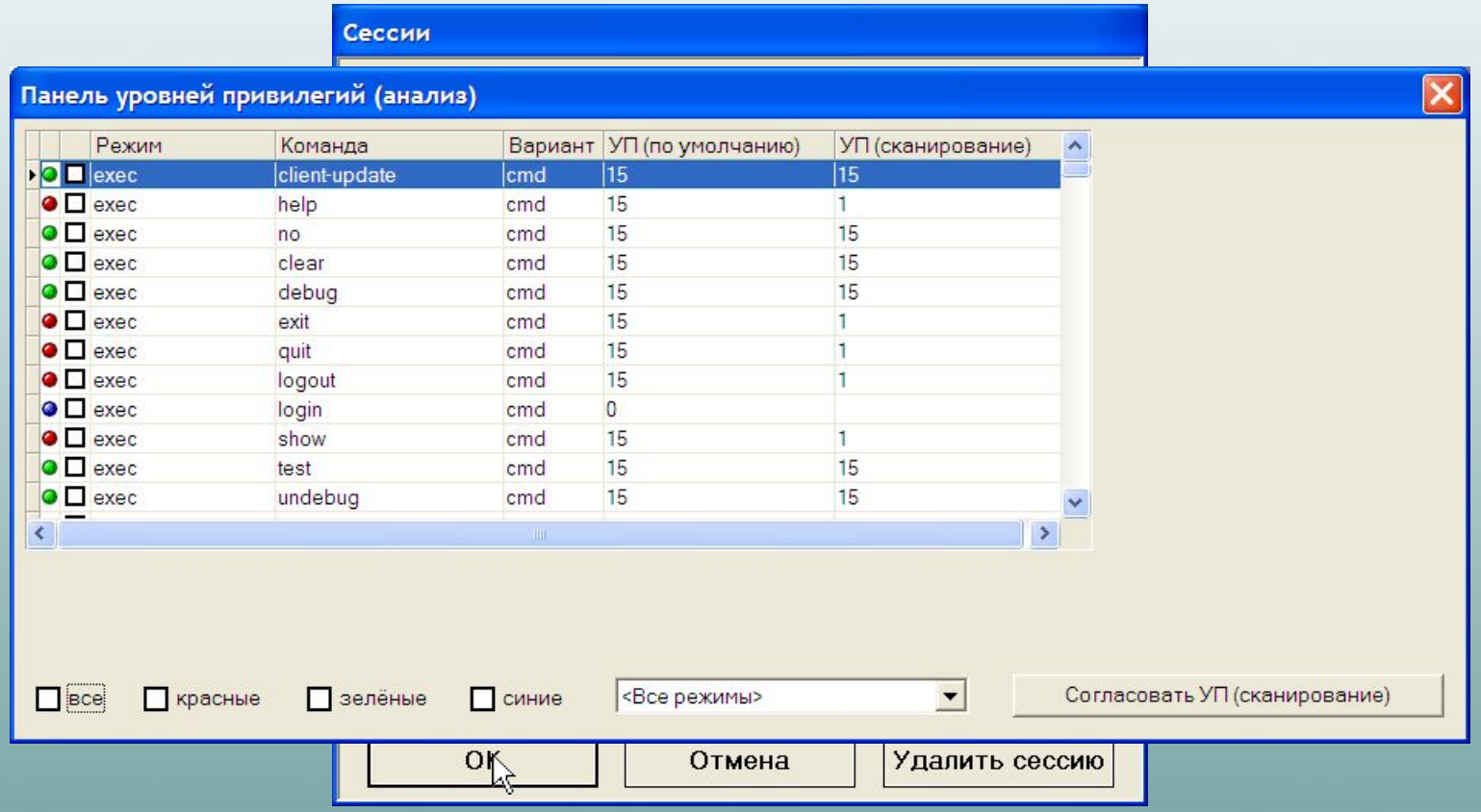
Анализ состава и уровней привилегий команд Cisco Pix

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

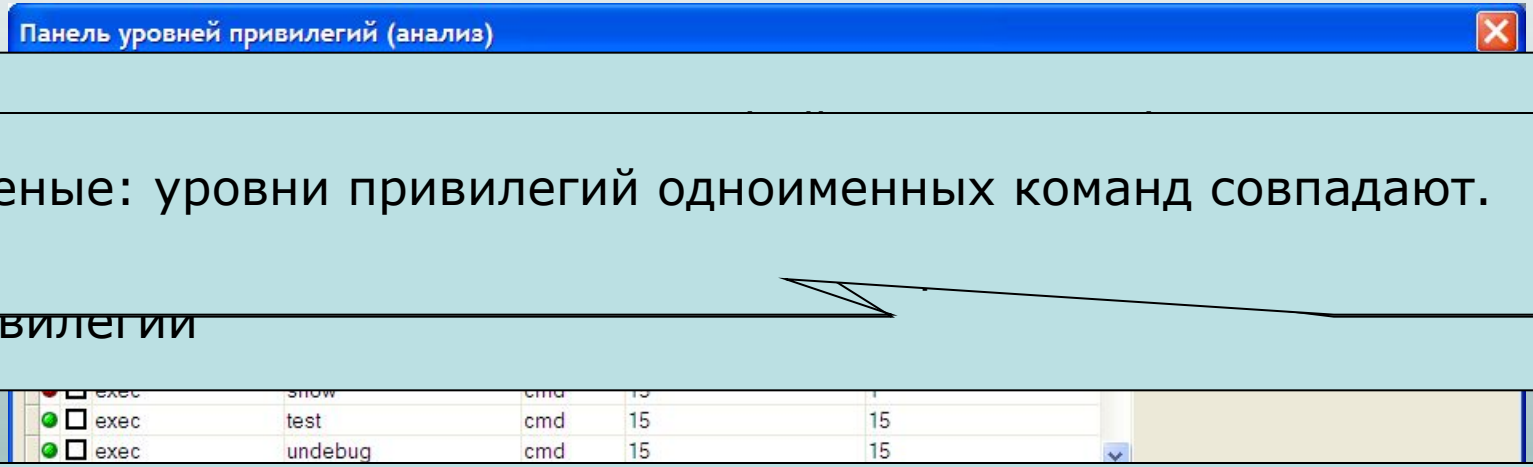
Создание новой сессии в режиме анализа



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



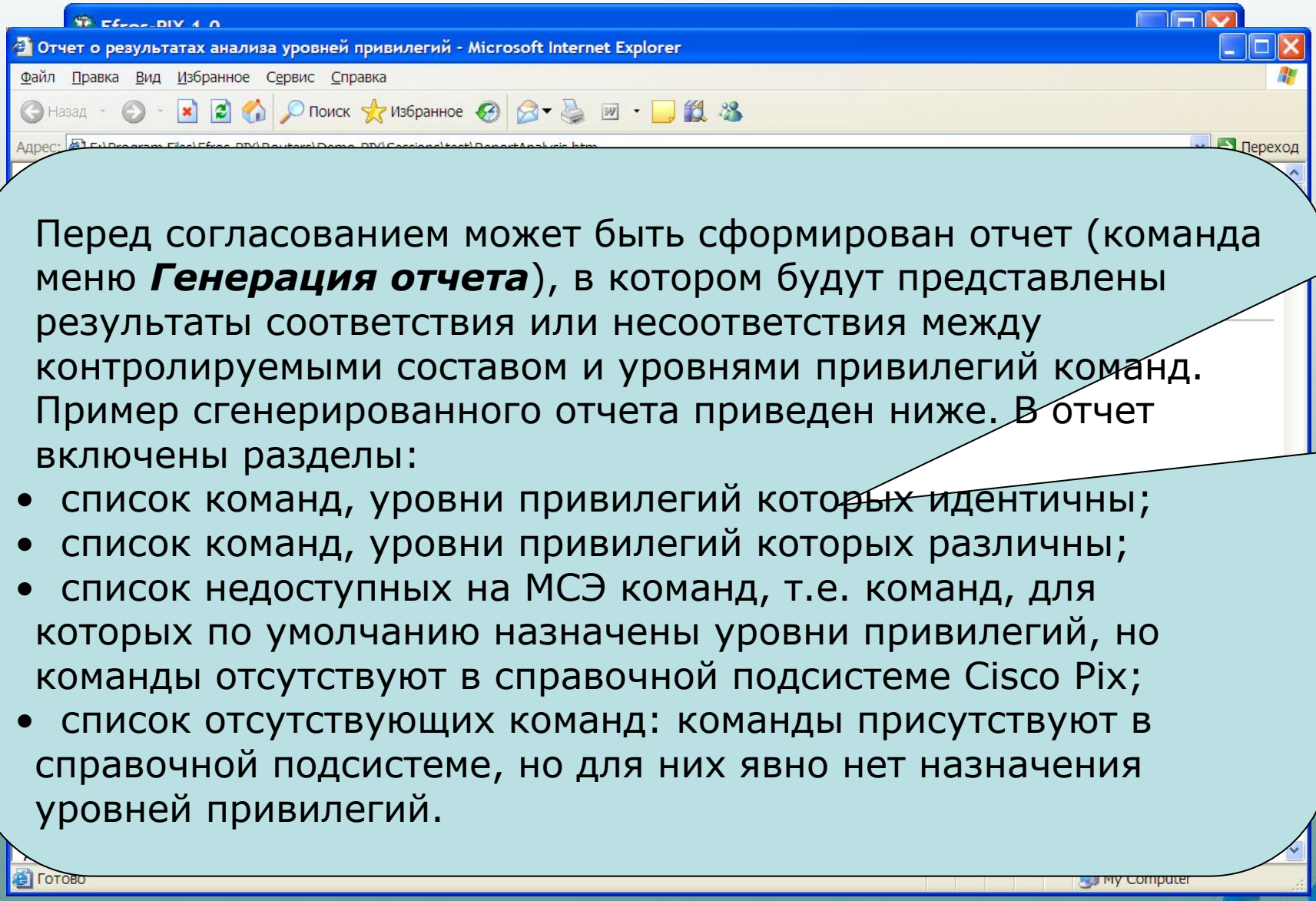
зеленые: уровни привилегий одноименных команд совпадают.

привилегий

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



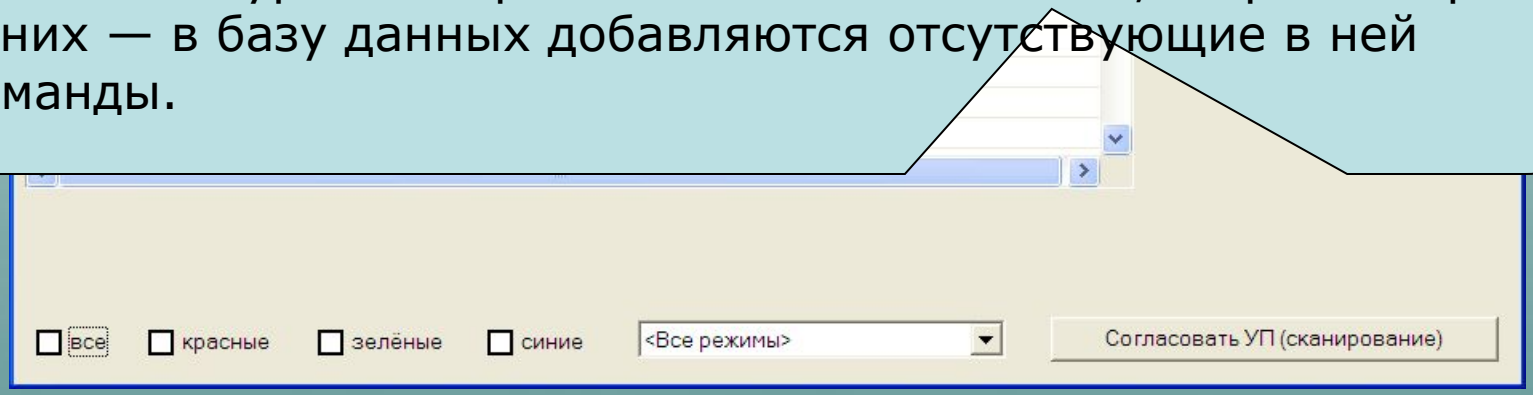
Перед согласованием может быть сформирован отчет (команда меню ***Генерация отчета***), в котором будут представлены результаты соответствия или несоответствия между контролируемыми составом и уровнями привилегий команд. Пример сгенерированного отчета приведен ниже. В отчет включены разделы:

- 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.



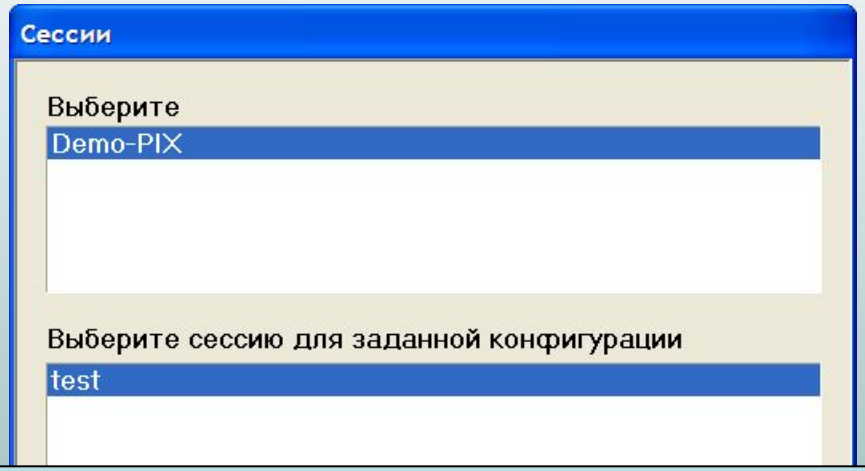
Создание файла конфигурации для МСЭ Cisco Pix

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 exec;
- обработка подчиненных режимов;
- создание файла конфигурации.

Создание файла конфигурации для МСЭ Cisco Pix

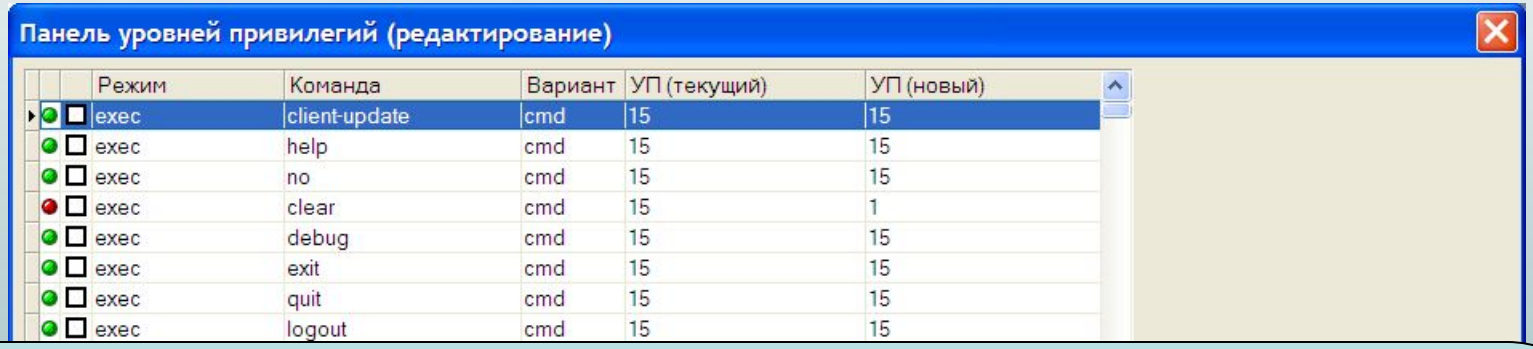
Создание новой сессии в режиме редактирования



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 приступать 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

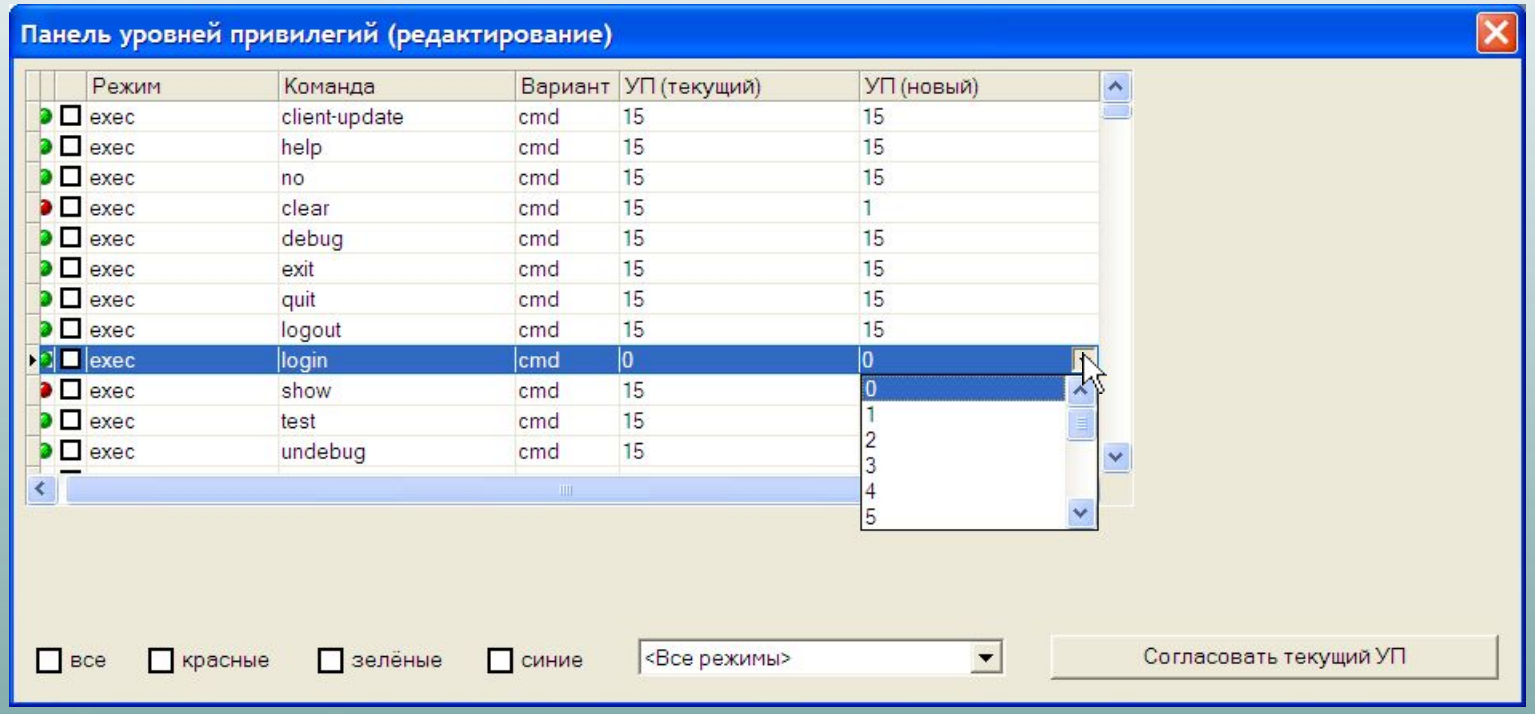


После открытия сессии в основном окне будет активизирована панель уровней привилегий команд режима редактирования.

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

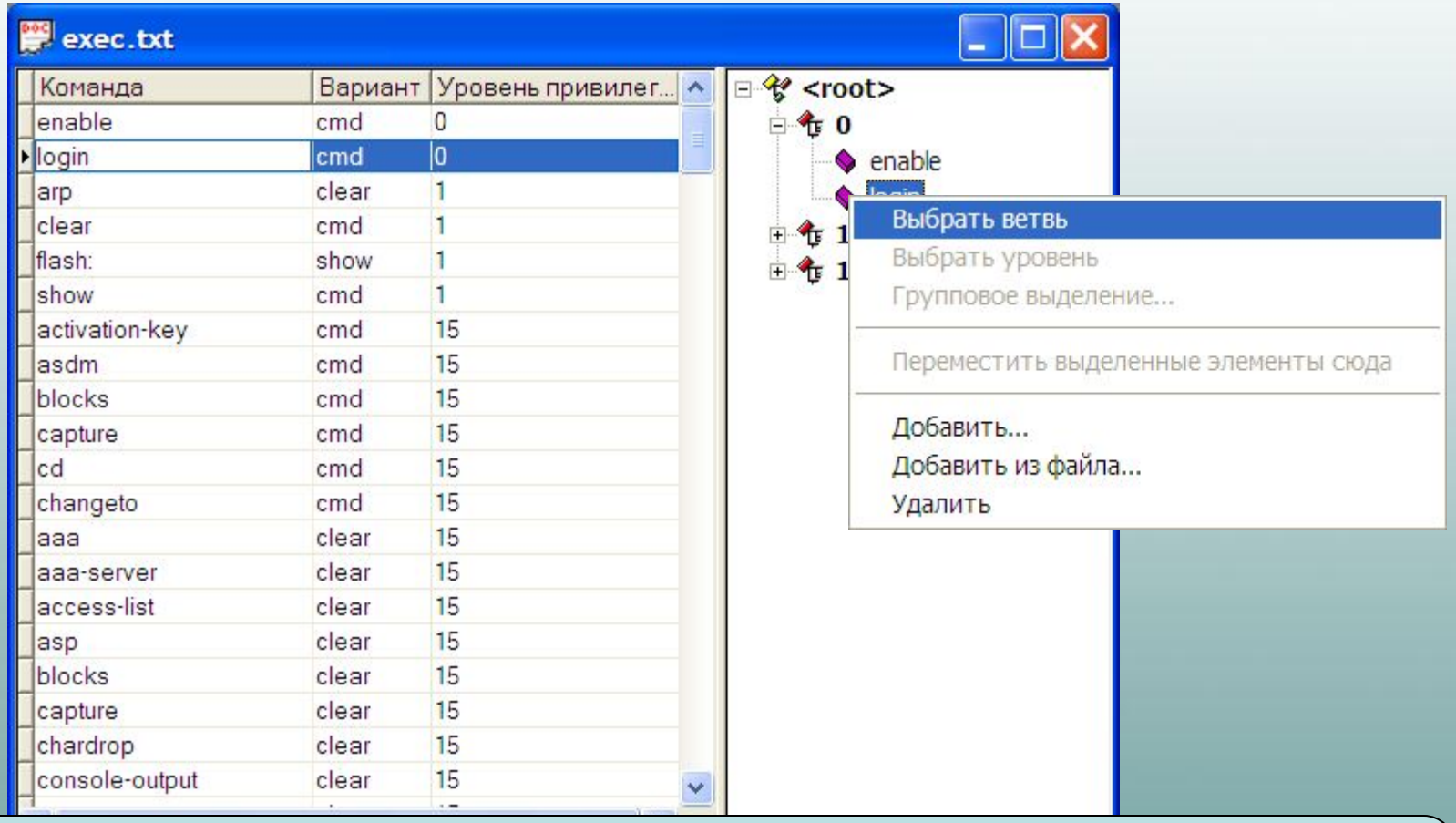
Создание новой сессии в режиме редактирования



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

Создание файла конфигурации для МСЭ Cisco Pix

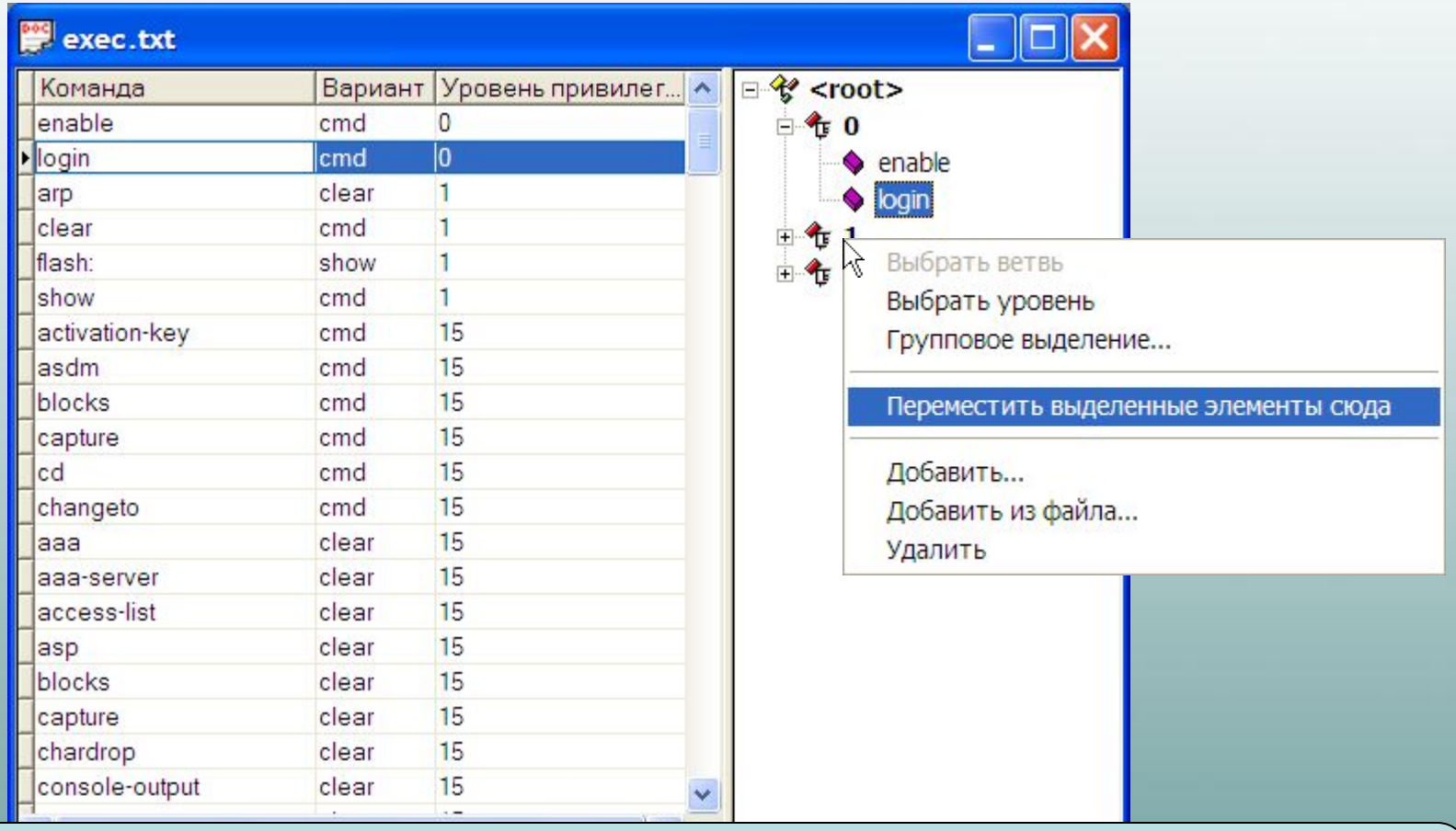
Создание новой сессии в режиме редактирования



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

Создание файла конфигурации для МСЭ Cisco Pix

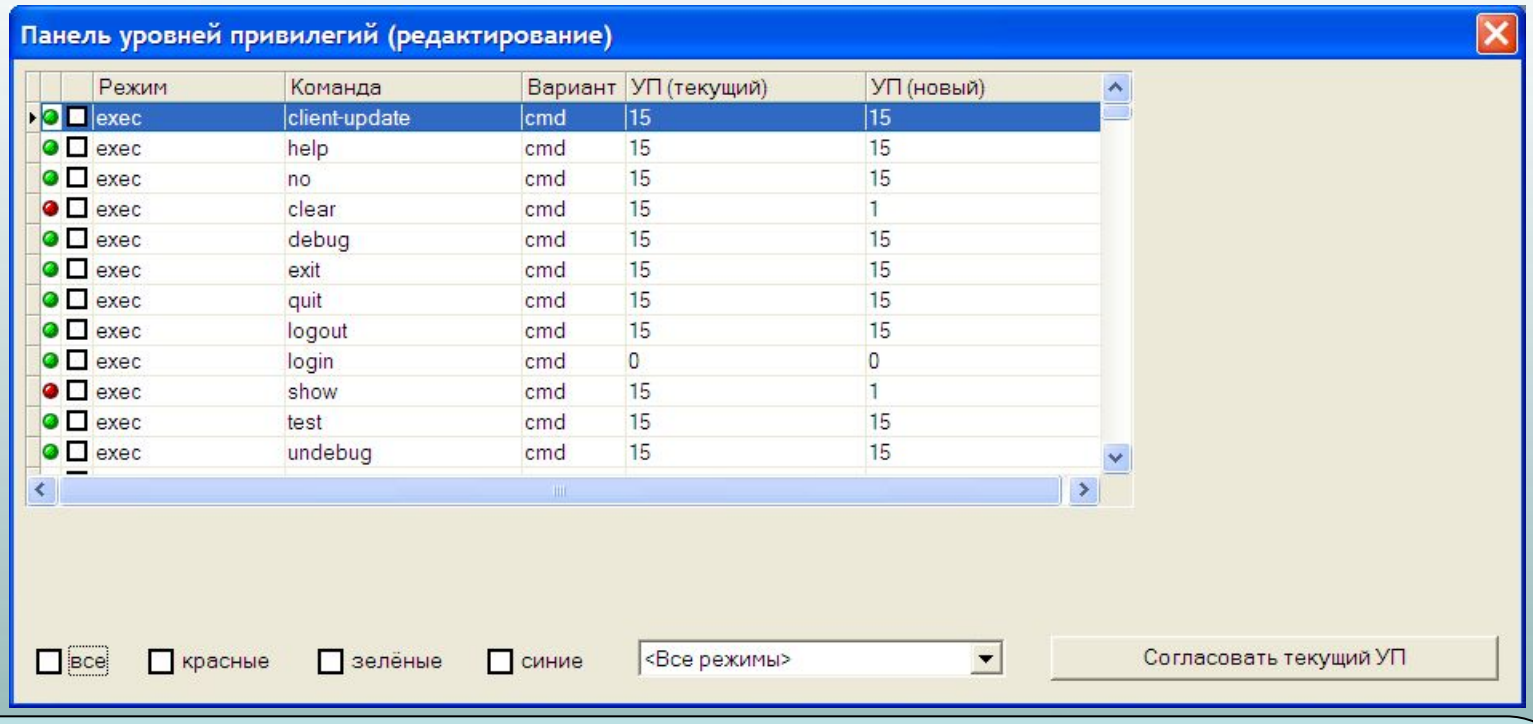
Создание новой сессии в режиме редактирования



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

Создание файла конфигурации для МСЭ Cisco Pix

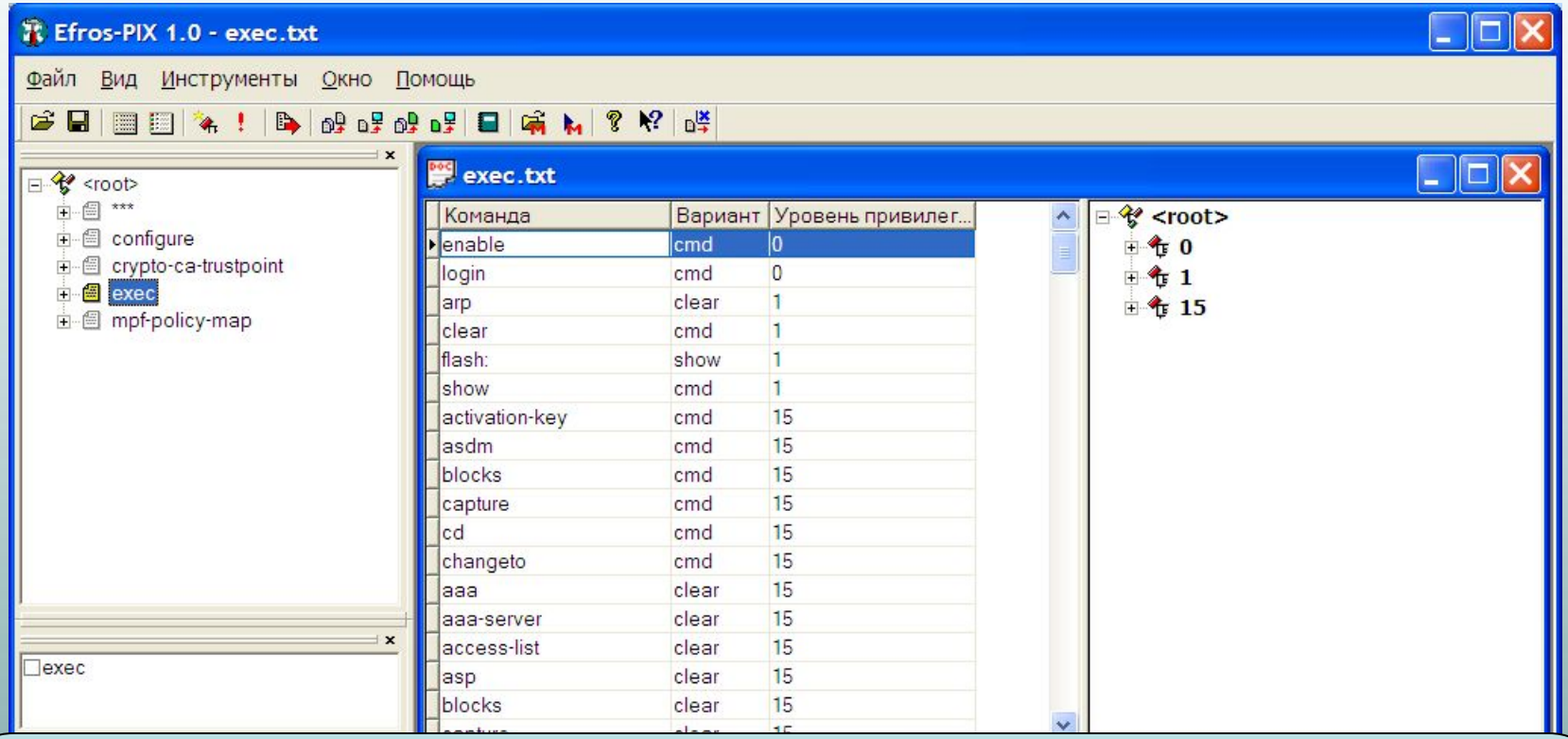
Создание новой сессии в режиме редактирования



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

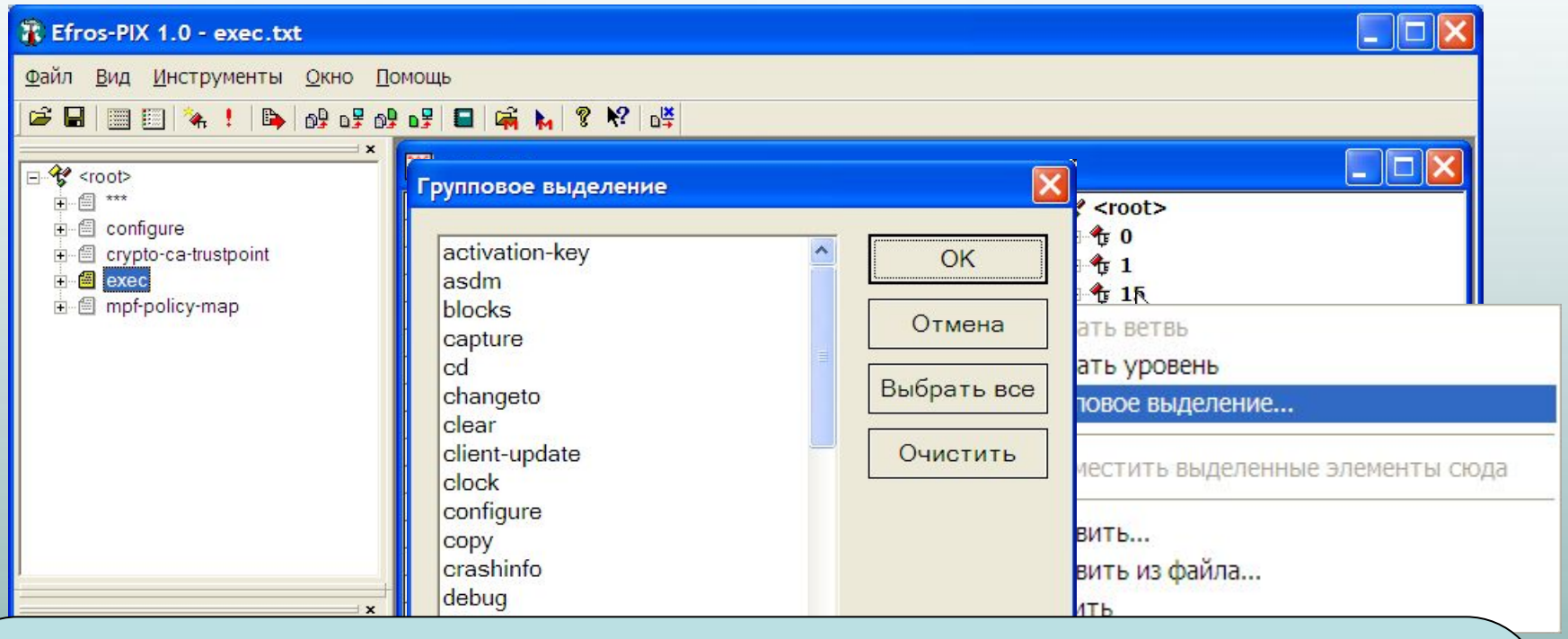
Обработка команд режима (на примере режима exec)



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

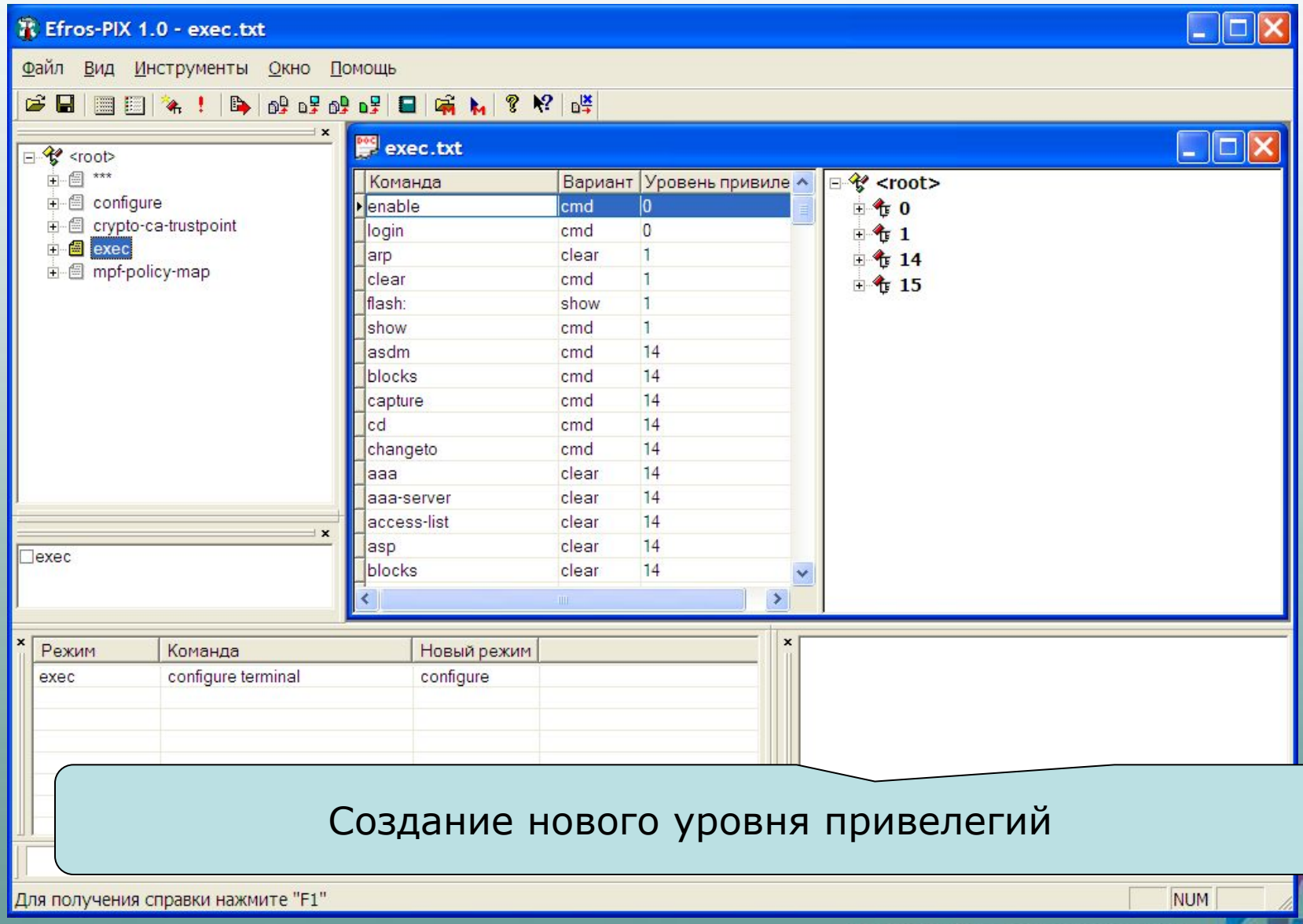
Обработка команд режима (на примере режима exec)



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.

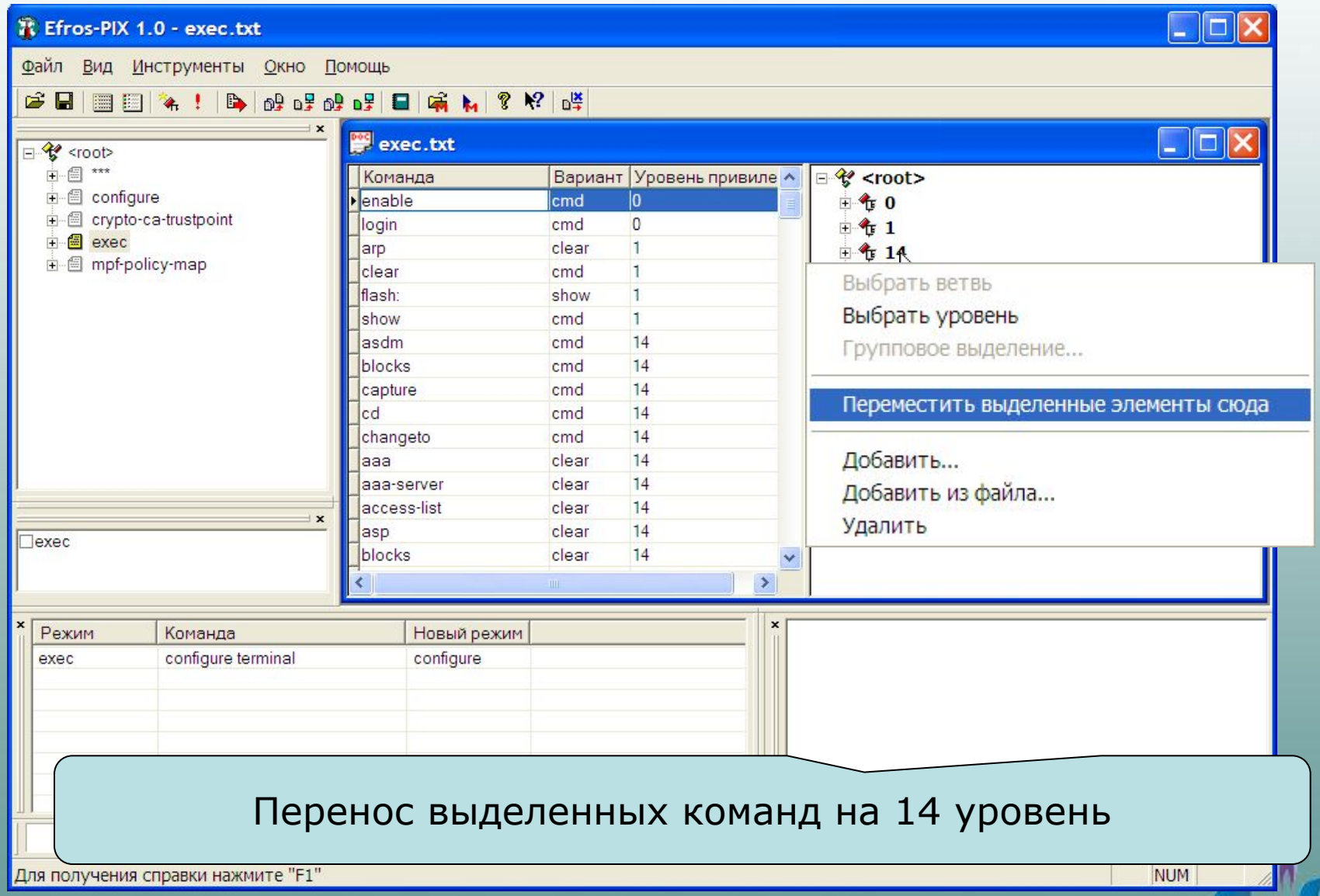
Создание файла конфигурации для МСЭ Cisco Pix

Обработка команд режима (на примере режима exec)



Создание файла конфигурации для МСЭ Cisco Pix

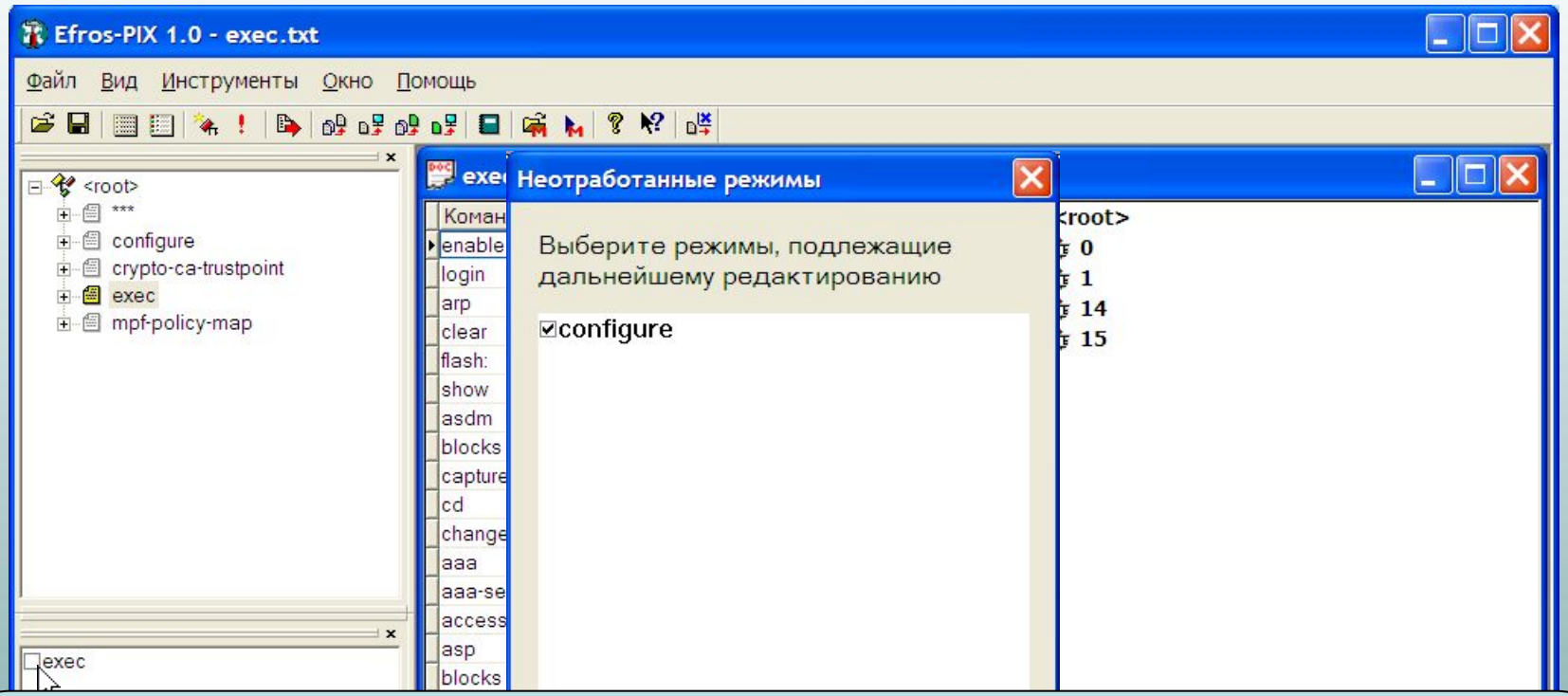
Обработка команд режима (на примере режима exec)



Перенос выделенных команд на 14 уровень

Создание файла конфигурации для МСЭ Cisco Pix

Обработка команд режима (на примере режима exec)

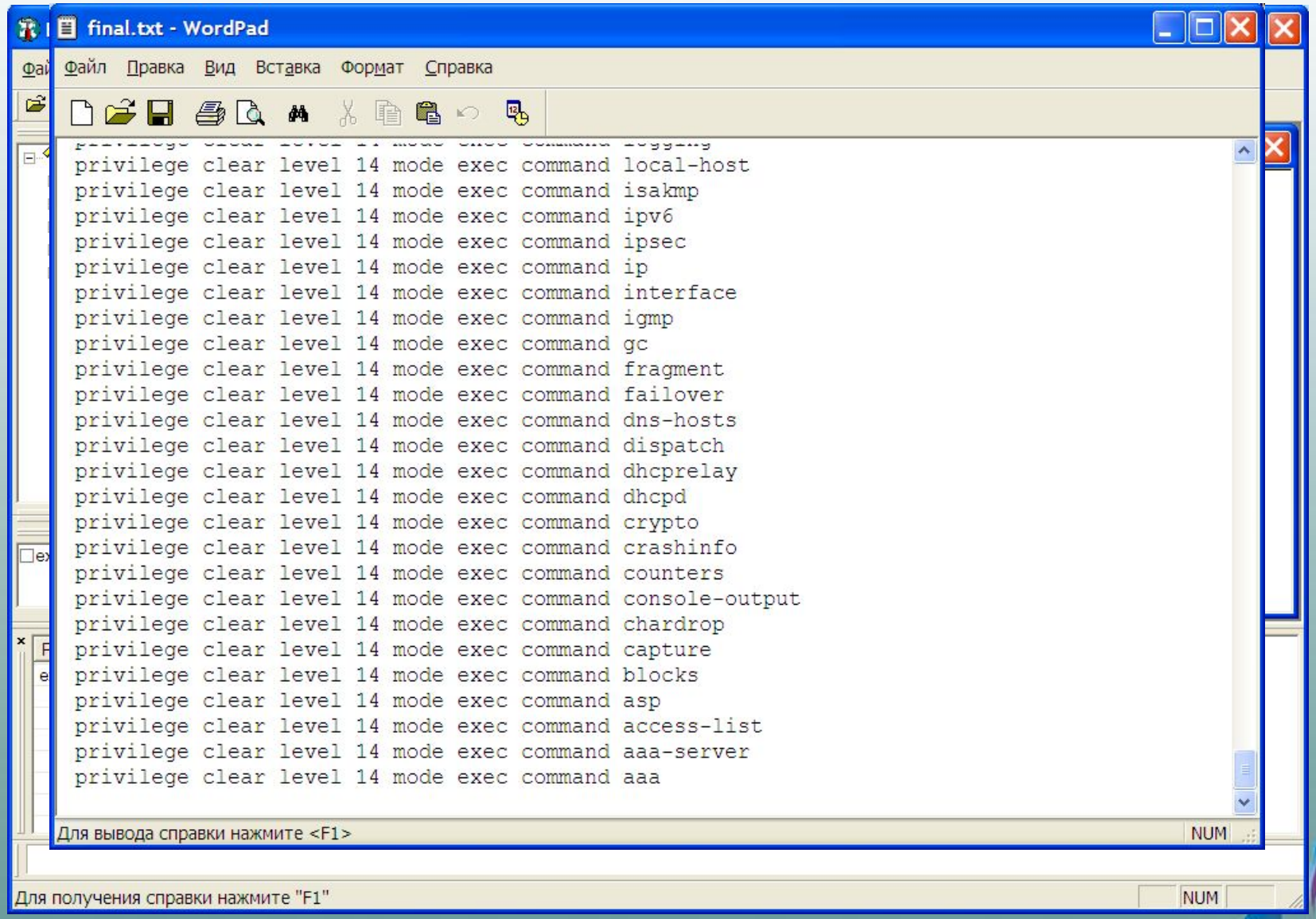


Если при изменении уровней привилегий были задействованы команды, которые переводят интерпретатор команд Cisco Pix в другой режим, после ~~дим~~ых отработки режима появится окно «Неотработанные режимы». Здесь нужно установить галочки напротив тех режимов, которые требуют дальнейшей обработки.

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

Создание файла конфигурации для МСЭ Cisco Pix

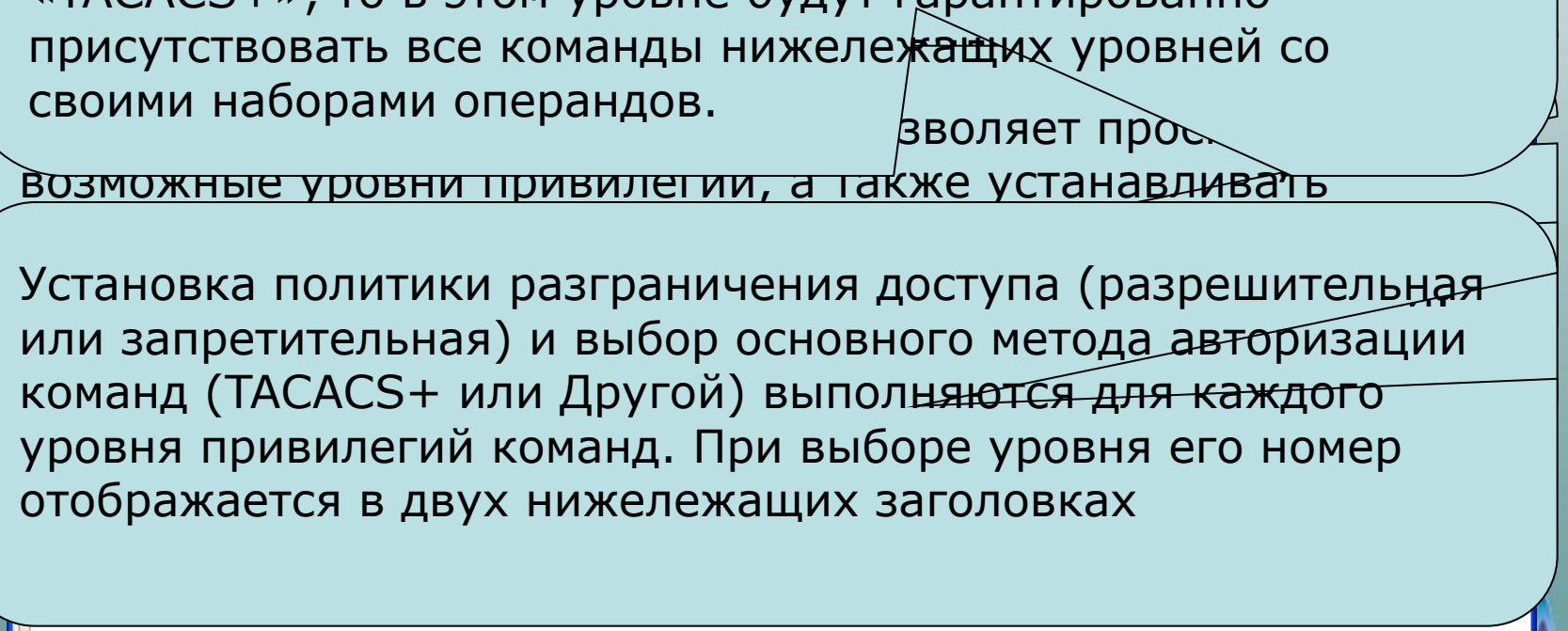
Создание файла конфигурации



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.



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

Создание файла конфигурации для сервера TACACS+

Просмотр конфигурации