МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**ACL**

Отчет по лабораторной работе № 8

по дисциплине «Компьютерные сети»

студента 2 курса группы ПИ-б-о-231(2)  
Аметов Кемран Ленверович

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2024

Теория

**ACL** (Access Control List) — это список правил, который используется для фильтрации трафика в сетевых устройствах, таких как маршрутизаторы и коммутаторы. ACL определяет, какой трафик разрешён или запрещён для прохождения через интерфейс устройства.

### Основные понятия

**Списки управления доступом** позволяют администратору:

* 1. Фильтровать пакеты по IP-адресам, портам, протоколам и другим критериям.
  2. Контролировать доступ к сети на основе определённых правил.
  3. Повышать уровень безопасности, ограничивая нежелательный трафик.

**Типы ACL**:

* 1. **Стандартные ACL**:
     1. Фильтруют только по IP-адресу источника.
     2. Могут использоваться для базового ограничения доступа.
     3. Пример: блокировать доступ из подсети 192.168.1.0/24.
  2. **Расширенные ACL**:
     1. Фильтруют по множеству параметров, таких как IP-адрес источника и назначения, порты, протоколы (TCP, UDP, ICMP и т. д.).
     2. Более гибкие и мощные.
     3. Пример: блокировать HTTP-трафик с определённого хоста.

**Именованные ACL**:

* 1. Вместо номеров используется имя для удобства управления.
  2. Пример: ip access-list extended BLOCK\_HTTP.

### Пример применения ACL

Стандартный ACL

access-list 1 deny 192.168.1.0 0.0.0.255

access-list 1 permit any

interface f0/0

ip access-group 1 in

Расширенный ACL

ip access-list extended BLOCK\_HTTP

deny tcp 192.168.1.0 0.0.0.255 any eq 80

permit ip any any

interface f0/0

ip access-group BLOCK\_HTTP in

### Где используются ACL?

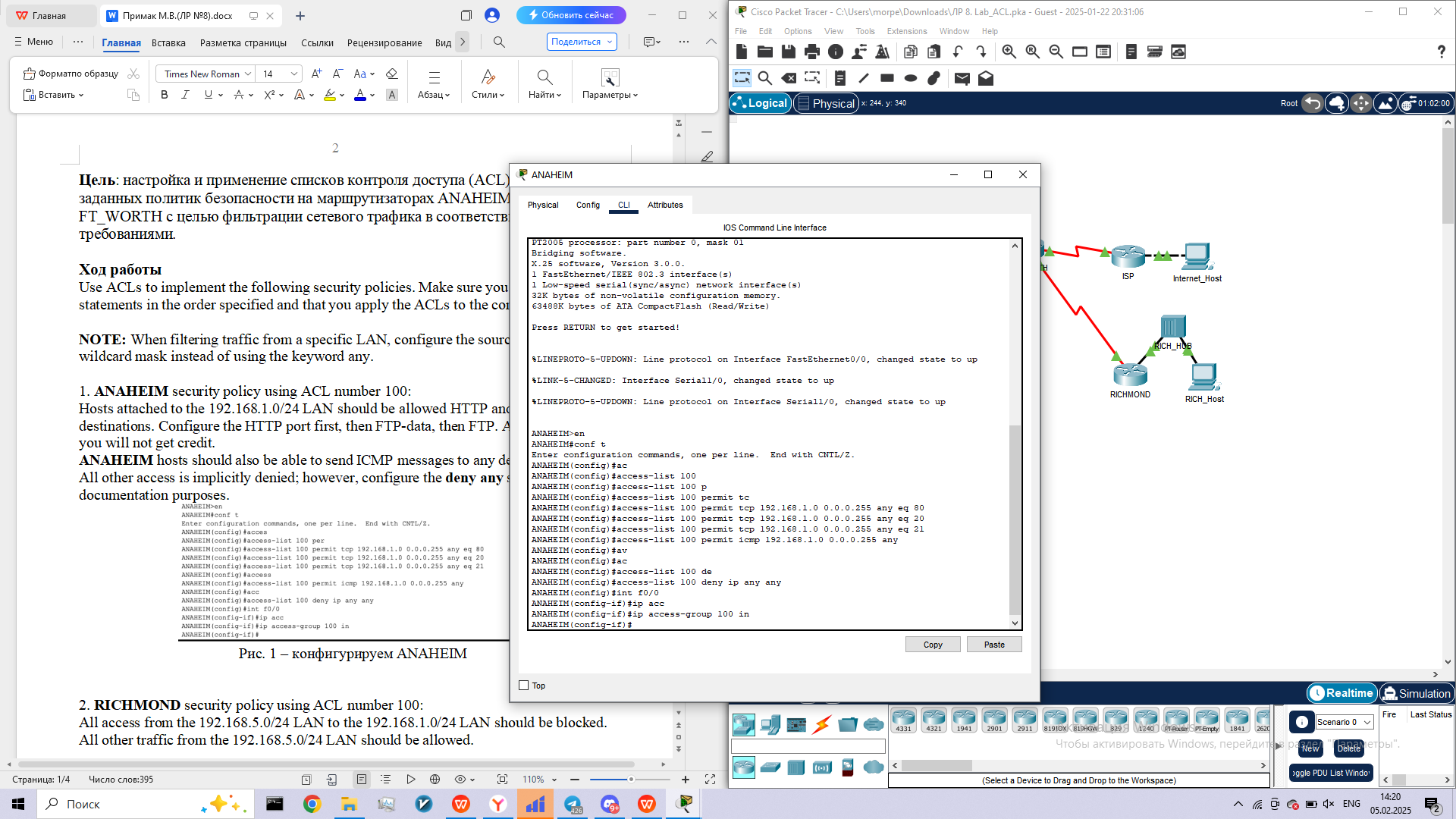
* **Фильтрация трафика**: Для ограничения доступа к определённым ресурсам.
* **NAT (перевод сетевых адресов)**: Чтобы указать, какие адреса переводить.
* **Маршрутизация**: Для контроля маршрутов (distribute lists).
* **QoS (Качество обслуживания)**: Для управления приоритетами трафика.

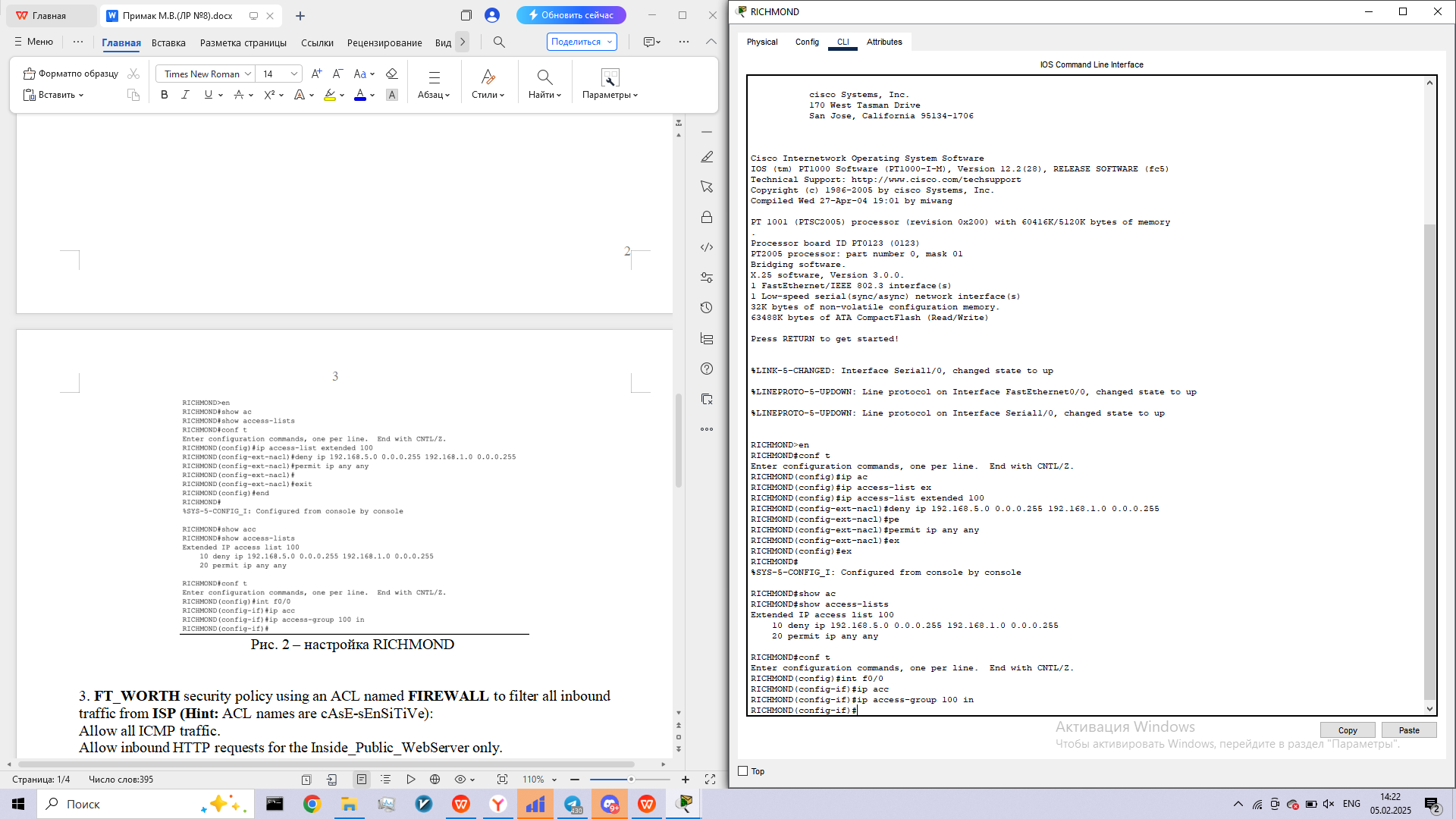
### Принципы работы ACL

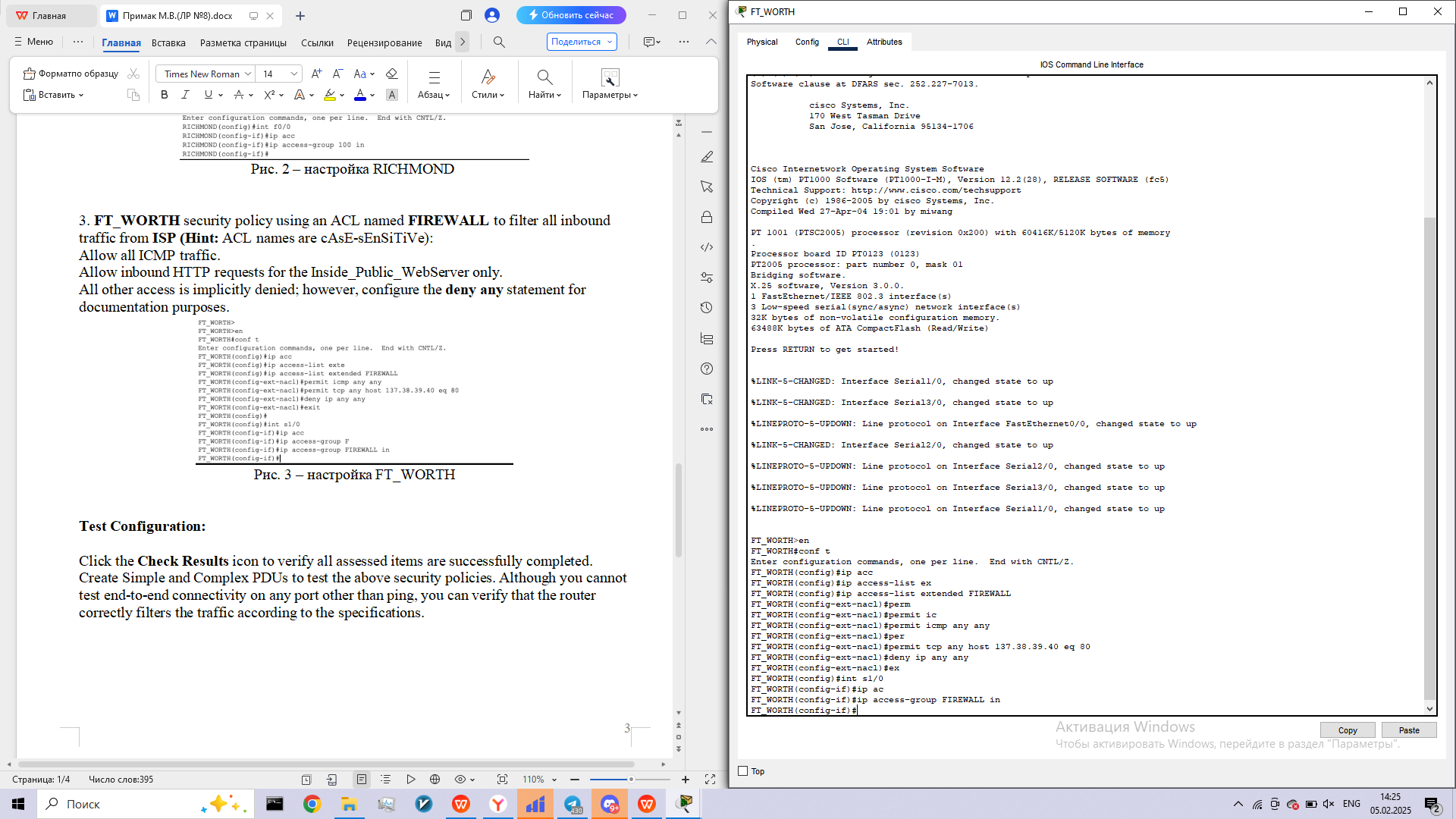
* Правила обрабатываются сверху вниз.
* Трафик проверяется до первого совпадения с правилом.
* Если ни одно правило не совпало, применяется **правило по умолчанию** — трафик блокируется.

ACL — мощный инструмент управления трафиком и обеспечения сетевой безопасности.

**Step 5 Configure Access Control Lists (ACLs)**  
  
Use ACLs to implement the following security policies. Make sure you enter the statements in the order specified and that you apply the ACLs to the correct interface.  
  
**NOTE:**When filtering traffic from a specific LAN, configure the source network and wildcard mask instead of using the keyword any.  
  
1. **ANAHEIM** security policy using ACL number 100:  
Hosts attached to the 192.168.1.0/24 LAN should be allowed HTTP and FTP access to all destinations. Configure the HTTP port first, then FTP-data, then FTP. Any other order and you will not get credit.  
**ANAHEIM** hosts should also be able to send ICMP messages to any destination.  
All other access is implicitly denied; however, configure the **deny any** statement for documentation purposes.

  
2. **RICHMOND**security policy using ACL number 100:  
All access from the 192.168.5.0/24 LAN to the 192.168.1.0/24 LAN should be blocked.  
All other traffic from the 192.168.5.0/24 LAN should be allowed.

  
  
3. **FT\_WORTH**security policy using an ACL named **FIREWALL** to filter all inbound traffic from **ISP (Hint:**ACL names are cAsE-sEnSiTiVe):  
Allow all ICMP traffic.  
Allow inbound HTTP requests for the Inside\_Public\_WebServer only.  
All other access is implicitly denied; however, configure the **deny any** statement for documentation purposes.

  
  
**Test Configuration:**  
  
Click the **Check Results** icon to verify all assessed items are successfully completed. Create Simple and Complex PDUs to test the above security policies. Although you cannot test end-to-end connectivity on any port other than ping, you can verify that the router correctly filters the traffic according to the specifications.