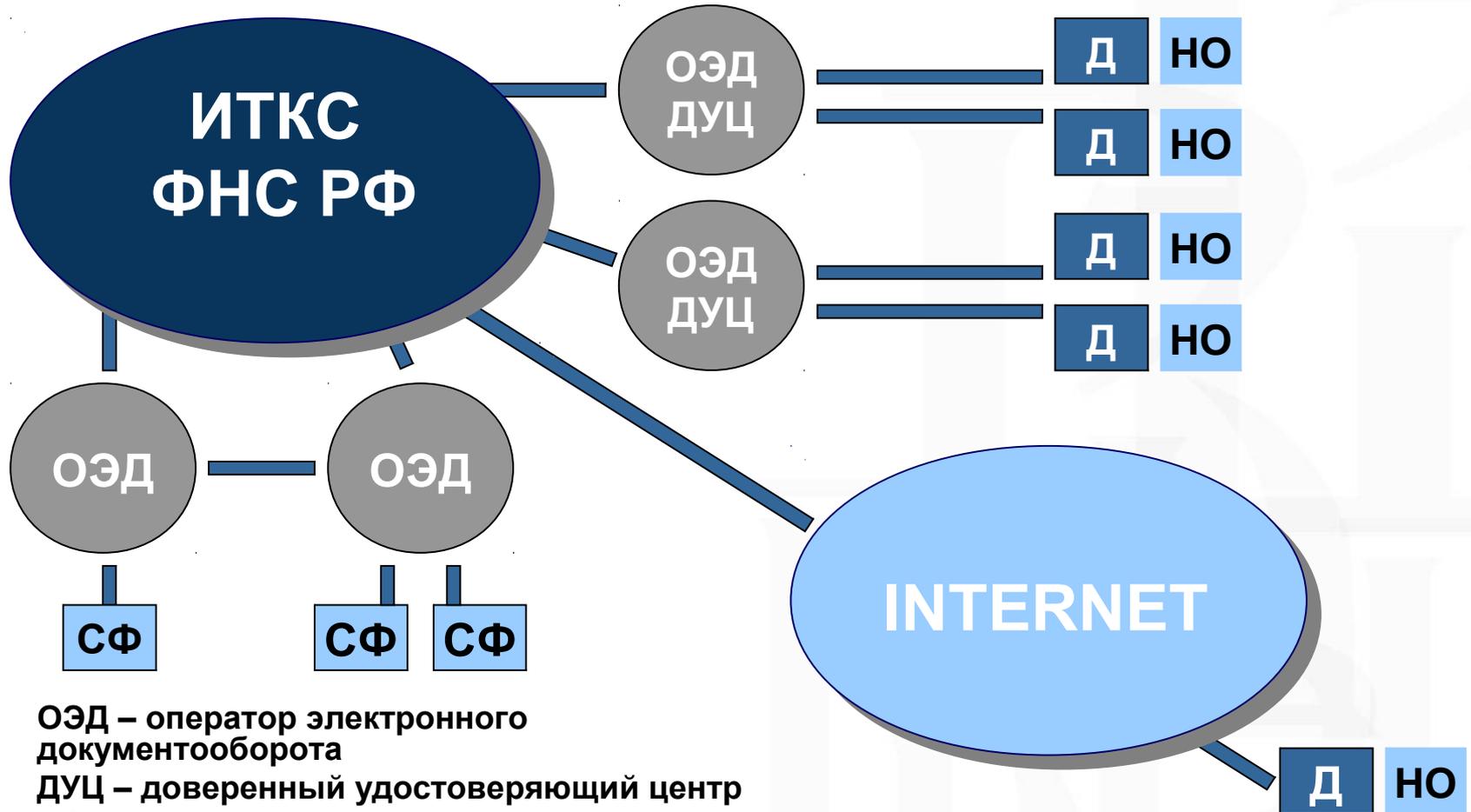
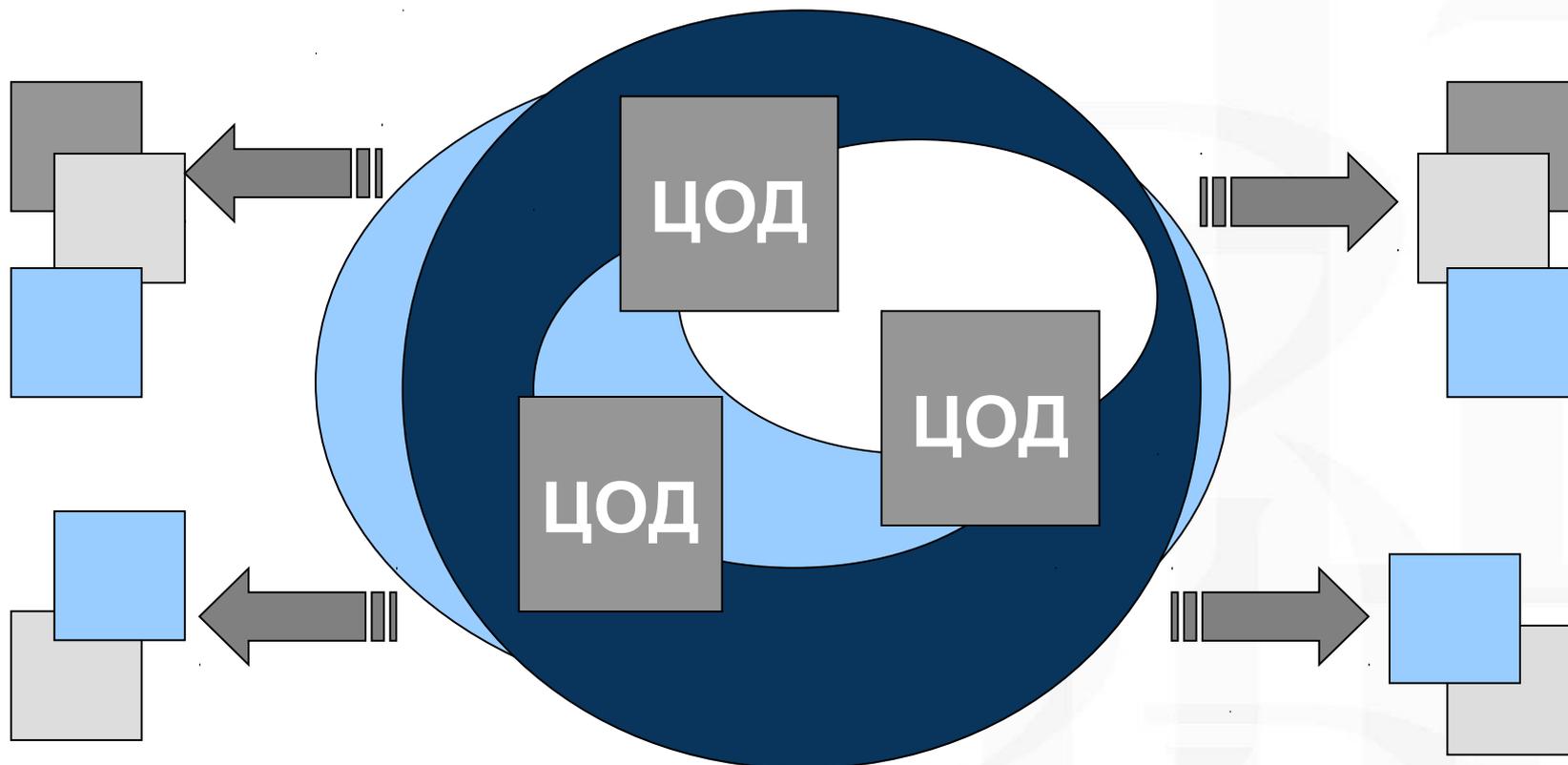


# **ПРИМЕНЕНИЕ АПОСТЕРИОРНОЙ ЗАЩИТЫ В СИСТЕМЕ НАЛОГОВЫХ ОРГАНОВ**

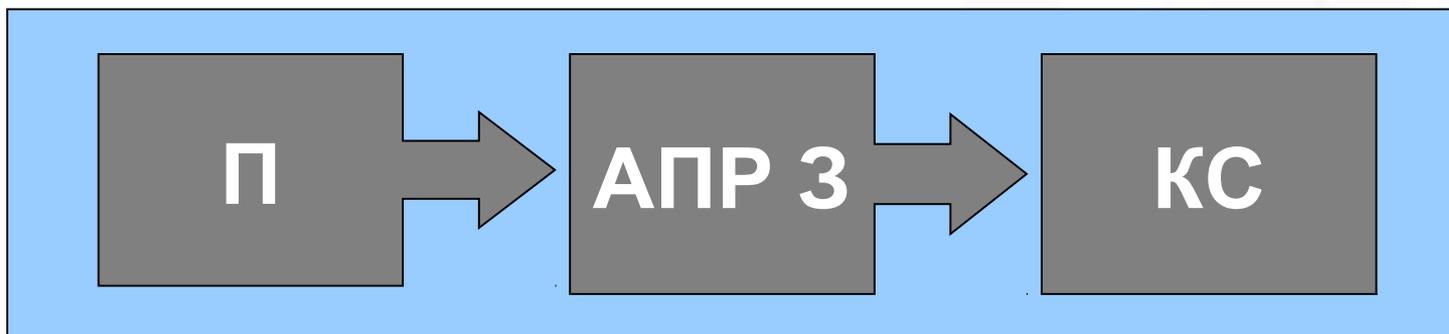
# СИСТЕМА «НАЛОГ»





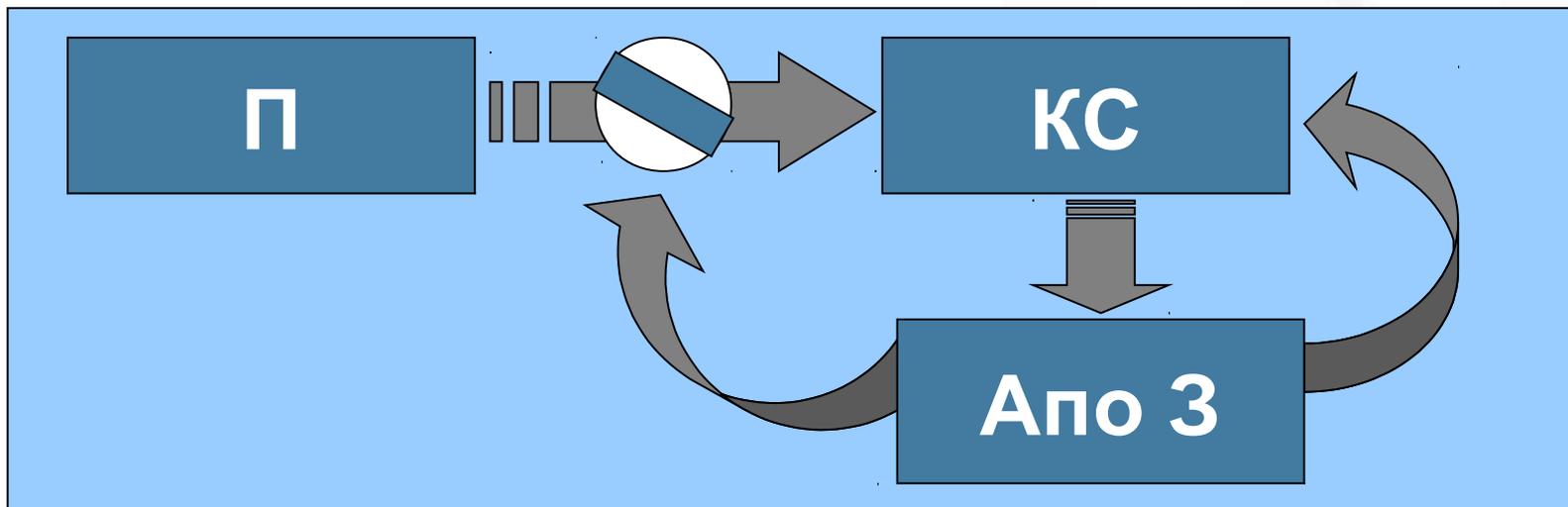
**120 тысяч рабочих мест  
сотрудников территориальных органов и ЦА**

- **Априорная защита – доступ после определения легитимности пользователя (процесса)**



- **Преимущество: высокая защищенность «Налог» - 1 Г по ФСТЭК России**
- **Недостатки: зависимость ППО и Апр 3**

- Апо 3 – доступ на основе штатных средств или элементов Апр 3
- Апо 3 - мониторинг и фиксация действий в компьютерной системе
- Преимущества: независимость ППО и ОС от Апо 3
- Недостаток: принятие мер к нарушителю после совершения инцидента, необходимость защищенности журнала действий





# ТРЕБОВАНИЯ ФСТЭК



**Требования  
руководящих  
документов  
ФСТЭК  
России**

Доверенная операционная среда

Обеспечение целостности и контроль  
соблюдения политик безопасности

Регистрация политик в системе и  
учет действий субъектов с информацией

Идентификация и аутентификация  
субъектов доступом управление  
доступом к объектам

Реализация функции сетевой  
безопасности

|   |   |  |
|---|---|--|
| <p>Технологическая компонента защиты виртуальных средств</p>  | <p>Trendmicro / Deep Security<br/>Код безопасности<br/>/ Vgate / Апр 3/</p> | <p>Защита оборудования виртуализаторов. В случае закупки новых серверов/ процессоров для ФХД АИС «Налог-3» потребуется дозакупка</p>           |
| <p>Подсистема выявления и предотвращения утечек</p>   | <p>Инфовотч<br/>/ Inforwatch Trafe Monitor,<br/>Device Monitor / Апр 3/</p> | <p>Мониторинг и анализ данных отправляемых за пределы сети, в тыс. съемных носителей, состояния PC</p>   |
| <p>Подсистема регистрации учета и формирования отчетности</p>   | <p>HP/Aresight<br/>/ Апо 3 /</p>  | <p>Сбор событий ИБ от АИС «Налог-3». Оценка проведена в соответствии с источниками событий безопасности, определенными на сегодняшний день</p> |
| <p>Подсистема управления электронными ключами<br/>Подсистема управления идентификационной информацией</p> | <p>Аванпост / ПК<br/>«Avanpost»<br/>/ Апр 3 /</p>                           | <p>Обеспечение управления электронными ключами пользователей и учетными записями. В 2015 г. – безлимитная лицензия</p>                         |
| <p>Имеющиеся компоненты</p>   | <p>/ Апр 3 /</p>  | <p>Шифрование трафика</p>  |

- Облегчать априорную защиту
- Сохранять защиту системы мониторинга
- Развивать аналитическую часть мониторинга