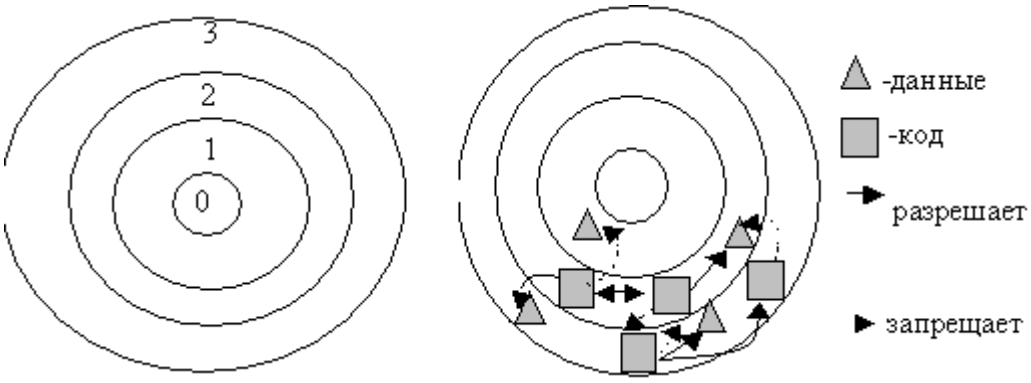
В ЭВМ для целей защиты предусматриваются как минимум два режима работы:

- системный режим (режим супервизора, Superevisor) - программам доступны все ресурсы системы.
- пользовательский режим (User). программам запрещается выполнение некоторых команд, влияющих на общесистемные ресурсы (т.н. привилегированные команды).

В архитектуре x86 этот принцип реализуется через поддержку 4-х уровней привилегий – PL.



DPL (двухбитное поле уровня привилегий дескриптора системных объектов) - определяет, каким программам разрешен доступ к описываемому им объекту.
CPL (текущий уровень привилегий) - уровень привилегий выполняющегося в данный момент сегмента кода.
IOPL - поле (2 бит) в регистре EFLAGS
RPL (запрашиваемый уровень привилегий)

Программам не разрешается доступ к данным, которые имеют более высокий уровень привилегий.

Привилегированные команды:

- Команды, воздействующие на механизм сегментации и защиты (выполняются только в нулевом кольце)
- команды, которые изменяют состояние флажка прерываний IF и проводят ввод–вывод (требуется, чтобы CPL ≤ IOPL.)

Защита доступа к данным:

Процессор не разрешает обращаться к данным, которые более привилегированны, чем выполняемая программа. Основное правило защиты CPL ≤ DPL.

Защита сегментов кода:

x86 запрещает передачу управления сегменту кода, находящемуся на другом уровне привилегий, тем самым предотвращая произвольное изменение уровня привилегий.

Передача управления между уровнями привилегий:

- Подчиненные сегменты кода (с ними не ассоциируется конкретный уровень привилегий, т.к. они подчиняются уровню привилегий того кода, который передает управление с помощью команд CALL или JMP. Значение DPL дескриптора подчиненного сегмента кода ≤ CPL, т.е. передача управления разрешается только во внутренне более защищенные кольца)
- Шлюзы вызова (дескриптор шлюза вызова действует как посредник между сегментами кода, находящимися на различных уровнях привилегий. Шлюзы вызова идентифицируют разрешенные точки в более привилегированном коде, которым может быть передано управление, и являются единственным средством смены уровня привилегий).

Одно из правил защиты по привилегиям требует, чтобы уровень привилегий стека всегда был равен уровню CPL. Чтобы не нарушать это правило процессор x86 при смене уровня привилегий автоматически переключает и стек для соответствия новому, более привилегированному коду.