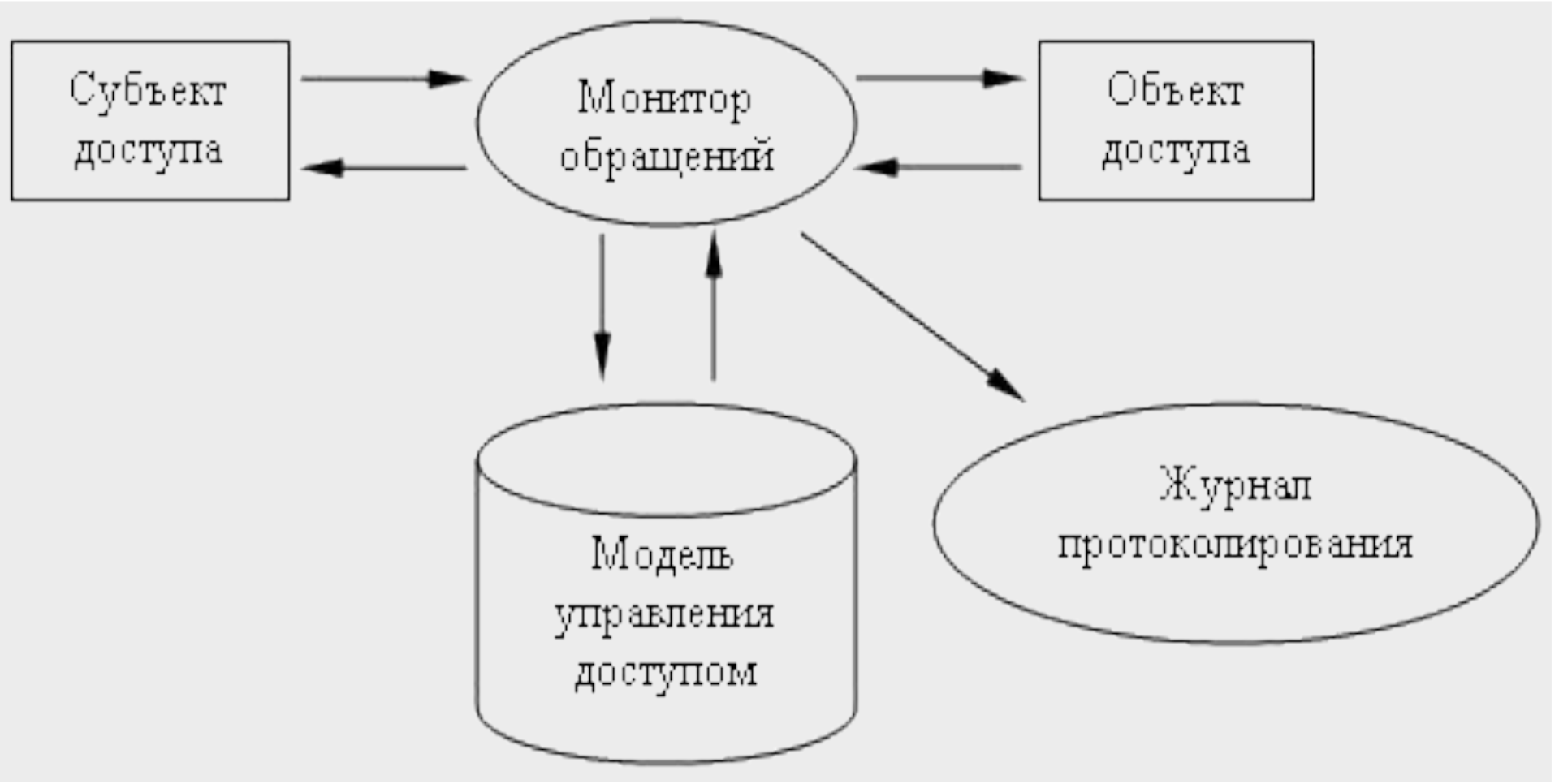
Тема: Модель системы защиты информации

- При разработке современных АС используется один из двух методов:
- **Нисходящий метод** (сверху вниз). Сначала составляется общее описание системы, выделяются компоненты системы, поэтапно увеличивается степень детализации компонентов системы (выделение компонентов в компонентах) до момента окончания разработки.
- **Восходящий метод** (снизу вверх). Сначала формируется задача системы, затем разрабатывается некоторый набор элементарных функций. На базе элементарных функций разрабатываются более крупные компоненты системы, и так, поэтапно разработка ведется до момента объединения отдельных компонентов в единую систему.


Неформальная разработка
Требования безопасности
(демонстрация)
Функциональная спецификация
(тестирование)
Реализация
Формальная разработка
Требования безопасности
Абстрактная модель
(доказательство)
Формальная спецификация
(тестирование)
Требования безопасности

- При создании программно-аппаратных средств защиты, руководствуются следующими принципами:
- **Принцип обоснованности доступа**.
- **Принцип достаточной глубины контроля доступа**.
- **Принцип разграничения потоков информации**.
- **Принцип персональной ответственности**.
- **Принцип целостности средств защиты**.

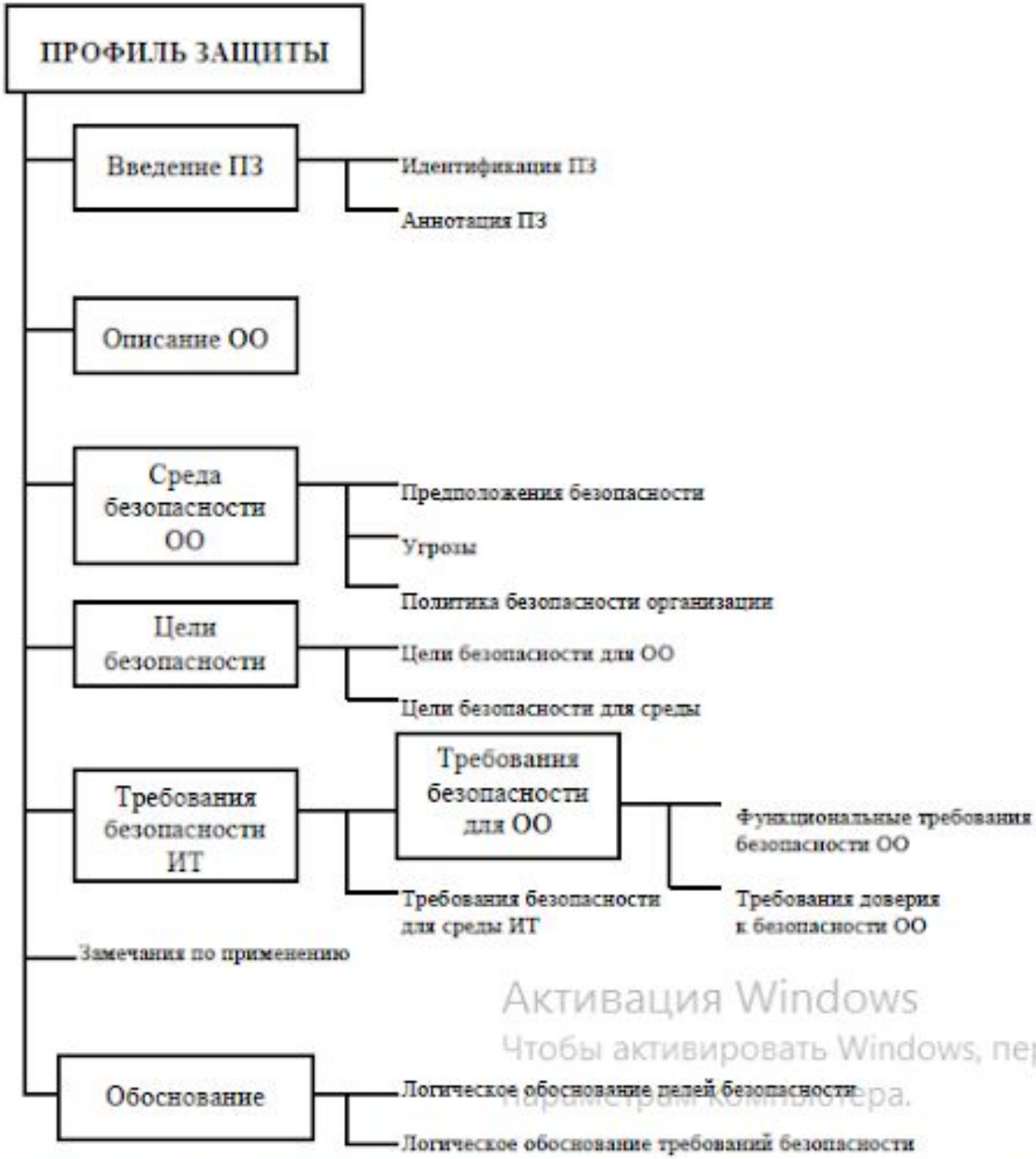
- Средства защиты должны точно выполнять свои функции и быть изолированы от пользователя. Все средства защиты должны выполняться в виде отдельного модуля, и называется он "монитор обращения".

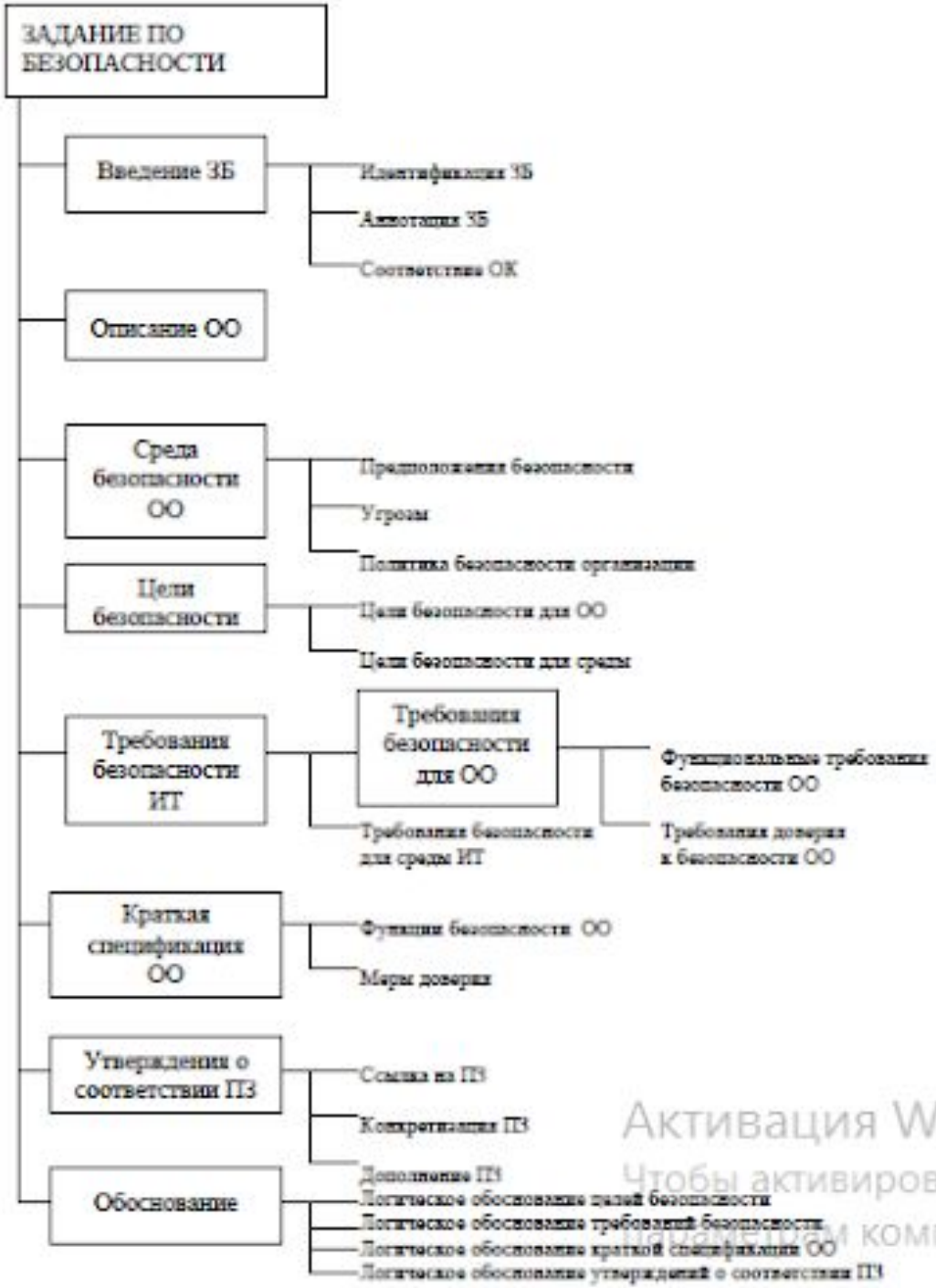


- Для построения монитора обращений необходимо выполнить следующие требования:Монитор обращений должен быть защищен от постороннего вмешательства в его работу, включая несанкционированную подмену и модификацию.
- Монитор обращений должен всегда присутствовать и работать надлежащим образом .
- Монитор обращений должен быть компактен и удобен для проведения анализа и тестирования.

- Концепция монитора безопасности обращений является достаточно естественной формализацией некого механизма, реализующего разграничение доступа в системе. Монитор безопасности обращений (МБО) [3] представляет собой фильтр, который разрешает или запрещает доступ, основываясь на установленных в системе правилах

- Монитор безопасности обращений удовлетворяет следующим **свойствам**:
- Ни один запрос на доступ субъекта к объекту не должен выполняться в обход МБО.
- Работа МБО должна быть защищена от постороннего вмешательства.
- Представление МБО должно быть достаточно простым для возможности верификации корректности его работы.





- Британский стандарт ***BS 7799-3:2006 “Information security management systems –Part 3: Guidelines for information security risk management”*** (Системы управления информационной безопасностью – Часть 3: руководство по управлению рисками в информационной безопасности) пока не имеет международного статуса, однако рассматривается возможность его принятия в качестве стандарта ISO.
- Стандарт представляет собой набор руководств и рекомендаций, направленных на удовлетворение требований стандарта ISO/IEC 27001:2005 в части управления рисками, которое рассматривается как непрерывный четырёхфазный процесс

Рис. 3.5.4. Модель управления рисками


Стандарты в области ИБ
Оценочные стандарты
Спецификации
Предназначены для оценки и классификации автоматизированных систем и средств защиты информации по требованиям безопасности
«Оранжевая книга»
РД Гостехкомиссии России
«Общие критерии»
Регламентируют различные аспекты реализации и использования средств и методов защить
X.509 – инфраструктура открытых ключей
ГОСТ 28147-89 - симметричный криптографический алгоритм
Управленческие стандарты (ISO 17799, ISO 27001 и др.)