

Децентрализованная система разграничения доступа

Чадов А.Ю.,
Аспирант МФТИ

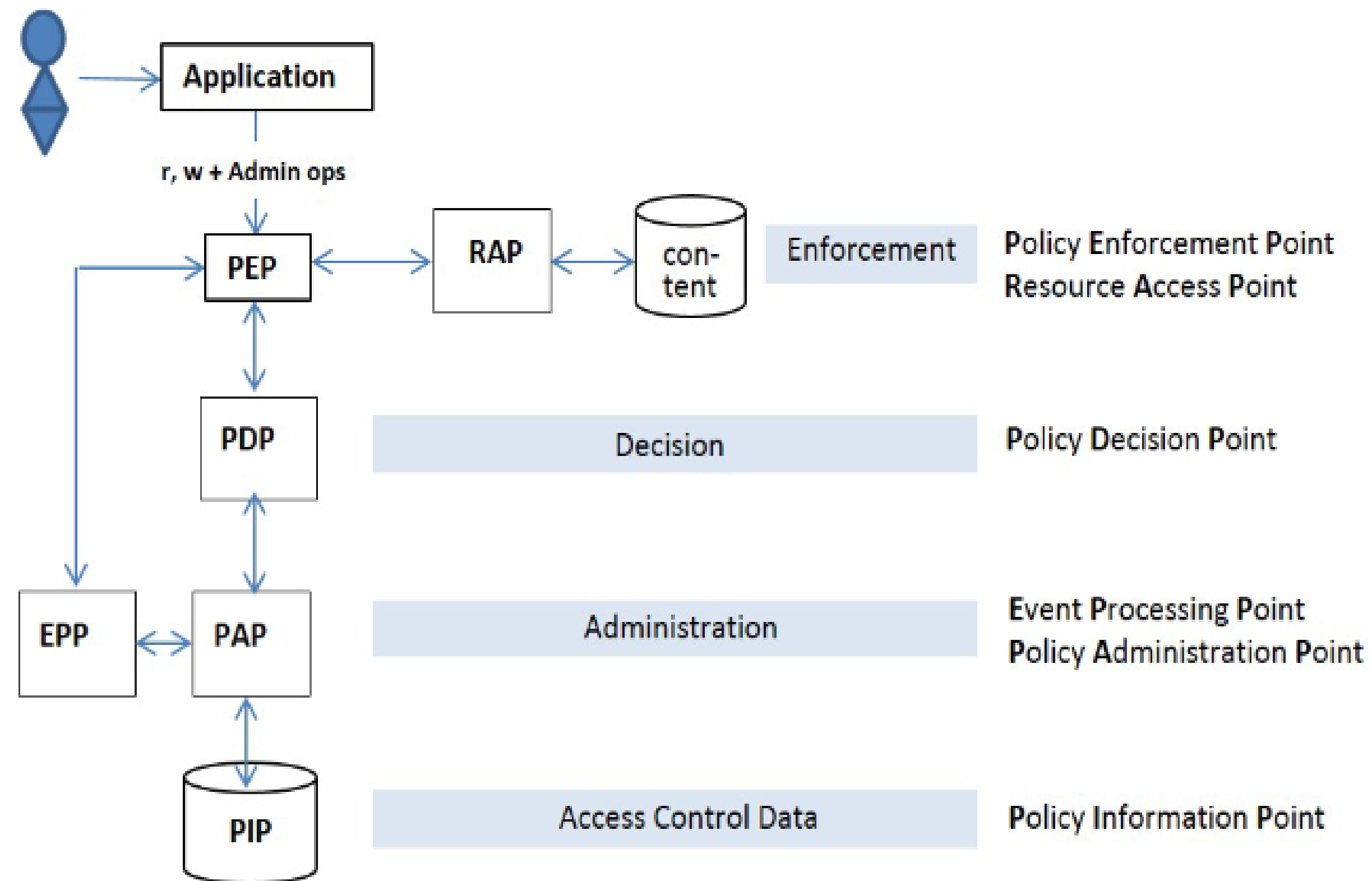
НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ ПРОДУКТЫ

- Secret Net («Код Безопасности»): степень охвата рынка – 52%
- «Аккорд» (ОКБ САПР): степень охвата рынка – 25,8%
- Dallas Lock («Конфидент»): степень охвата рынка – 5,8 %

ПОДХОДЫ К РАЗГРАНИЧЕНИЮ ДОСТУПА

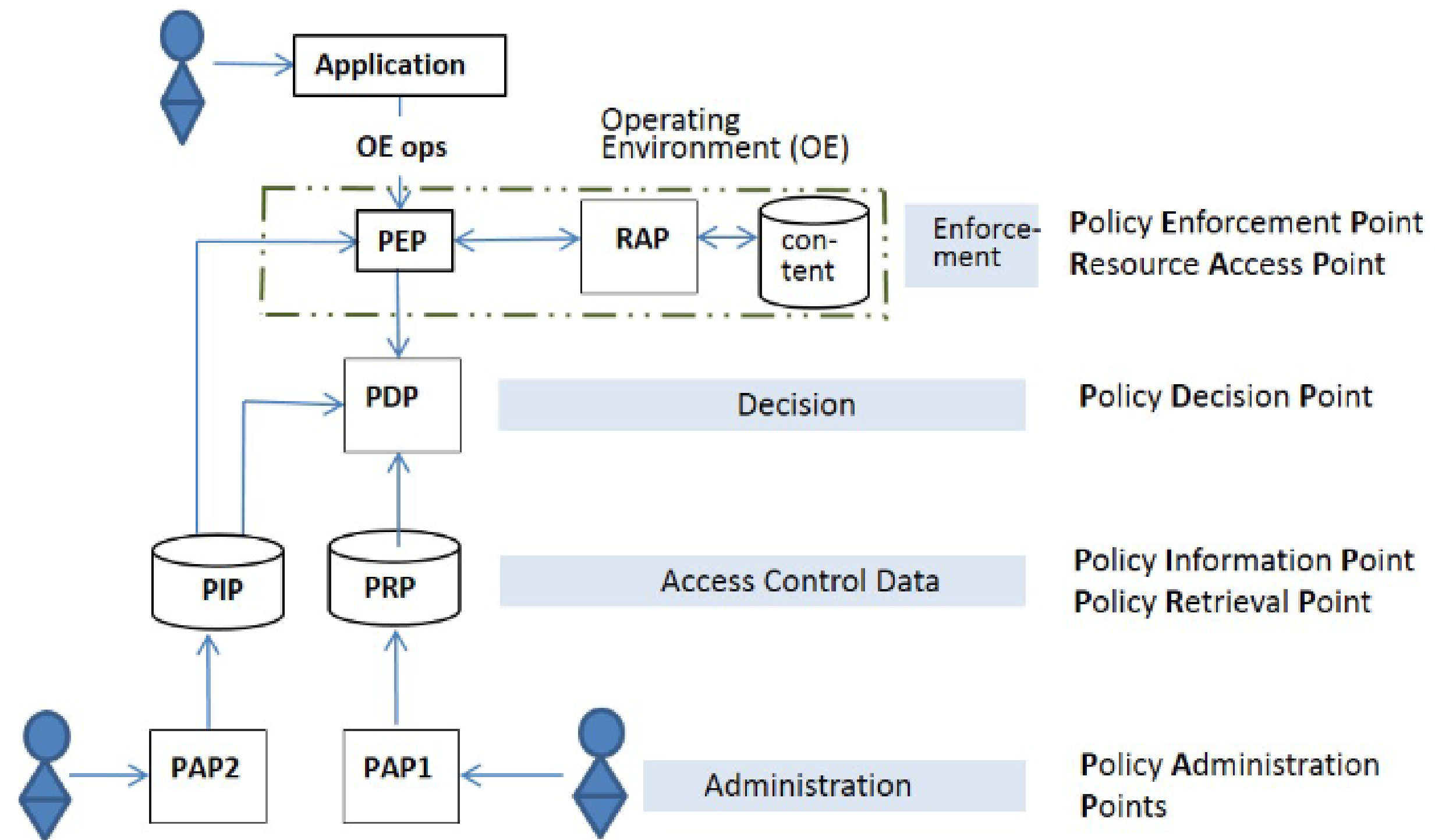
- RBAC (Role-Based Access Control) – подход к разграничению доступа на основе ролей
- ABAC (Attribute-Based Access Control) – подход к разграничению доступа на основе атрибутов

АРХИТЕКТУРА СИСТЕМЫ ДЛЯ СТАНДАРТОВ NGAC И XACML






Функциональная архитектура NGAC

АРХИТЕКТУРА СИСТЕМЫ ДЛЯ СТАНДАРТОВ NGAC И XACML



Функциональная архитектура XACML



-  Запросы на чтение и запись в базу данных политик.
-  Запрос на чтение из базы данных политик.
-  Запросы на разрешение доступа субъекта к объекту.

СПИСОК ТРЕБОВАНИЙ

1. Система должна состоять из отдельных модулей.
2. Решения о доступе принимает центральный модуль.
3. Задержка, вносимая работой системы должна быть того же порядка, что и время обращения к диску или меньше.
4. Модули должны уметь проводить взаимную аутентификацию.
5. Данные, передаваемые в запросах модулей друг к другу должны быть защищены.