ASTRALINUX®

Мандатные управление доступом и контроль целостности при разработке сетевых сервисов в среде ОССН Astra Linux Special Edition

Инженер-программист «РусБИТех-Астра»
Шишов Максим Николаевич

Актуальность

Постановление Правительства России от 16.11.15 № 1236

Об установлении запрета на допуск иностранного программного обеспечения при закупках для государственных и муниципальных нужд

Приказ Минкомсвязи России от 29.06.17 № 334

Об утверждении методических рекомендаций по переходу федеральных органов исполнительной власти государственных внебюджетных фондов на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения

md.mos.ru — сайт государственных услуг «Мои документы»

pfrf.ru — сайт пенсионного фонда России

nalog.ru — сайт федеральной налоговой службы

Правила применения мандатных управления доступом и контроля целостности

Операция записи	Операция чтения	Операция исполнения
$L_{субъекта} == L_{объекта}$ $C_{субъекта} == C_{объекта}$ $iL_{субъекта} >= iL_{объекта}$	$L_{субъекта} >= L_{объекта}$ $C_{субъекта} >= C_{объекта}$ $\forall iL_{субъекта}$; $\forall iL_{объекта}$	$L_{субъекта} >= L_{объекта}$ $C_{субъекта} >= C_{объекта}$ $iL_{субъекта} <= iL_{объекта}$

где L — уровень конфиденциальности, iL — уровень целостности, C — категории

Мандатная метка определяется **уровнем целостности** (категориями целостности) и **классификационной меткой** (определяется уровнем и категориями). **Категории** представлены в виде разрядов битовой маски.

Инженерные задачи, связанные с реализацией разграничения доступа

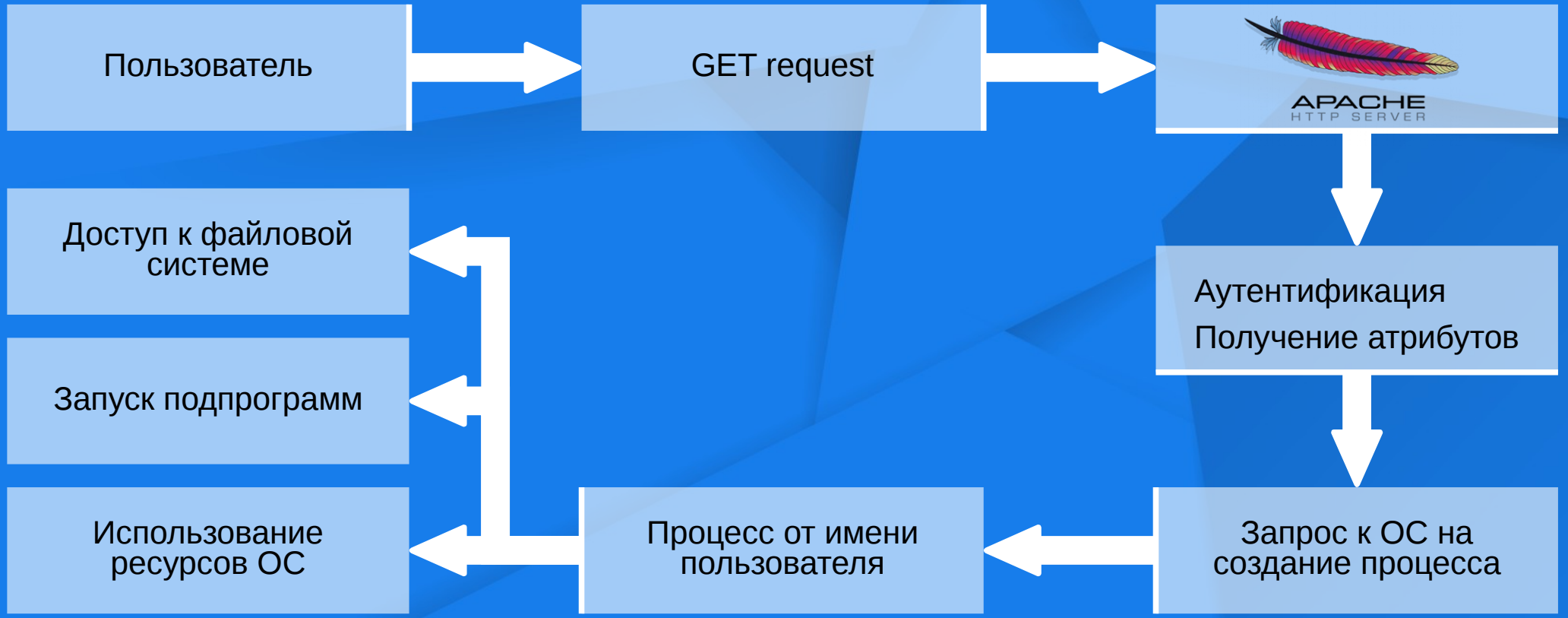
Файловая система	Программные процессы	Оперативная память
Файлы — объекты защиты. Каталоги — контейнеры для объектов. Символьные ссылки — имеют смешанное поведение.	Процессы операционной системы являются субъектами защиты информации.	Оперативная память — отдельное для каждого процесса хранилище оперативной информации.

Инфраструктура операционной системы

Проекты, использующиеся в среде ОССН ASTRA LINUX

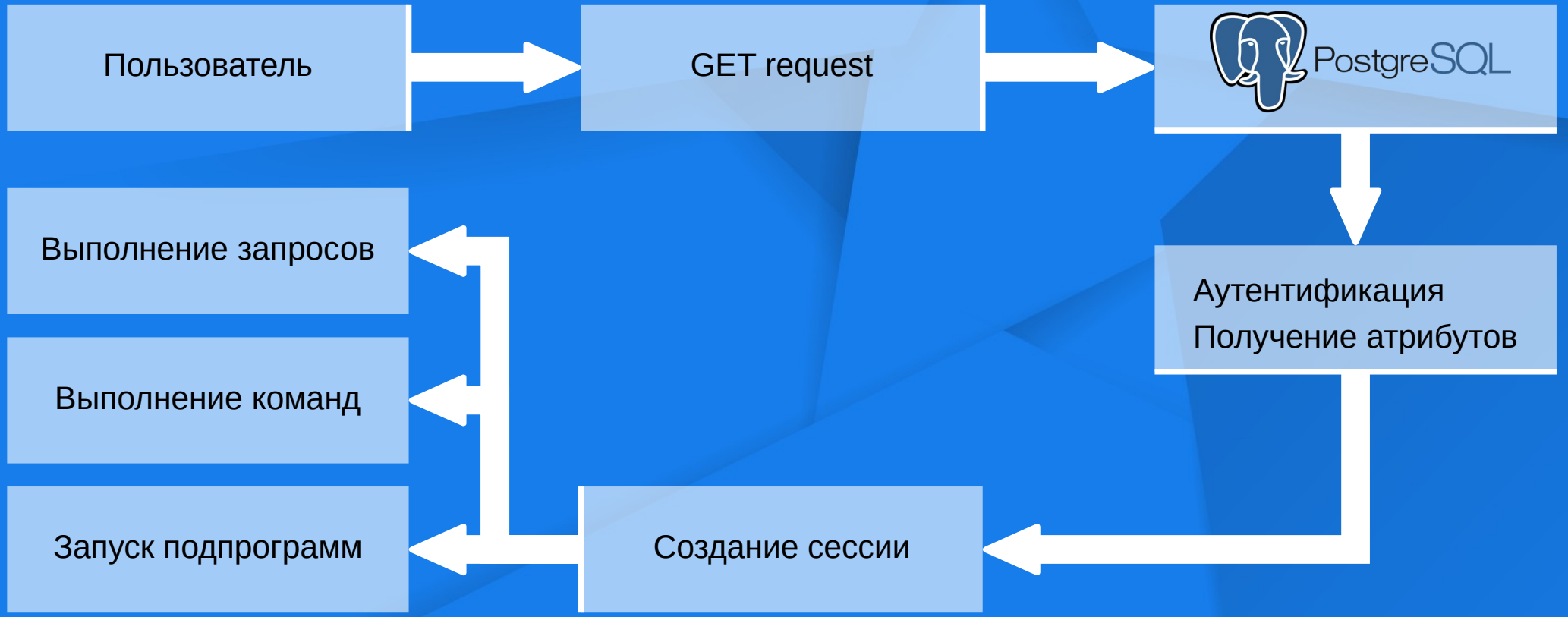
- Гибкость за счет модульности
- Открытый исходный код
- Популярность и распространенность

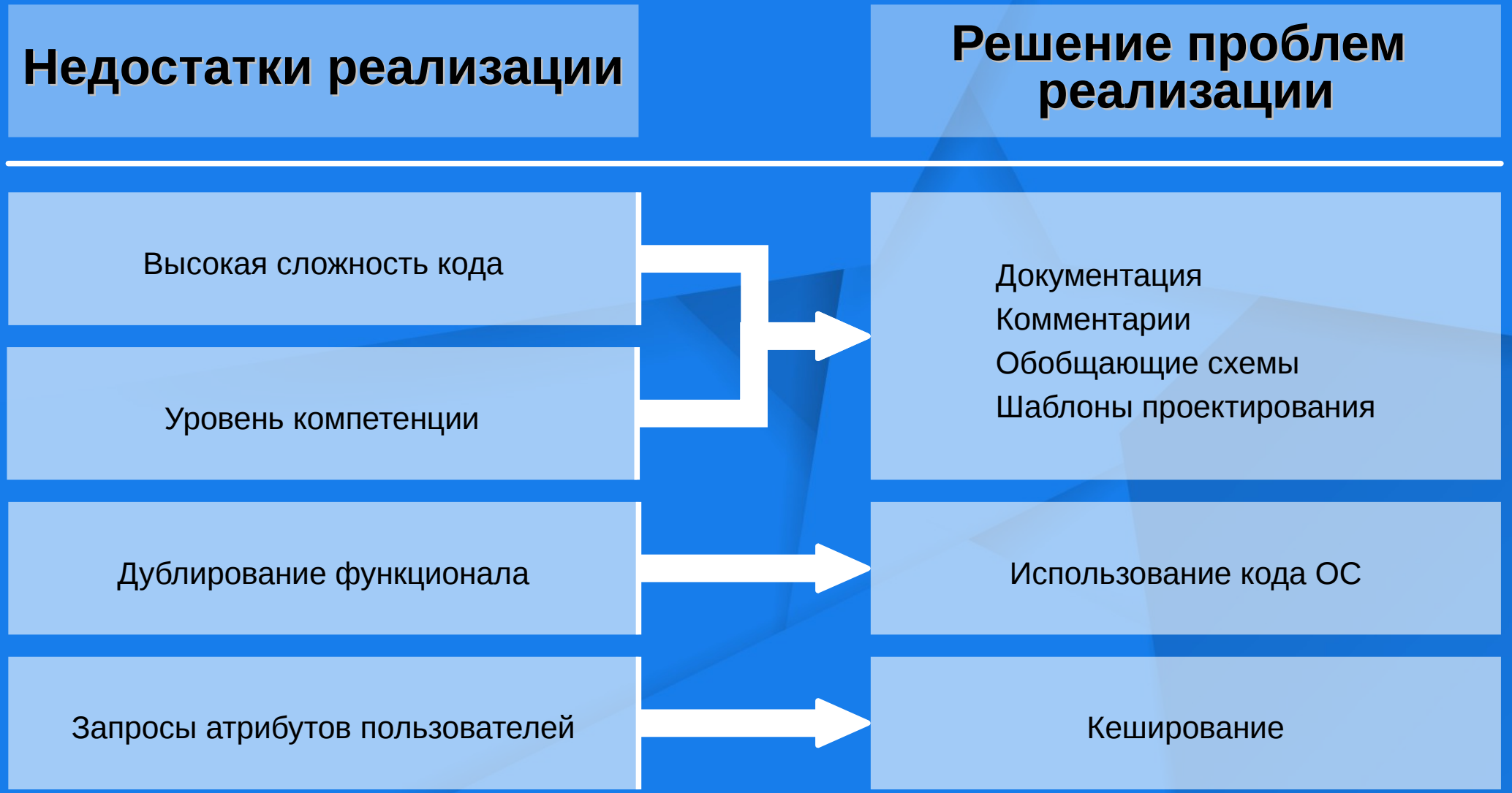
Реализация разграничения доступа вэб-сервера



Недостатки реализации	Решение проблем реализации
Потребление оперативной памяти	Пулер единого мандатного уровня
Переключение контекста	
Повышенная нагрузка на процессор	
Запросы атрибутов пользователей	Кеширование

Реализация разграничения доступа СУБД




Недостатки реализации
Решение проблем реализации
Высокая сложность кода
Уровень компетенции
Документация
Комментарии
Обобщающие схемы
Шаблоны проектирования
Дублирование функционала
Использование кода ОС
Запросы атрибутов пользователей
Кеширование

Выводы

Потребление оперативной памяти

Дублирование функционала

Переключение контекста

Уровень компетенции

Повышенная нагрузка на процессор

ASTRALINUX®

Спасибо за внимание