

ПРОБЛЕМЫ УПРАВЛЕНИЯ ПРАВАМИ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ КРУПНОЙ ТОРГОВОЙ СЕТИ

Вячеслав Муравлев

Архитектор решений, группа компаний CUSTIS

Технологии безопасности

8 февраля 2017 года

УТЕЧКИ ИНФОРМАЦИИ

По данным InfoWatch за 2016 год

- | Большая доля утечек информации (67%) произошла по вине внутренних нарушителей
- | Более половины утечек (69%) возникло по вине сотрудников (как бывших, так и настоящих) и подрядчиков



ОСОБЕННОСТИ ИТ-ЛАНДШАФТА КРУПНОГО ПРЕДПРИЯТИЯ

- | Есть множество **информационных систем** и **пользователей**: сотрудников, подрядчиков, клиентов
- | Сквозные бизнес-процессы проходят через **несколько информационных систем**
- | Пользователи работают в **различных** ИТ-системах и выполняют в них **разные** функции
- | В каждой информационной системе есть **свои настройки прав доступа** и **своя процедура аутентификации**

АКТУАЛЬНОСТЬ ТЕМЫ ДЛЯ РИТЕЙЛА

| Высокая текучка персонала

- По различным данным – до 100%

| Интенсивное перемещение сотрудников

- Рост количества магазинов и складов
- Перемещение в служебной иерархии

| Большое число внешних пользователей ИТ-систем

- Поставщики товаров и поставщики услуг: транспортные компании, службы доставки и др.

| Географическая распределенность сети

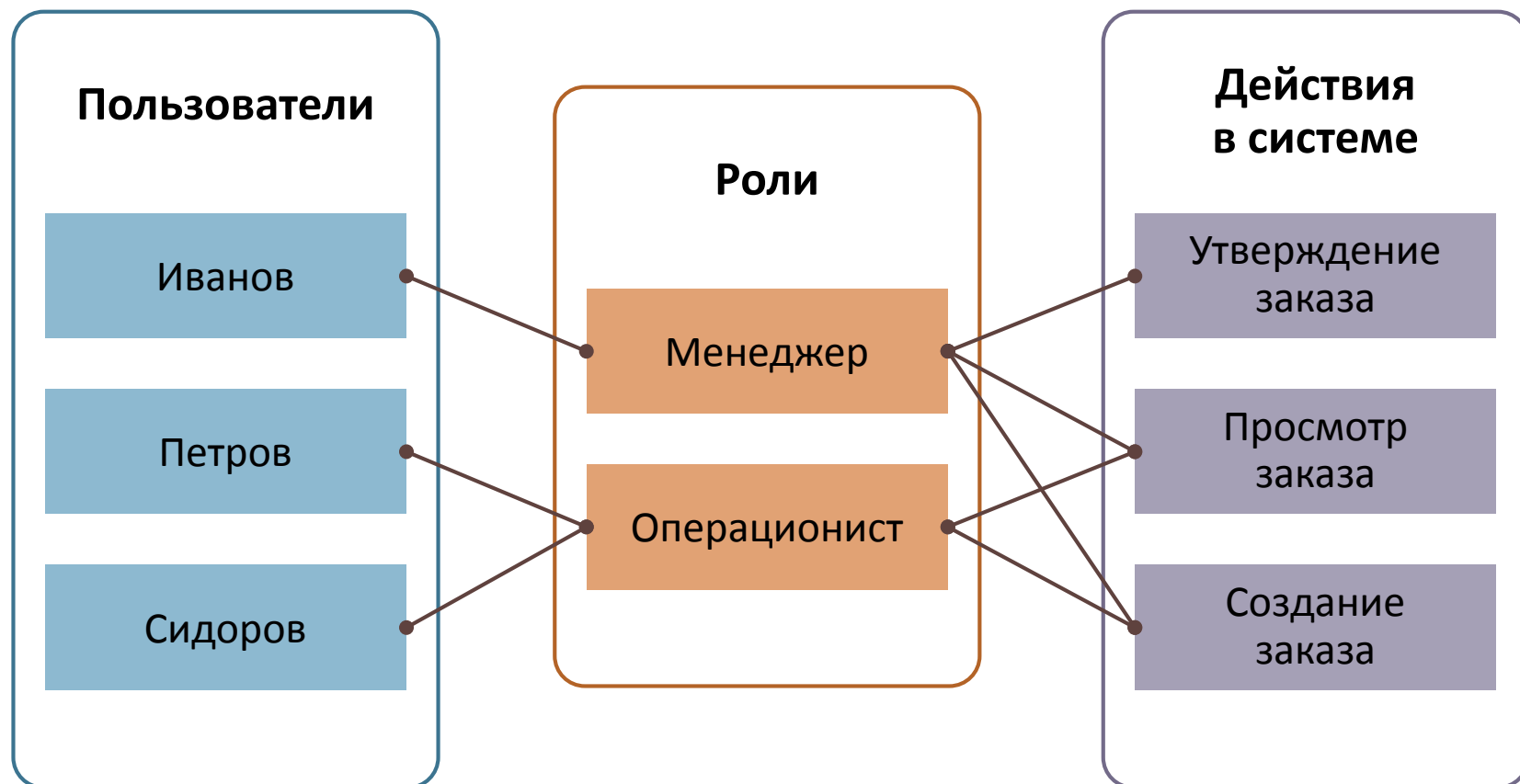
- Разные часовые пояса и страны присутствия

| Необходимость гибкого разграничения доступа при централизации данных

ЦЕЛИ УПРАВЛЕНИЯ ПРАВАМИ ДОСТУПА

- | **Снижение рисков**, связанных с неправомерной или несвоевременной выдачей или отзывом прав доступа пользователей
- | **Снижение стоимости** управления правами доступа
- | **Повышение оперативности** управления правами
 - Быстрая выдача временных прав
 - Минимальное время настройки прав
 - Минимальное время ожидания пользователя

РОЛЕВАЯ МОДЕЛЬ ДОСТУПА (RBAC)



БОЛЕЗНИ РОСТА RBAC

| Модель **не учитывает**:

- Контекст действий пользователей
- Атрибуты пользователей
- Параметры окружения, в котором работают пользователи

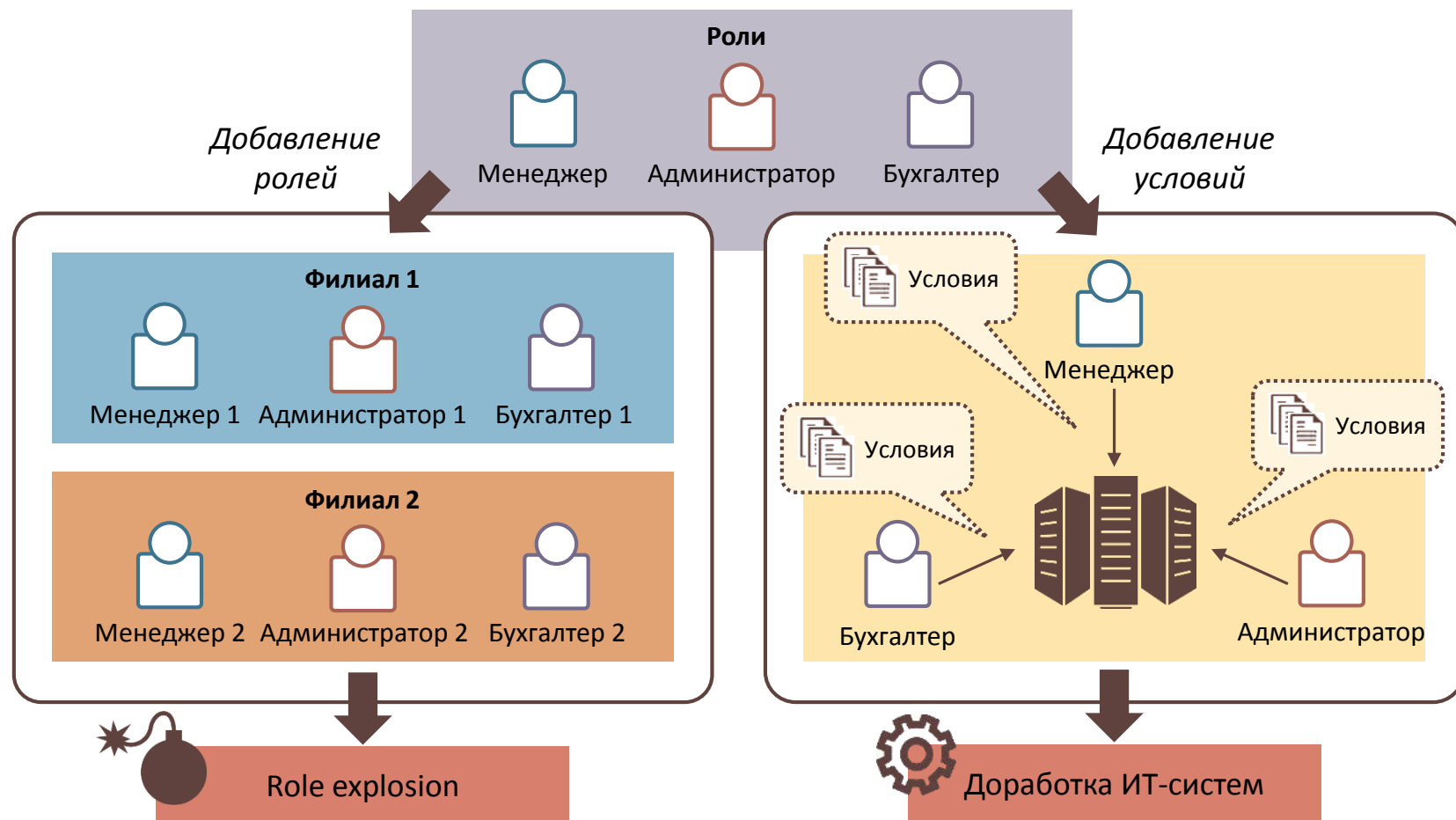
| Служебные обязанности многих пользователей требуют создания **множества уникальных ролей**

| Сложно поддерживать **актуальное состояние прав доступа** при организационных изменениях

УПРАВЛЕНИЕ РОЛЯМИ: МАТРИЦА

[illegible]

RBAC: ВАРИАЦИИ И РАЗВИТИЕ



IDENTITY MANAGER КАК ПОПЫТКА РЕШЕНИЯ

ФУНКЦИОНАЛЬНОСТЬ

- | Приводит все варианты управления ролями к единой модели
- | Централизованно управляет правами в ИТ-системах предприятия
- | Реализует бизнес-сценарии: найм, увольнение, отпуск и т. п.

«УЗКИЕ МЕСТА»

- | Действует в рамках RBAC-модели
- | Не учитывает атрибуты бизнес-объектов
- | Ограничен существующими в ИТ-системе ролями

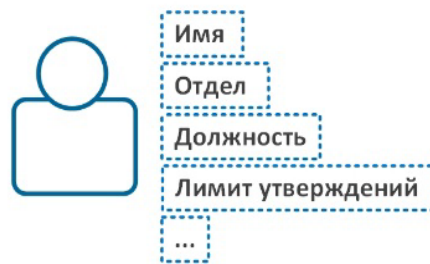
АТРИБУТНАЯ МОДЕЛЬ ДОСТУПА (АВАС)

- | Права доступа определяются логическими правилами, составленными в терминах бизнес-атрибутов
- | Атрибутами обладают субъекты (пользователи), ресурсы (объекты), действия и среда
- | Модель стандартизована в рамках [XACML 3.0](#) (первая версия – 2003 год)

Атрибуты ресурса



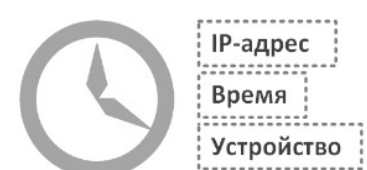
Атрибуты субъекта



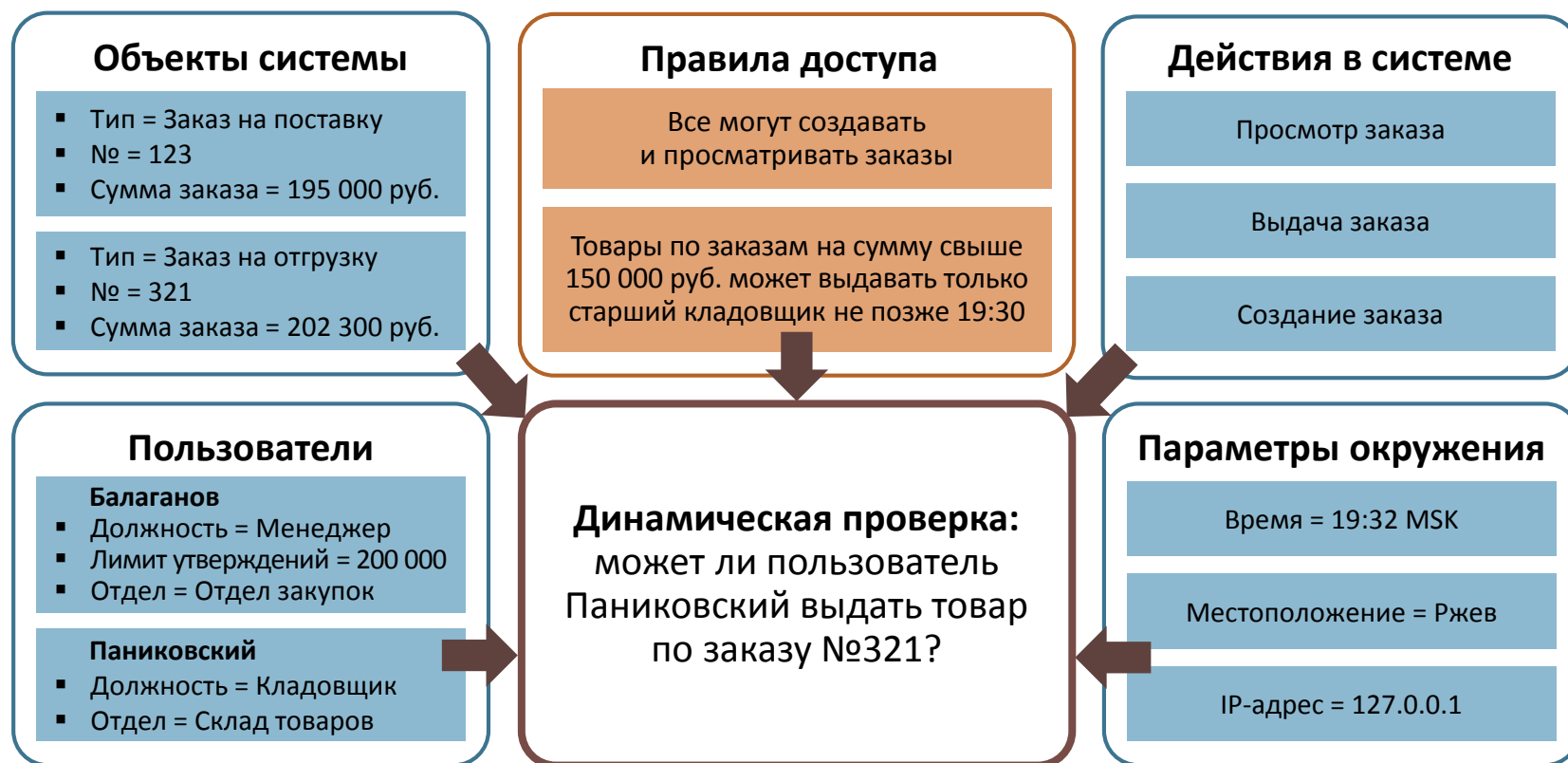
Атрибуты действия



Атрибуты среды



АВАС: СХЕМА ОРГАНИЗАЦИИ ДОСТУПА

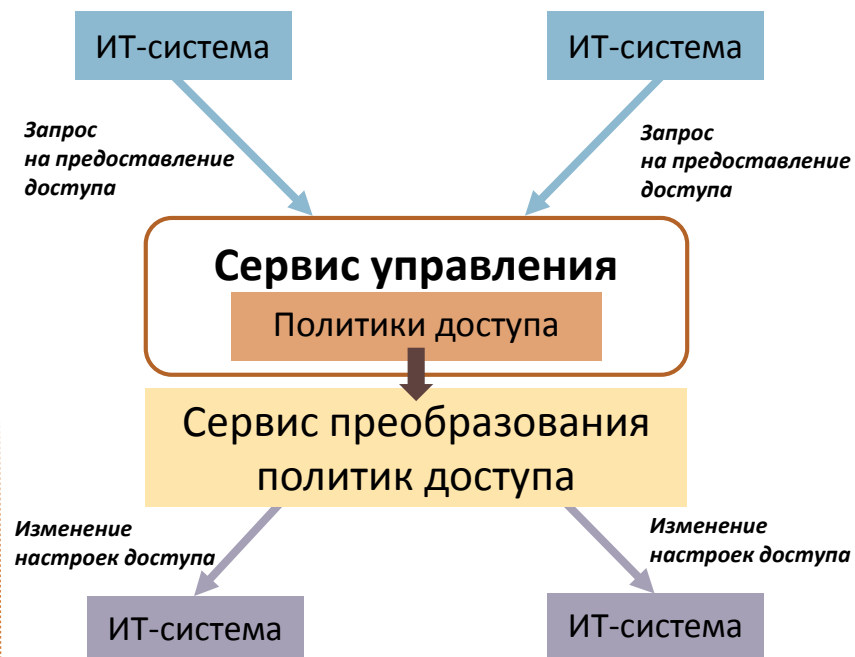


ПОДХОДЫ К УПРАВЛЕНИЮ ДОСТУПОМ

Стандартный подход



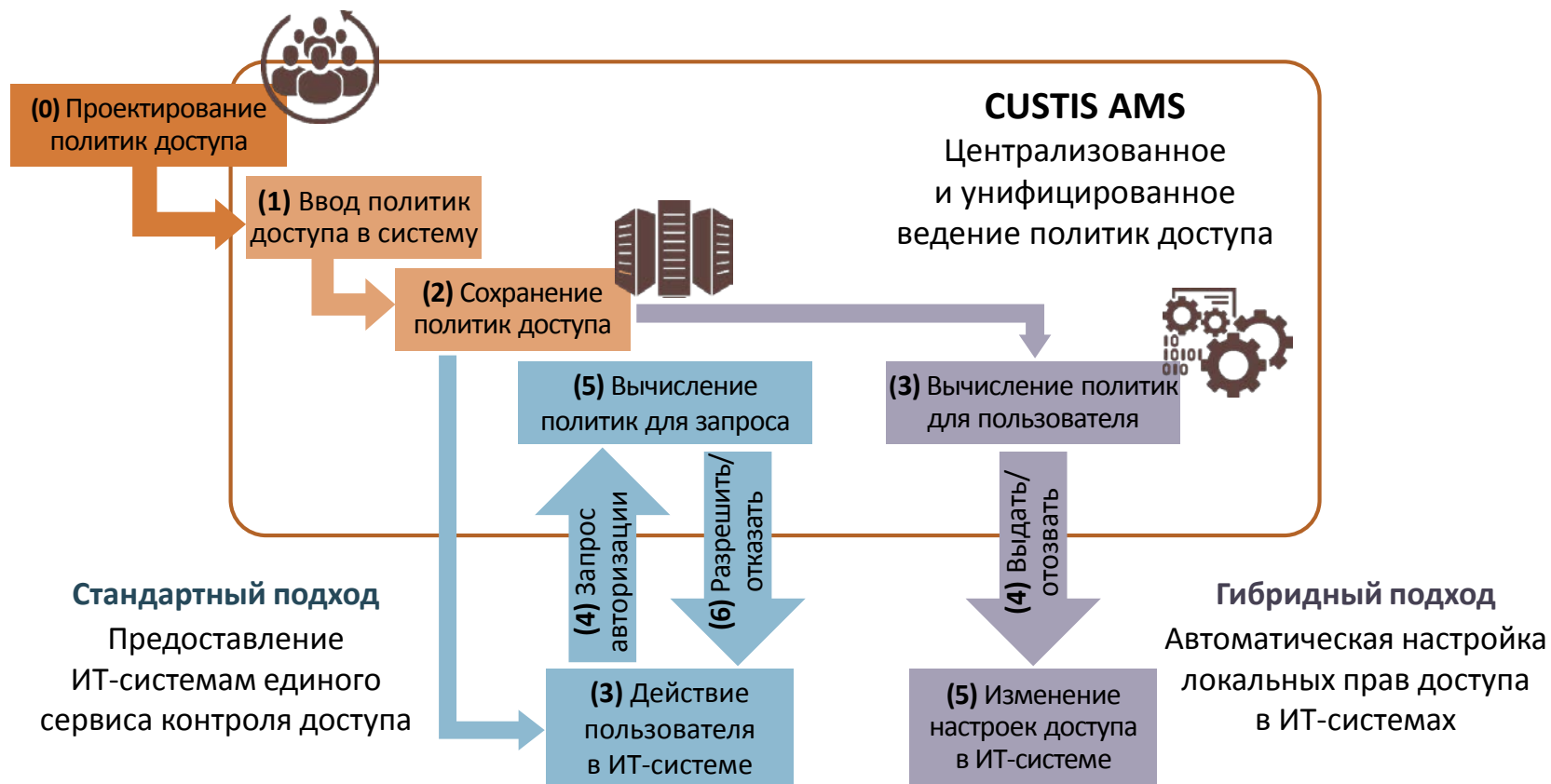
Гибридный подход



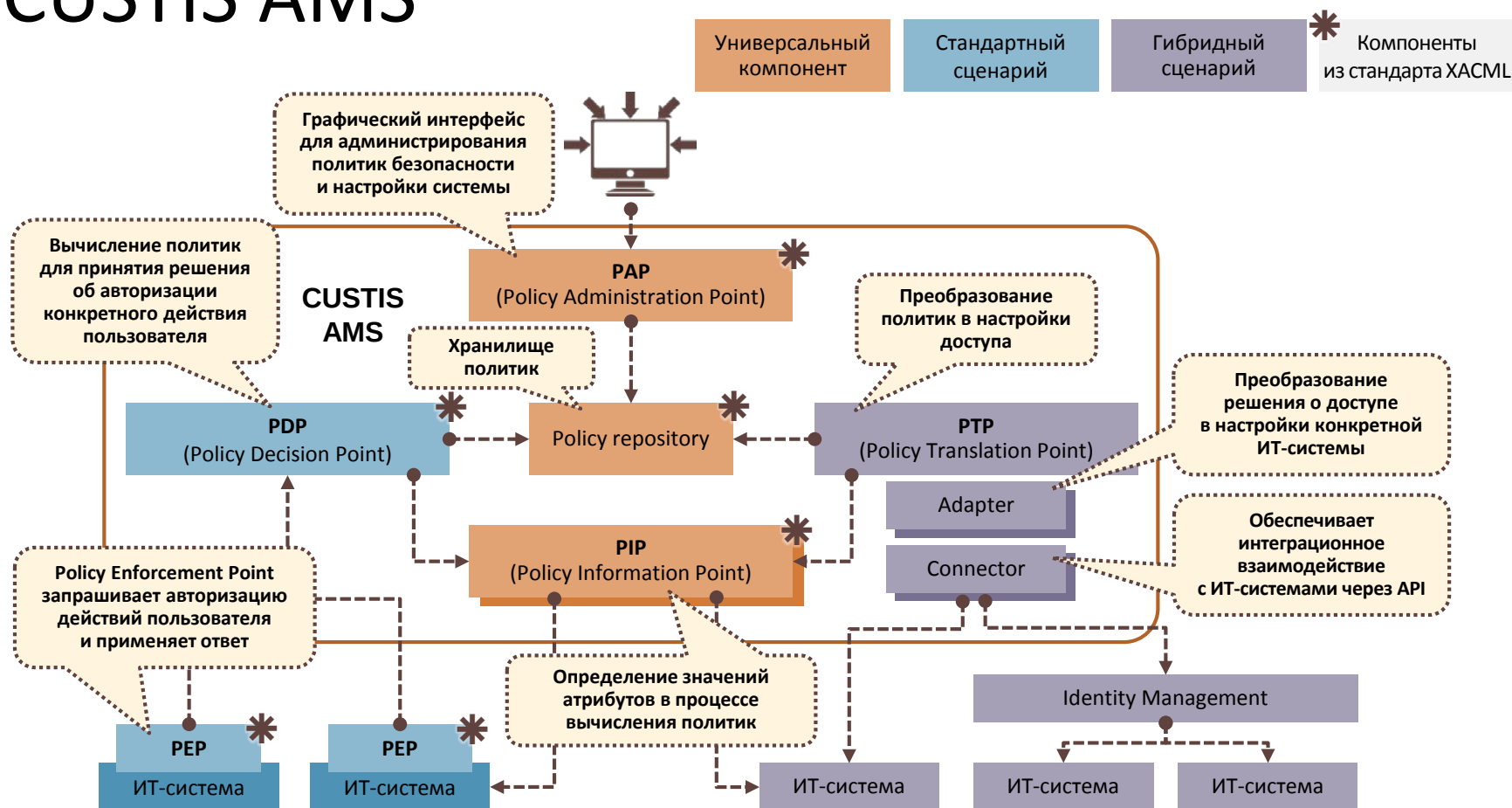
ФУНКЦИИ РЕШЕНИЯ CUSTIS AMS

- | **Проектирование прав доступа** в виде множества политик (наборов правил) при участии бизнес-подразделений, ИТ-службы и службы безопасности
- | **Централизованное и унифицированное** ведение политик доступа
- | **Интеграция** с информационными системами предприятия
- | **Контроль доступа** в соответствии с описанными политиками
 - Автоматическая настройка локальных прав доступа в ИТ-системах
 - Предоставление ИТ-системам единого сервиса контроля доступа
- | **Формирование отчетов** для аудита и анализа
 - Когда и на каком основании выданы права
 - Кто имеет доступ к определенным действиям и данным
 - Соответствует ли распределение прав политикам доступа и т. п.

СХЕМА РАБОТЫ РЕШЕНИЯ CUSTIS AMS



ФУНКЦИОНАЛЬНЫЕ КОМПОНЕНТЫ CUSTIS AMS



ПРЕИМУЩЕСТВА РЕШЕНИЯ CUSTIS AMS

Возможность задавать логические правила на основе множества атрибутов информационных ресурсов, объектов и самих пользователей

1

Увеличение гибкости настроек
Снижение стоимости управления правами

Возможность использовать решение как дополнение к существующей системе авторизации либо самостоятельно

2

Сохранение инвестиций в систему информационной безопасности предприятия

Автоматическое определение прав пользователей в соответствии с политиками, автоматизация стандартных процедур

3

Повышение эффективности, оперативности и надежности процесса управления правами

Централизованные настройки прав в виде обобщенных правил

4

Снижение сложности управления правами

Ведение правил доступа в формате, приближенном к регламентам безопасности

5

Повышение прозрачности системы распределения прав

ГРУППА КОМПАНИЙ CUSTIS

- | **20 лет** на российском ИТ-рынке
- | **Масштабные проекты** для отраслевых лидеров и организаций с высокой динамикой бизнес-процессов: Банка России, Газпромбанка, ГК «Спортмастер» (розничных сетей «Спортмастер», O'STIN, FUNDAY)
- | **Работа на стратегическое развитие клиентов,** решение критически важных бизнес-задач средствами ИТ, поддержка передовых технологических проектов



ГАЗПРОМБАНК



**ДЕПАРТАМЕНТ
ОБРАЗОВАНИЯ
ГОРОДА МОСКВЫ**

СПАСИБО ЗА ВНИМАНИЕ!

Вячеслав Муравлев

Архитектор решений, группа компаний CUSTIS

www.custis.ru

+7 (495) 772-97-02

vmuravlev@custis.ru