CUSTIS®

RBAC & ABAC:
ГИБРИДНОЕ РЕШЕНИЕ ДЛЯ УПРАВЛЕНИЯ ПРАВАМИ ДОСТУПА

Вячеслав Муравлев

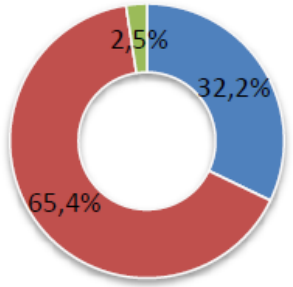
Ведущий разработчик, группа компаний CUSTIS

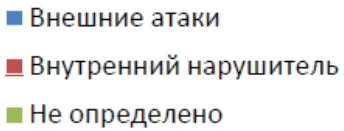
InfoSecurity Russia
20 сентября 2016 года

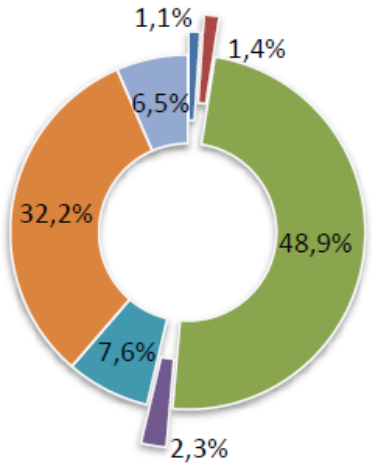
УТЕЧКИ ИНФОРМАЦИИ

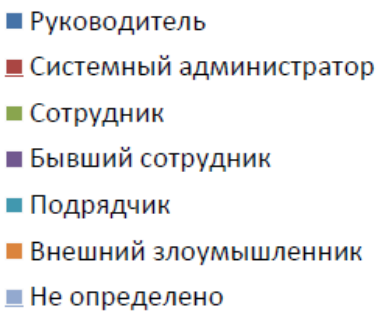
По данным InfoWatch за 2015 год

- Большая доля утечек информации (65,4%) происходит по вине внутренних нарушителей
- Почти половина утечек (49%) происходит по вине сотрудников (как бывших, так и настоящих)









CUSTIS®

ОСОБЕННОСТИ ИТ-ЛАНДШАФТА КРУПНОГО ПРЕДПРИЯТИЯ

- 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

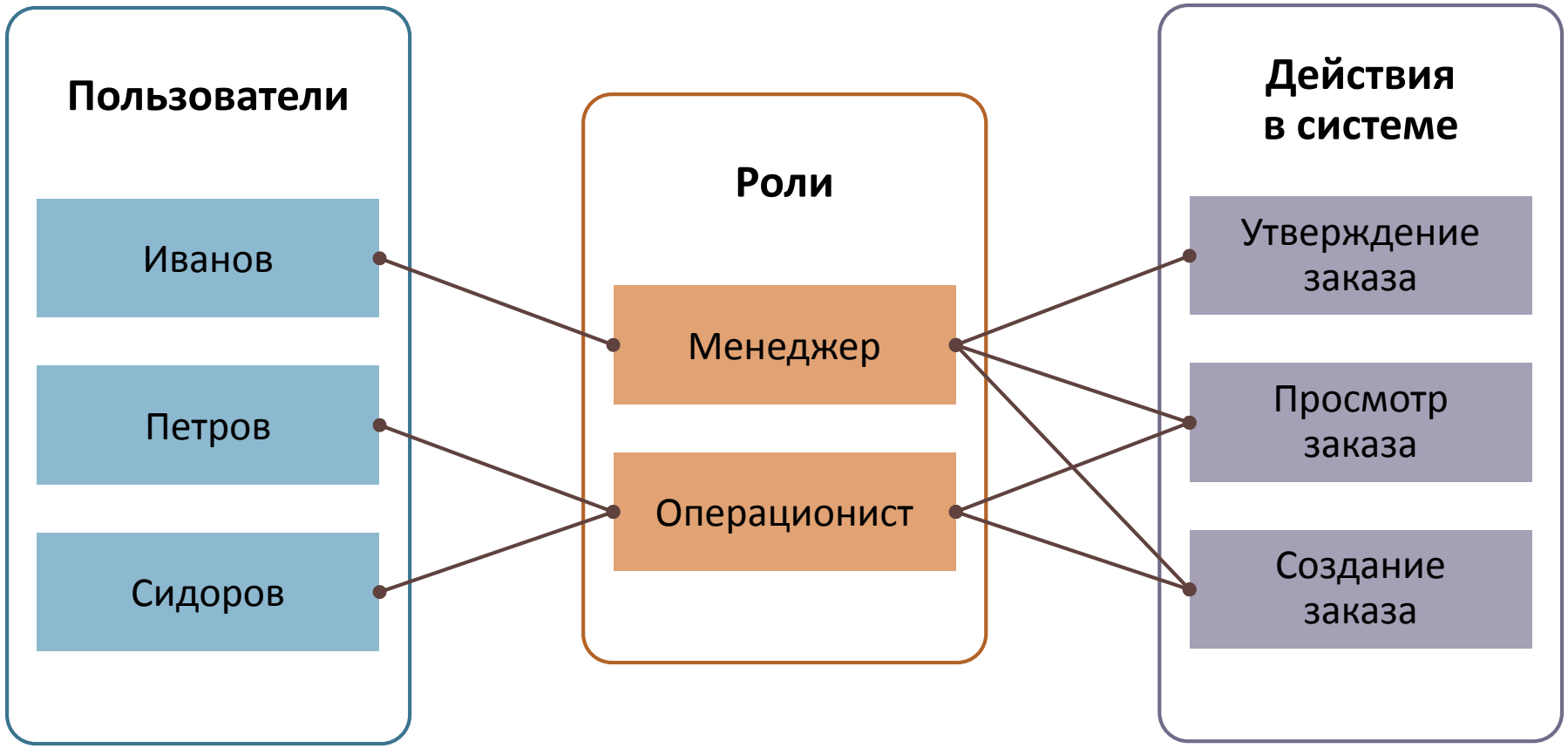
CUSTIS®

ЦЕЛИ УПРАВЛЕНИЯ ПРАВАМИ ДОСТУПА

- **Снижение рисков,** связанных с неправомерной или несвоевременной выдачей или отзывом прав доступа пользователей
- **Снижение стоимости** управления правами доступа
- **Повышение оперативности** процессов управления правами: быстрая выдача временных прав, минимальное время простоя при настройке прав и т. д.

CUSTIS®

РОЛЕВАЯ МОДЕЛЬ ДОСТУПА (RBAC)



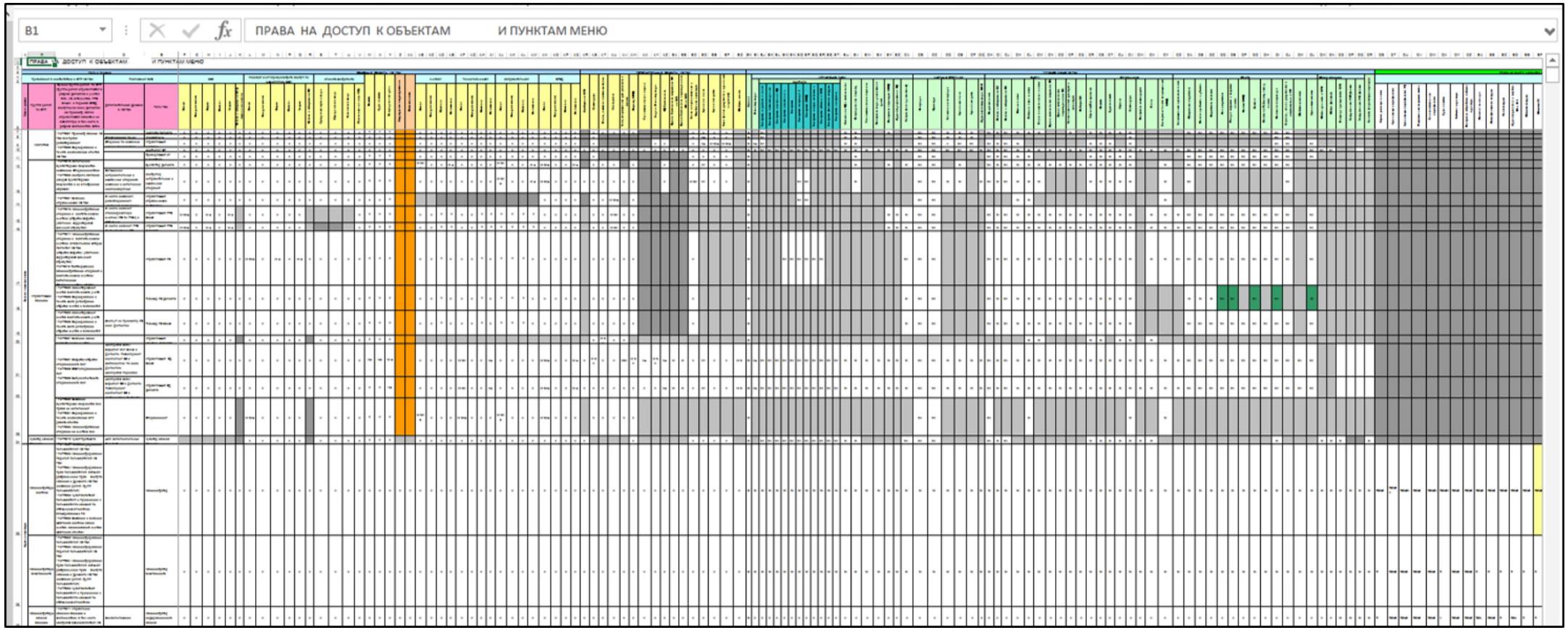
CUSTIS®

БОЛЕЗНИ РОСТА RBAC

- В чистом виде модель недостаточно гибка, поскольку не учитывает:
  - контекст действий пользователей
  - атрибуты пользователей
  - параметры окружения, в котором работают пользователи
- У большого числа пользователей служебные обязанности требуют создания уникальных ролей
- Сложно поддерживать актуальное состояние прав доступа при организационных изменениях

CUSTIS®

УПРАВЛЕНИЕ РОЛЯМИ: МАТРИЦА



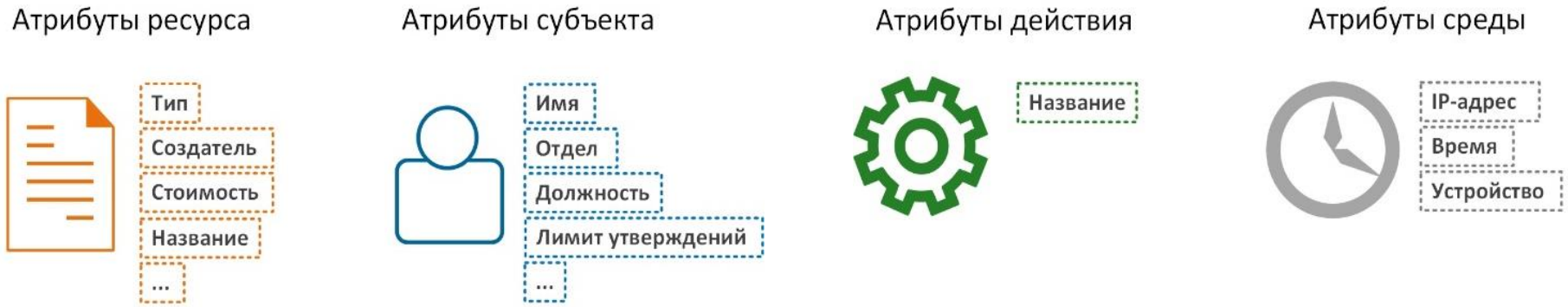
CUSTIS®

RBAC: ВАРИАЦИИ И РАЗВИТИЕ

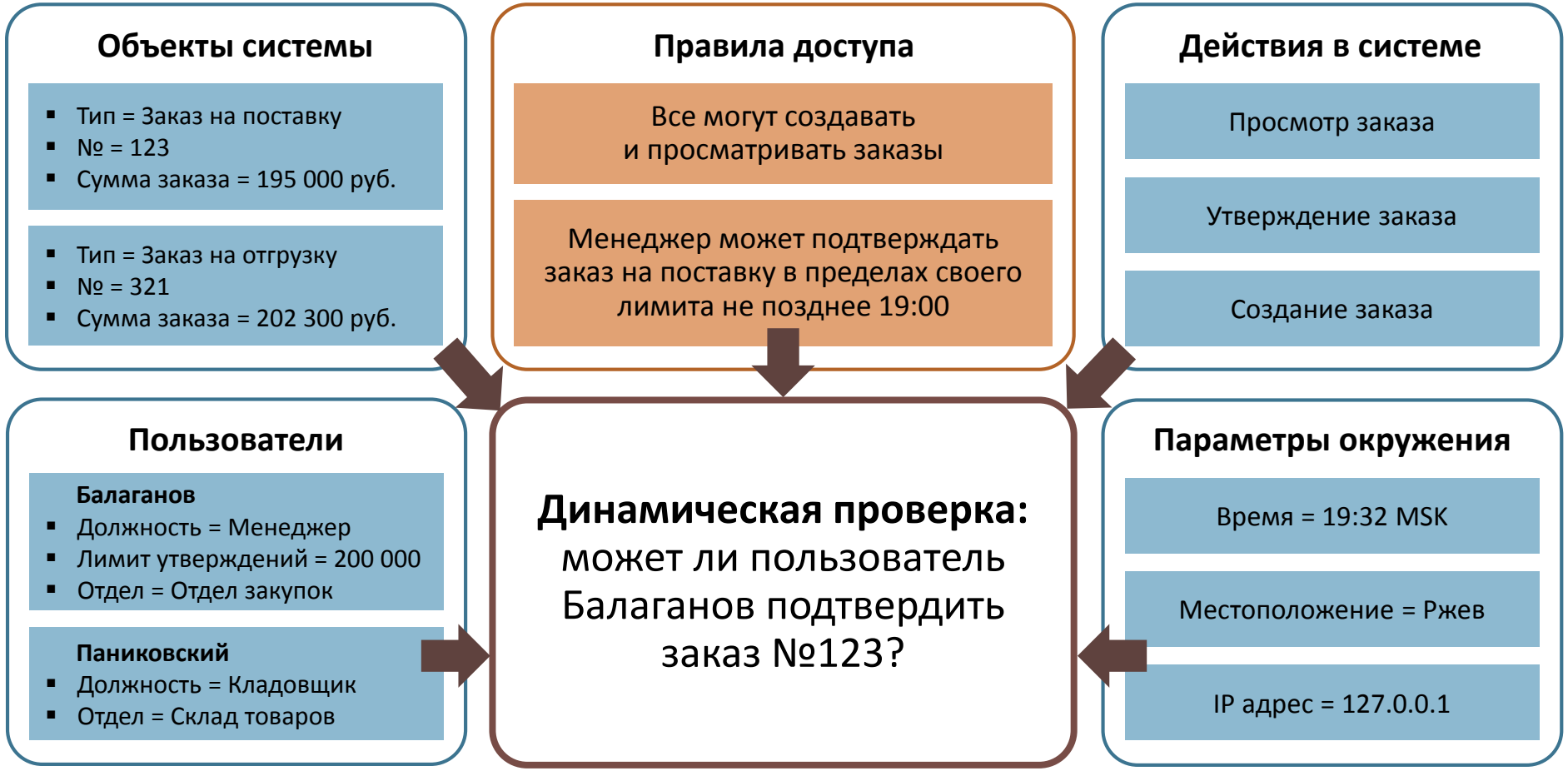
- «Классический» RBAC – статические привилегии
  - Роль *«Менеджер» = «Просмотр заказов» + «Изменение заказов»*
  - `if (user.hasPrivilege('view_order')) …`
  - Недостаток: не поддерживает разрез по атрибутам объектов
- Динамическая проверка атрибутов объекта
  - Роль *«Менеджер филиала 123» = «Просмотр заказов филиала 123» + «Изменение заказов филиала 123»*
  - `if (user.hasPrivilege('view_order_' + order.branch) …`
  - Недостаток: приводит к «role explosion» – созданию роли для каждого значения атрибута
- Динамическая проверка атрибутов субъекта
  - Роль *«Менеджер филиала» = «Просмотр заказов <u>своего</u> филиала» + «Изменение заказов <u>своего</u> филиала»*
  - `if (user.hasPrivilege('view_order') && user.branch==order.branch))`
- Логическое продолжение – ABAC (Attribute-Based Access Control)

АТРИБУТНАЯ МОДЕЛЬ ДОСТУПА (ABAC)

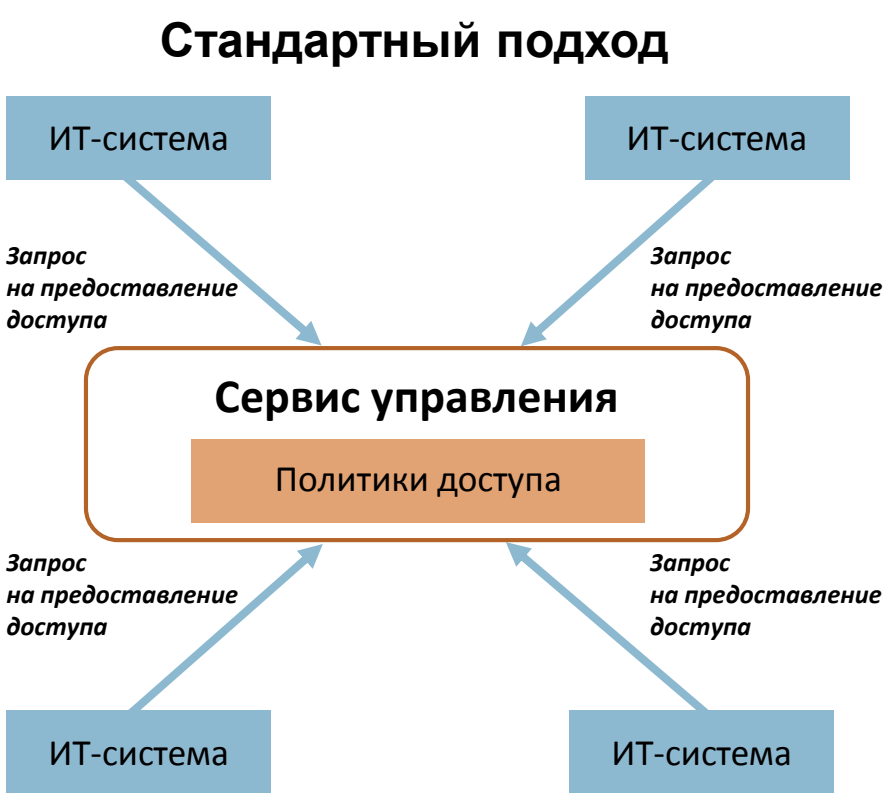
- Права доступа определяются логическими правилами, составленными в терминах бизнес-атрибутов
- Атрибутами обладают субъекты (пользователи), ресурсы (объекты), действия и среда
- Модель стандартизована в рамках XACML 3.0 (первая версия – 2003 г.)

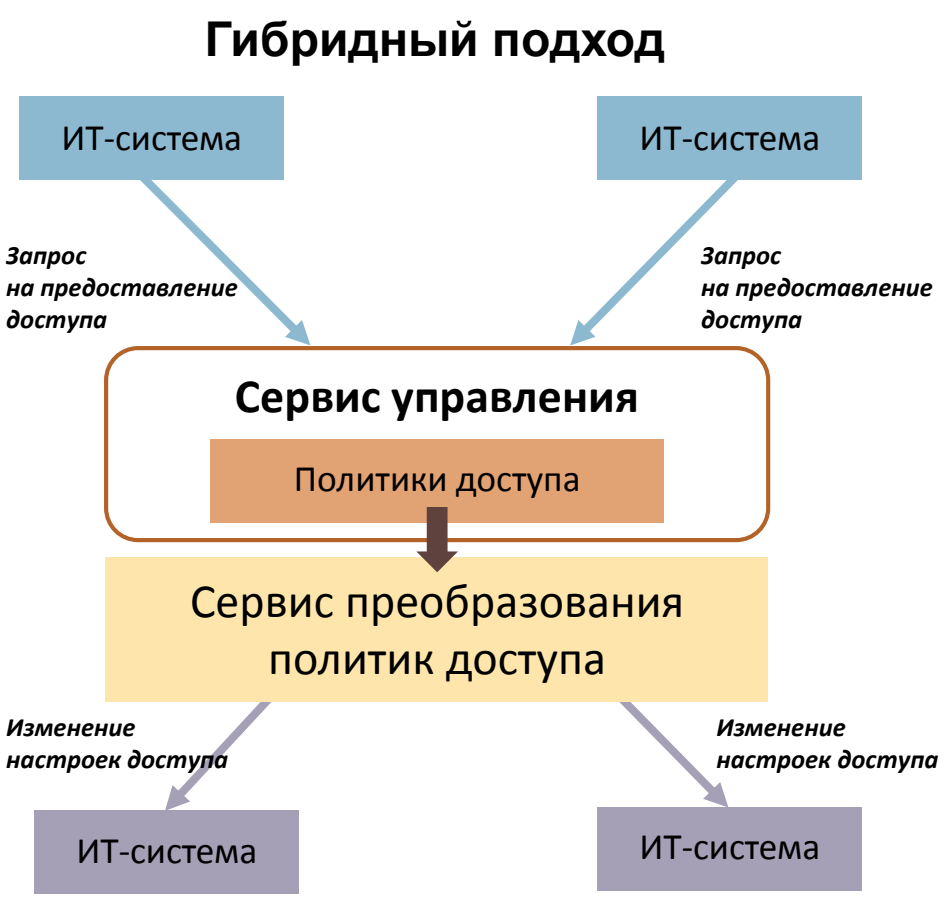


ABAC: СХЕМА ОРГАНИЗАЦИИ ДОСТУПА



ПОДХОДЫ К УПРАВЛЕНИЮ ДОСТУПОМ



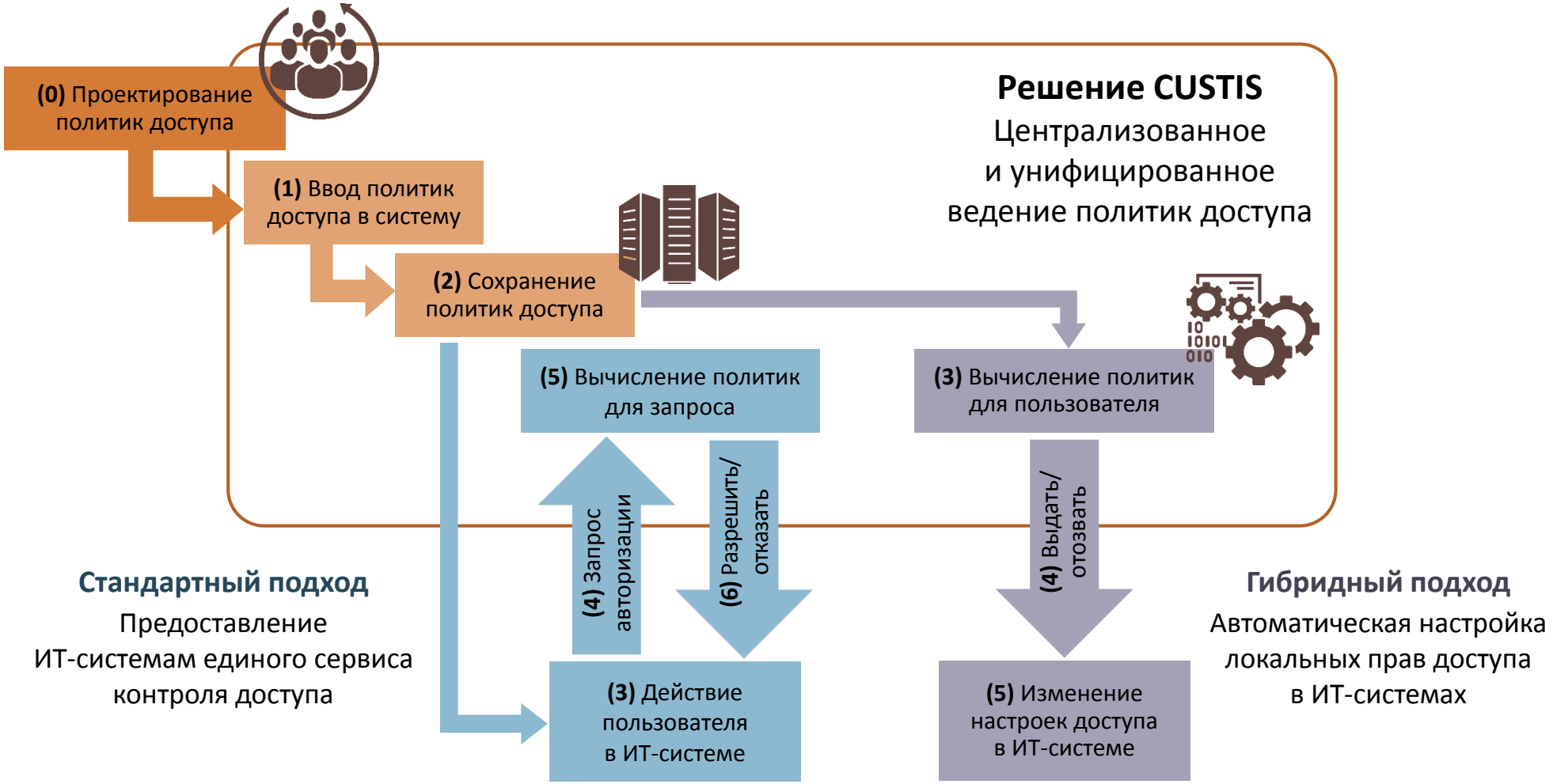


CUSTIS®

ФУНКЦИИ РЕШЕНИЯ

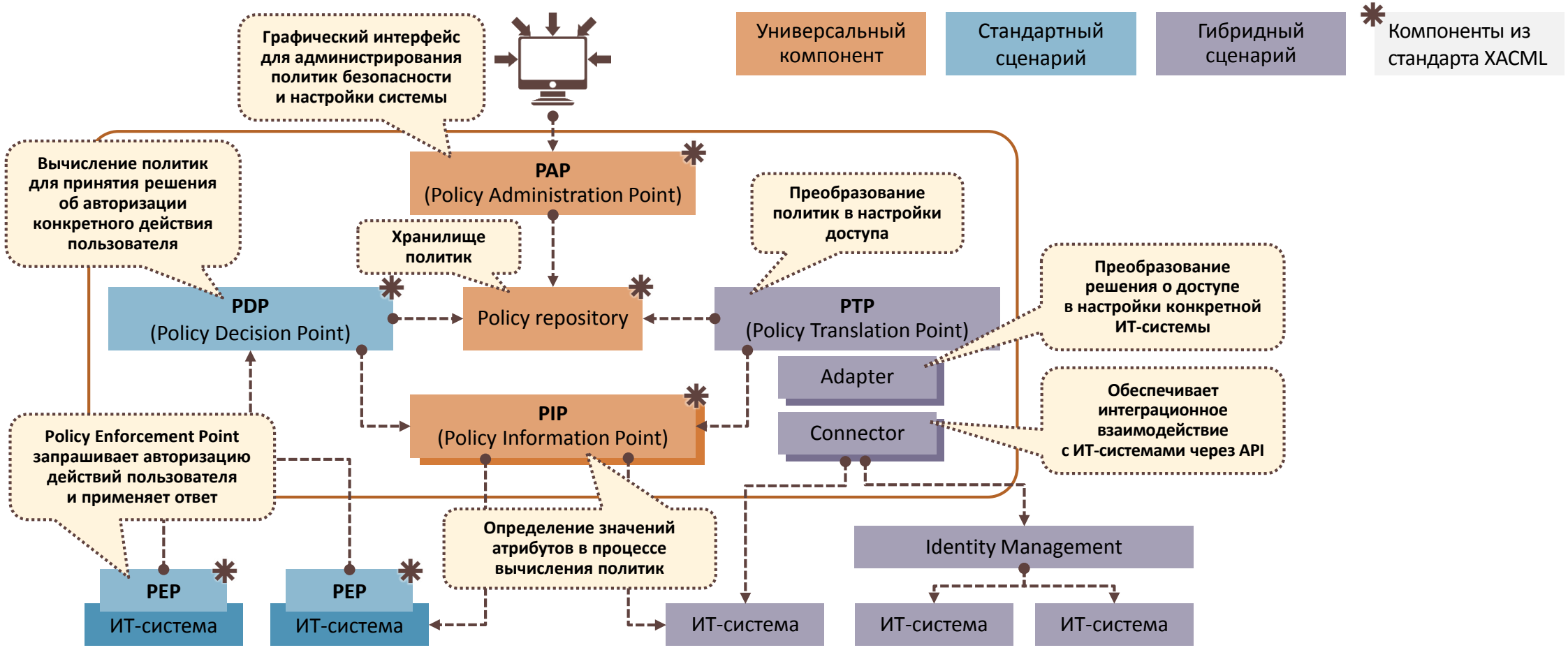
- **Проектирование прав доступа** в виде множества политик (наборов правил) при участии бизнес-подразделений, ИТ-службы и службы безопасности
- **Централизованное и унифицированное ведение политик доступа**
- **Интеграция** с различными информационными системами предприятия
- **Контроль доступа** по двум вариантам
  - Автоматическая настройка локальных прав доступа в ИТ-системах в соответствии с описанными политиками
  - Предоставление ИТ-системам предприятия единого сервиса контроля доступа в соответствии с описанными политиками
- **Формирование отчетов** для аудита и анализа
  - Например, текущие права конкретного пользователя, когда и на каком основании выданы, кто из пользователей имеет доступ к определенным действиям и данным, соответствие распределения прав политикам доступа и т. п.

СХЕМА РАБОТЫ РЕШЕНИЯ



CUSTIS®

ФУНКЦИОНАЛЬНЫЕ КОМПОНЕНТЫ РЕШЕНИЯ



CUSTIS®

ПРЕИМУЩЕСТВА РЕШЕНИЯ

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

CUSTIS®

ГРУППА КОМПАНИЙ CUSTIS

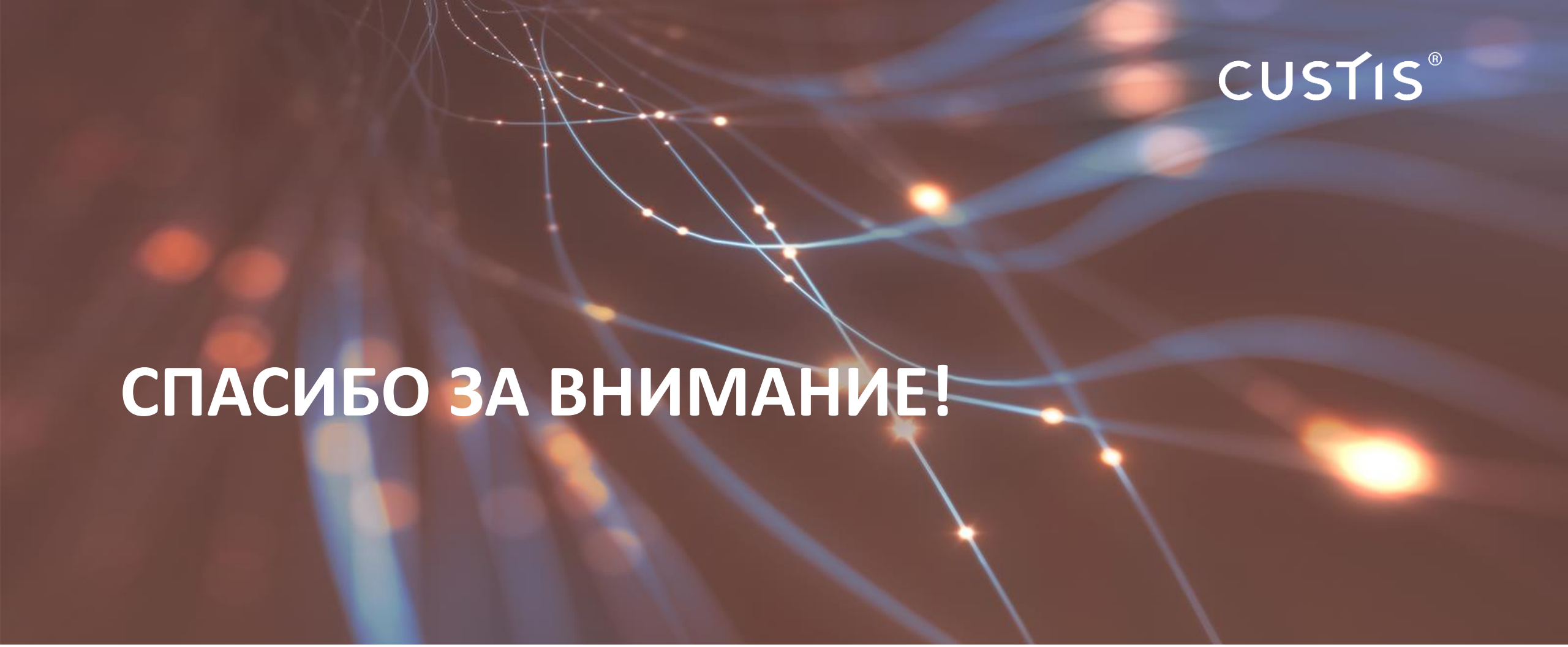
- **20 лет** на российском ИТ-рынке
- **Масштабные проекты** для отраслевых лидеров и организаций с высокой динамикой бизнес-процессов: Банка России, Газпромбанка, ГК «Спортмастер» (розничных сетей «Спортмастер», O'STIN, FUNDAY)
- **Работа на стратегическое развитие клиентов,** решение критически важных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

БАНК РОССИИ

ГАЗПРОМБАНК

спортмастер

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ



СПАСИБО ЗА ВНИМАНИЕ!

Вячеслав Муравлев

Ведущий разработчик, группа компаний CUSTIS

www.custis.ru

+7 (495) 772-97-02

vmuravlev@custis.ru