

Подход к выявлению конфликтов и реализации разграничения полномочий

Петр Михеев, Ведущий консультант
15 декабря 2010



Масштаб проблемы

Изменения системы полномочий (ролей, профилей)

Большое количество транзакций

Список лиц, уполномоченных вносить изменения, не формализован

Отсутствие формализованных процессов предоставления/изменения доступа

Значительное количество пользователей

Существенные изменения бизнес-процессов и выполняемых операций

Изменения должностных обязанностей пользователей

Значительное количество ролей

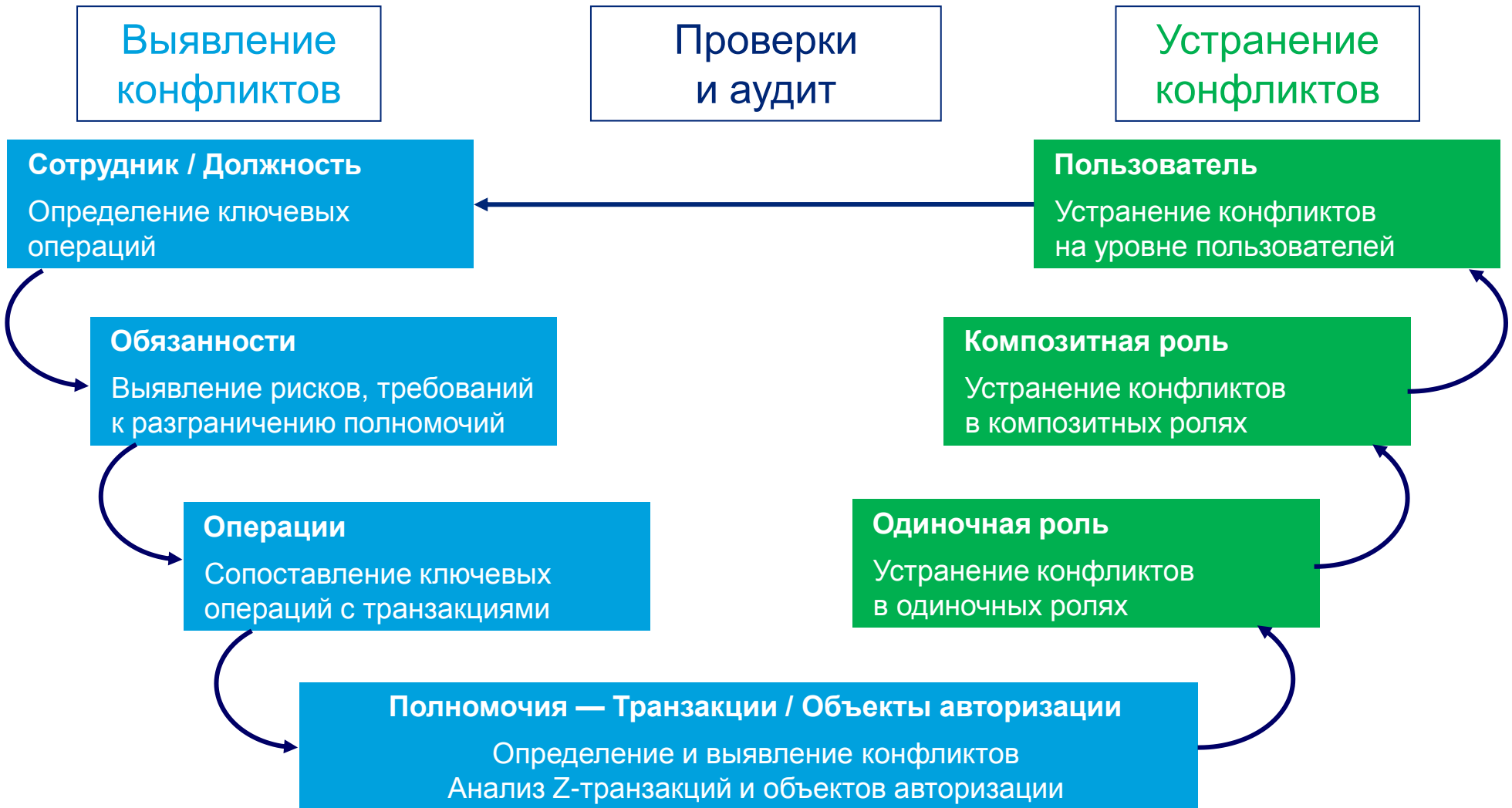
Изменения функциональности системы

Отсутствие формализованного списка владельцев информационных ресурсов

Отсутствие формализованных процессов изменения конфигурации / системы полномочий (ролей, профилей)

Методология разграничения полномочий

Постановка процесса обеспечения надлежащего разделения полномочий
Интеграция с процессами предоставления логического доступа, управления изменениями и аудита



Выявление конфликтов разграничения полномочий

Выявление ключевых операций

- Анализ проектных решений и описаний бизнес-процессов, реализованных/ планируемых к реализации в системе.
- Проведение интервью с функциональными консультантами и пользователями бизнес-процессов.

Определение требований к разграничению полномочий

- Классификация ключевых операций (Авторизация, Отражение в учете, Сохранность ценностей).
- Выявление рисков, конфликтующих ключевых операций и построение матрицы разграничения полномочий.

Сопоставление ключевых операций с транзакциями

- Анализ проектных решений, описаний бизнес-процессов и выявление используемых транзакций.
- Определение используемых стандартных и нестандартных (Z) транзакций, детализация на уровне объектов авторизации.

Определение и выявление конфликтов

- Выявление конфликтов стандартных и нестандартных (Z) транзакций на уровне ключевой операции, с учетом объектов авторизации.

Устранение конфликтов разграничения полномочий

Устранение конфликтов в одиночных ролях

- Корректировка одиночных ролей, в том числе исключение конфликтующих транзакций, разделение одиночных ролей и изменений соответствующих объектов авторизации.

Устранение конфликтов в композитных ролях

- Корректировка композитных ролей, в том числе исключение конфликтующих одиночных ролей, разделение композитных ролей.
- Разработка и внедрение компенсирующих контрольных процедур — контрольных процедур, снижающих риск конфликта полномочий.

Устранение конфликтов на уровне пользователя

- Корректировка перечня композитных ролей, назначенных пользователю.
- Разработка и внедрение компенсирующих контрольных процедур.

Процессы с учетом разграничения полномочий

- Постановка процесса обеспечения разграничения полномочий.
- Интеграция с процессами предоставления доступа и управления изменениями.

Процессы с учетом разграничения полномочий



Результаты применения методологии

Концепция разграничения полномочий

- Концепция обеспечения разграничения полномочий – основные принципы и подход.

Матрица разграничения полномочий

- Формирование матрицы разграничения полномочий для выявления и разрешения возможных конфликтов, включая настройку автоматизированных инструментов.

Роли и ответственность

- Определение ролей и ответственности за разграничение полномочий, включая управление доступом, внесение изменений и аудит. Обучение персонала.

Регламентирующие документы

- Подготовка и доработка регламентирующих документов (политики, регламенты, инструкции).

Пример. Конфликты разграничения полномочий



Спасибо за внимание.



Наименование «Делойт» относится к одному либо любому количеству юридических лиц, входящих в «Делойт Туш Томацу Лимитед», частную компанию с ответственностью участников в гарантированных ими пределах, зарегистрированную в соответствии с законодательством Великобритании; каждое такое юридическое лицо является самостоятельным и независимым юридическим лицом. Подробная информация о юридической структуре «Делойт Туш Томацу Лимитед» и входящих в нее юридических лиц представлена на сайте www.deloitte.com/about. Подробная информация о юридической структуре «Делойта» в СНГ представлена на сайте www.deloitte.com/ru/about.

«Делойт» предоставляет услуги в области аудита, налогообложения, управленческого и финансового консультирования государственным и частным компаниям, работающим в различных отраслях промышленности. «Делойт» – международная сеть компаний, которые используют свои обширные отраслевые знания и многолетний опыт практической работы при обслуживании клиентов в любых сферах деятельности в более чем 140 странах мира. 169,000 специалистов «Делойта» по всему миру привержены идеям достижения совершенства в предоставлении профессиональных услуг своим клиентам.

Сотрудники «Делойта» объединены особой культурой сотрудничества, которая в сочетании с преимуществами культурного разнообразия направлена на развитие высоких моральных качеств и командного духа и повышает ценность наших услуг для клиентов и рынков. Большое внимание «Делойт» уделяет постоянному обучению своих сотрудников, получению ими опыта практической работы и предоставлению возможностей карьерного роста. Специалисты «Делойта» способствуют укреплению корпоративной ответственности, повышению общественного доверия к компаниям объединения и созданию благоприятной атмосферы в обществе.