Опыт внедрения и результаты проекта

«Контроль конфликтов полномочий, оптимизация процессов управления ролями и предоставления доступа на базе решения SAP GRC AC»

Балабанов Дмитрий
Руководитель направления
по интеллектуальным системам защиты
ДБ АО «ОМК»

17.04.2019

Цели и задачи проекта

ЦЕЛИ

ЦЕЛИ ПРЕДПРОЕКТА

- Анализ действующего процесса управления доступом, определение узких мест и сбор требований к целевому процессу;
- Анализ применимости стандартного функционала системы GRC AC для реализации требований к целевому процессу
- Разработка ТЗ внедрение целевого процесса управления доступом в системы SAP и разделения прав полномочий
- Экспресс-оценка текущих конфликтов полномочий в SAP системах;
- Проведение ретроспективы по возможным злоупотреблениям с оценкой потенциальных потерь Компании.

ЦЕЛИ ПРОЕКТА

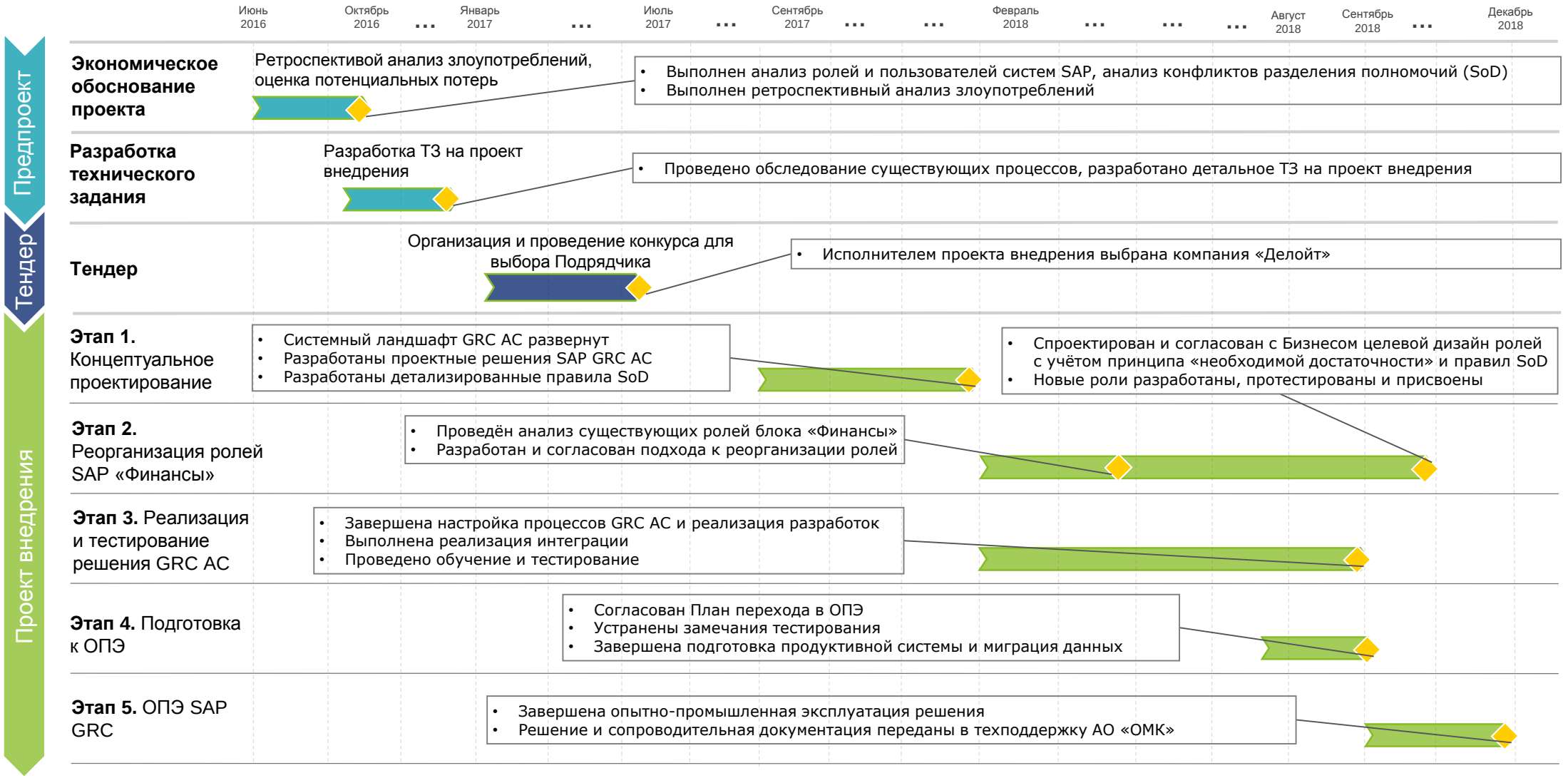
- Повышение эффективности процесса управления доступом пользователей в SAP путем автоматизации отдельных шагов и повышения контроля использования полномочий;
- Предотвращение нарушений правил разделения полномочий (SoD) у пользователей SAP систем, приводящих к потенциальным финансовым потерям;
- Внедрение ролевой модели систем SAP, учитывающей принципы разделения полномочий (SoD) и недостатки действующей ролевой модели;
- Контроль за использованием расширенных полномочий в SAP;
- Оптимизация количества и состава используемых ролей блока «Финансы»;
- Разрешение SoD-рисков в ролях бизнес-процесса «Финансы» продуктивной системы SAP ERP и у пользователей.

ОСНОВНЫЕ ЗАДАЧИ

- Разработка матрицы конфликтов полномочий (SoD), детализированной в части пилотных бизнес-процессов;
- Внедрение единой ролевой модели для систем SAP, централизованные процессы и единые инструменты управления правами и учетными записями пользователей;
- Автоматизация набора SoD-правил с учетом специфики реализации бизнес-процессов ОМК в SAP системах на уровне транзакций и объектов полномочий согласно списку бизнес процессов, включённых в периметр проекта;
- Автоматизация централизованного процесса управления доступом к SAP-системам и процесс управления изменениями ролей на базе SAP GRC AC;
- Реализация процесса поддержания и дальнейшего развития принципов и правил SoD в SAP системах;
- Оптимизация ролей бизнес-процесса «Финансы» SAP ERP для устранения SoD-конфликтов, сокращения количества ролей и облегчения выбора ролей в заявке на доступ;
- Более глубокое вовлечение участников со стороны Бизнеса в процессы управления доступом.

План проекта

Июнь 2016 – Ноябрь 2018



Анализ рисков и ретроспектива злоупотреблений

Подход к выполнению работ

Результаты анализа рисков и ретроспективы злоупотреблений

Наблюдения по результатам анализа		Выгоды на основании анализа
Ретроспективный анализ злоупотреблений	Пользователи систем SAP, использовавшие конфликтующие полномочия в работе Пользователи систем SAP, выполнившие бизнес-процесс целиком	• Количественная оценка стоимости операций, выполняемых пользователями систем SAP в разрезе анализируемых бизнес-процессов • Статистика в разрезе бизнес-процессов и компаний используется для определения организационного и функционального объёма проекта
Выявление рисков доступа	Пользователи (внутренние, ИТ, внешние) и роли в системах SAP с рисками и доступа	• Устранение критичных рисков доступа в ролях и у пользователей • Определение наиболее часто встречающихся рисков в разрезе бизнес-процессов
Учетные записи пользователей	Учетные записи, неиспользуемые более 2-х месяцев Действующие учетные записи, принадлежащие уволенным сотрудникам Дублированные учетные записи	• Исключение неиспользуемых УЗ для их исключения из пакета закупаемых лицензий; • Снижение вероятности некорректного использования (злоупотребления входом, некорректное делегирование, ошибочный выбор сотрудника в справочниках); • Снижение вероятности злоупотреблений с использованием чужой неиспользуемой учётной записи.
Полномочия пользователей	Учетные записи с расширенными полномочиями Бизнес пользователи, которым присвоены роли с критичными транзакциями Неиспользуемые в течение длительного периода времени полномочия в ролях пользователей	• Исключение заведомо избыточных полномочий у пользователей; • Сокращение трудозатрат на поддержку благодаря сокращению общего числа поддерживаемых присвоений; • Сокращение трудозатрат на поддержку в результате оптимизации ролей; • Повышение контроля за распространением критичного доступа; • Снижение вероятности злоупотреблений с использованием расширенных полномочий.

Перечень автоматизируемых бизнес-процессов

Группа БП	Бизнес-процесс	Описание
Анализ рисков доступа	Анализ SoD конфликтов в ролях и у пользователей	Выявление конфликтов SoD в запросах на доступ в SAP и в запросах на изменение ролей, моделирование потенциальных конфликтов;
	Ведение матрицы SoD конфликтов	Ведение матрицы конфликтов полномочий SAP в системе GRC AC;
	Назначение компенсирующих контролей к рискам доступа	Назначение ККП сотруднику с SoD конфликтом для его митигации, контроль актуальности назначенных сотрудникам ККП;
Управление доступом	Создание/изменение учетной записи и присвоение/отзыв ролей, включая запрос на нескольких пользователей	Создание запроса на доступ, включая запрос на нескольких пользователей и его анализ на конфликты SoD;
	Автоматическая обработка кадровых мероприятий	Автоматизированный процесс обработки принятия нового сотрудника на работу в компанию, смены должности, перемещения сотрудника, увольнения и ухода в декрет;
	Продление срока действия учетной записи или ролей	Автоматический контроль истекающих у пользователя полномочий и уведомления о необходимости продлить доступ;
	Удаление учётной записи	Запрос на удаление полномочий и УЗ пользователя в отдельной системе SAP;
	Блокировка и разблокировка УЗ пользователя	Центральная блокировка и разблокировка пользователя во всех системах SAP;
	Создание/изменение учетной записи технического пользователя и присвоение/отзыв ролей	Упрощённая форма подачи запроса на создание/ изменение доступа в SAP технического пользователя;
Управление ролями	Управление созданием/ изменением ролей	Определение параметров ролей систем SAP и анализ на SoD, согласование изменения ролей, документирование тестирования;
FireFighter	Предоставление расширенных полномочий в системах SAP	Согласование предоставления и использование расширенных полномочий для выполнения критичных операций в системах SAP;

Целевая архитектура решения

Конечный пользователь
- Формирование заявки на доступ
- Сброс пароля в SAP

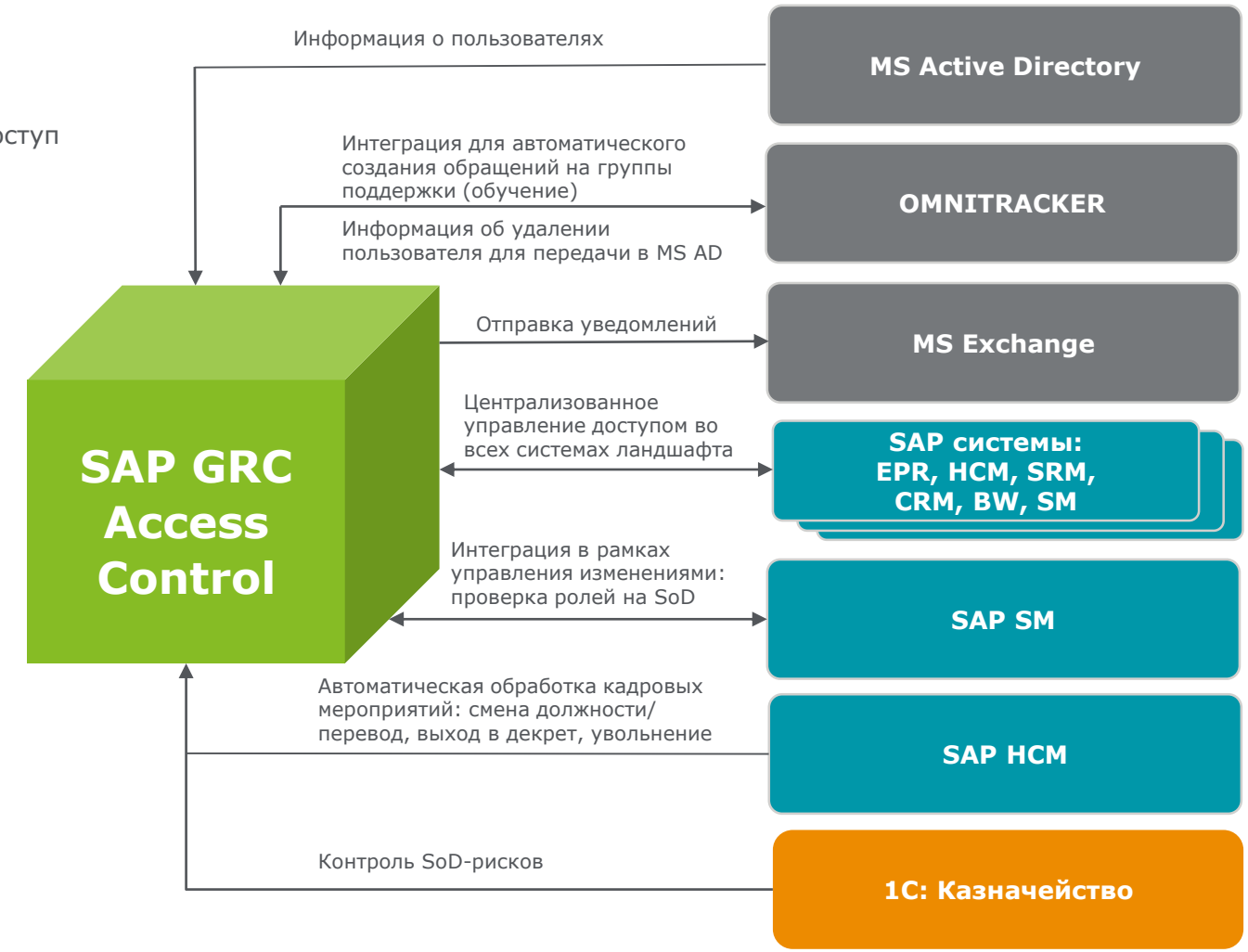
Линейный руководитель
- Согласование заявок
- SoD анализ
- Предложение ККП

Владелец роли
- Согласование заявок на доступ
- Согласование изменения ролей

Ответственный за проверку SoD
- Согласование заявок
- SoD анализ
- Управление ККП

Сотрудник ИБ
- Согласование заявок
- Управление блокировками

Ответственный за обучение
- Согласование заявок
- Проверка прохождения пользователями обучения
- Обучение пользователя



Предоставление доступа в SAP

Бизнес-пользователь	**Линейный руководитель**	**Владелец роли и Ответственный за ПнД**	**Ответственный за проверку SOD** при наличии SoD-рисков	**Сотрудник ИБ** доступ внешним пользователям	**Ответственный за обучение** доступ в продуктивные системы
					
Формирование запроса на доступ	**Согласование необходимости полномочий**	**Согласование необходимости полномочий**	**Согласование запросов и компенсирующих КП**	**Согласование необходимости полномочий**	**Подтверждение прохождения обучения**
Обязательный шаг процесса	Обязательный шаг процесса	Обязательный шаг процесса			Обязательный шаг процесса
Основные действия					
Формирование запроса: • Информация о пользователе; • Выбор ролей, ввод срока присвоения; • Ввод обоснования и добавление приложений.	• Анализ необходимости запрошенных ролей; • Просмотр выявленных конфликтов SOD; • Предложение ККП; • Полное или частичное согласование ролей.	• Анализ запроса с точки зрения обоснованности запрошенных полномочий; • Полное или частичное согласование ролей. • Если роль требует соглашения о неразглашении ПнД, запрос согласуется Ответственным за ПнД по БЕ.	• Анализ выявленных рисков SOD; • Согласование ККП; • Полное или частичное согласование запрошенных ролей.	• Анализ необходимости запрошенных ролей для внешних пользователей • Проверка заключенных контрактов, подписанного NDA	Контроль прохождения обучения пользователем в соответствии с согласованными на предыдущих этапах ролями.

Результат:

- Автоматическое создание УЗ и/или присвоение ролей пользователю(ям) в системах SAP;
- Уведомление согласующих о получении запроса на согласование, уведомление пользователя о выполнении запроса;
- Риски конфликтов разделения полномочий снижены при помощи компенсирующей контрольной процедуры;
- Эскалация запроса в случае задержки согласования на этапе. История согласования задокументирована в GRC AC.

Владельцы Ролей

Владелец роли - **это руководитель**, **обладающий правами на информацию**, предоставляемую и ограниченную в рамках ролей в соответствии со служебными обязанностями или нормативными документами, и **несущий ответственность за эту информацию**.

1. Владелец роли участвует в согласовании запросов на доступ в SAP (согласование ролей, Владельцем которых сотрудник является).
2. Владелец роли участвует в согласовании запросов на создание/ изменение ролей.
3. Экспертное участие в вопросах, связанных с предоставлением доступа к информации Владельца (критичность и актуальность рисков доступа, пути разрешения конфликтов, уточнение особенностей бизнес-процессов).
4. Владельцу роли рекомендуется не реже двух раз в год выполнять полный пересмотр предоставленного доступа в системах SAP.
5. Обязанности Владельца ролей закреплены в Регламенте по управлению доступом в системы SAP.
6. Владельцы ролей назначаются Владельцами функций.
7. Владелец одной роли в разных юридических лицах может отличаться.

Определение Владельцев ролей

- Определены Владельцы **95,6 %** ролей
- Реестр ролей и Владельцев утвержден приказом по Компании
- Запросы с ролями без Владельцев согласуются «техническим» согласующим от ДБ

Определение Владельцев ролей на оставшиеся и новые роли

- Для ролей, оставшихся без Владельцев, подготовлена аналитика для направления запросов в бизнес-подразделения для принятия решений.
- Определение Владельцев новых ролей проводится в соответствии с действующей НМД

Основные выводы по итогам работы Владельцев ролей

- Сложность при согласовании первых запросов из-за новизны системы
- Специфика «своих» ролей не всегда прозрачна Владельцам. Помогает каталог ролей и адаптация наименований ролей.
- Первоначальный список Владельцев должен быть формально закреплён
- Внимание дополнительным коммуникациям с целью обучения Владельцев работе в системе и вовлечения в процедуры управления изменениями «своих» ролей

Статистика работы системы SAP GRC AC с перехода в ОПЭ (~6 мес.)

Статистика по управлению доступом

5,498 запросы от сотрудников зарегистрированы в GRC AC

3,780 завершено согласование и выполнено запросов

1,496 запросы отклонены при согласовании или отменены администратором

222 запросы ожидают согласования на различных этапах

Управление паролями в SAP

14,145 сбросов паролей в GRC и SAP выполнено с начала ОПЭ

4,311 сотрудника получили новые пароли с помощью сервиса сброса паролей

Владельцы ролей

174 Владельцев ролей назначено для согласования доступа в SAP

Матрица SoD-рисков

5 Бизнес-процессов имеют согласованную матрицу рисков

56 Рисков активны в системе SAP GRC AC

6 Рисков были уточнены за время ОПЭ в части правил определения на уровне транзакций и объектов полномочий

Реорганизация ролей блока «Финансы»

С 117 до 3 Снижение среднего количества ролей у сотрудника блока Финансы

С 67 до 0 Снижен % пользователей с рисками

Контроль SoD при запросах и изменении ролей SAP

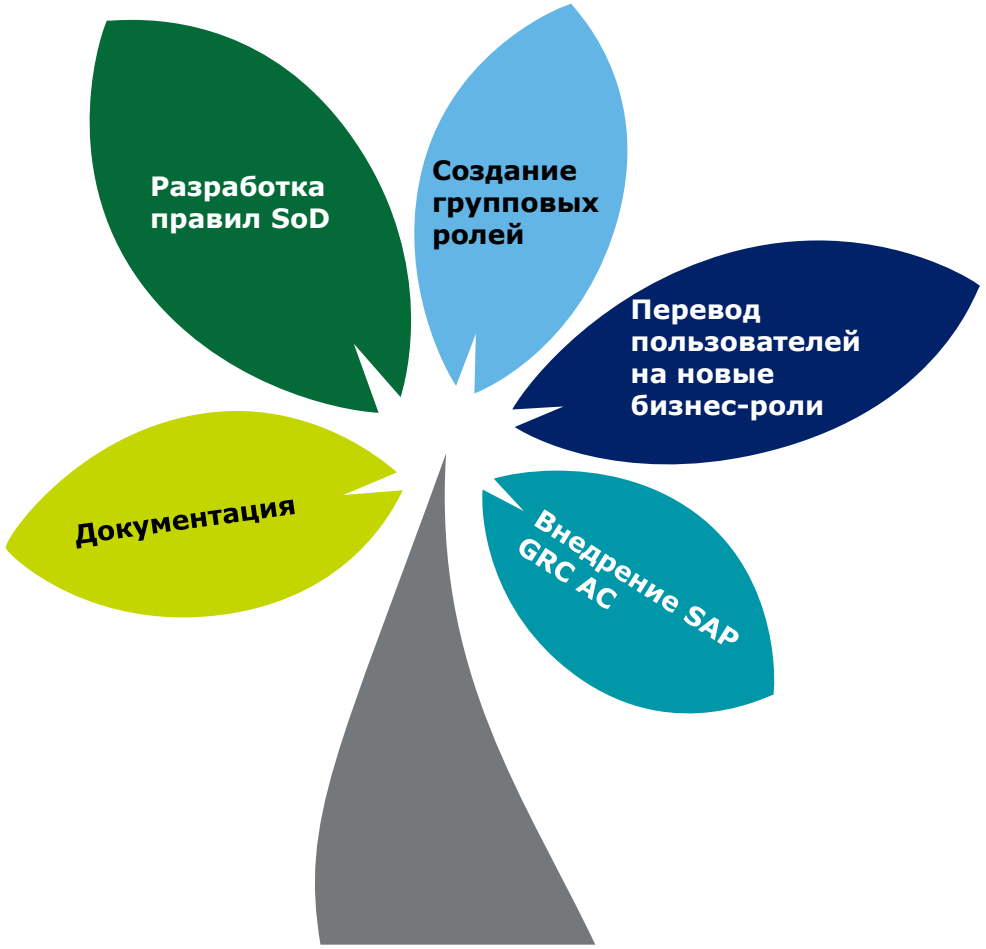
1,028 запросов проверено на этапе Ответственного за SoD

59 проведено проверок запросов на изменение ролей систем SAP

237 количество изменённых ролей SAP

569 общее количество ролей систем SAP, затронутых изменениями и участвовавших в проверке

Достижение целей



Внедрение SAP GRC AC
Внедрение и автоматизация процессов управления доступом в SAP-системах и процесса управления изменениями ролей на базе решения SAP GRC AC с автоматизированным контролем рисков конфликтов полномочий и критических полномочий.

Документация
Разработка и согласование следующих нормативных документов:
Регламент Р.12-450.5 «Предоставление доступа к системам SAP»
Регламент Р.50-45.54 «Управление изменениями ролей и полномочий в SAP системах»
Регламент Р.12-450.6 «Управление рисками конфликтов полномочий (SoD)»
Методика М.50-45.15 «Требования к ведению учётных записей пользователей в корпоративных информационных системах SAP
Методика М.12-450.7 «Управление рисками конфликтов полномочий
Методика М.50-45.14 «Требования к формированию ролей и полномочий в SAP системах»

Разработка правил SoD
Разработка правил разделения конфликтов полномочий в соответствии с утвержденным объемом и согласование их с владельцами бизнес-процессов.

Перевод пользователей на новые бизнес-роли
Перевод пользователей, работающих в процессе «Финансы», на новые бизнес-роли в системах SAP. Разработка ролей согласно требованиям новой НМД.

Создание групповых ролей
Создание групповых ролей во всех SAP-системах, исключение существовавших до проекта технических ролей для запроса. Исключение конфликтов полномочий в ролях до 98,5%.

Спасибо за внимание!

Балабанов Дмитрий
Руководитель направления
по интеллектуальным системам защиты
ДБ АО «ОМК»
dbalabanov@omk.ru