КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

27 СЕНТЯБРЯ 2018
ЕКАТЕРИНБУРГ

#CODEIB

Внедрение IDM-проекта в ПАО «СКБ-банк» Рекомендации при подготовке и внедрении

Яков Фишелев
Руководитель представительства в России и СНГ

ONE IDENTITY

IDM/IGA, DAG, SSO, 2FA, PAM

PAM, Analytics, Log management

18 Января 2018 компания Balabit стала частью One Identity

Успех и лидерство One Identity

Финансовый успех

$260M годовой доход

Самый большой IAM-focused производитель в мире

29% YoY рост (FY17)

Управление **130+ млн учетных записей** осуществляется с помощью решений One Identity

Лидер

отчета Gartner MQ IGA 2018 и Forrester Wave по решениям для управления идентификацией и доступом пользователей

Доля рынка IDM в России

в 2017 году около 30% среди всех IDM-проектов и 90% среди глобальных вендоров*

По данным ведущего интегратора IDM

18 Января 2018 компания Balabit стала частью One Identity

BALABIT

ONE IDENTITY™

Фокус на Россию

- Русский язык «из коробки»
- Локальный офис разработки 150+ человек
- Команда развития более 10 человек в СНГ
- Десятки проектов в России

Поддержка, отмеченная наградой

THE ASSOCIATION OF SUPPORT PROFESSIONALS Award Winner 2016 The Year's Ten Best Web Support Sites

Глубокая интеграция с SAP

Согласно отчету Gartner «Магический квадрант по решениям для администрирования и управления пользовательскими учетными записями»

7 000+

Клиентов решения One Identity в мире

Главный лидер

Отчета Kuppinger Cole Leadership Compass по решениям Access Governance

LeadershipCompass KuppingerCole Overall Leader Access Governance March 2013

Портфель продуктов One Identity

Комплексный контроль доступа

- **One Identity Manager (1IM)** – Комплексная система управления правами доступа уровня предприятия. Раздача прав при приеме/переводе/увольнении, организация ролевой модели, конструктор ролей, аттестация доступа, коннекторы к HR и целевым системам, конструктор коннекторов, портал для запроса доступа, цепочки согласования, делегирование, рисковая модель, контроль конфликтного доступа и разделение полномочий - SoD, обзор доступа на 360, отчетность и интерактивные панели управления и тд.
- **One Identity Manager – Data Governance Edition (1IM –DGE)** - расширение 1IM для неструктрированных данных на файловых серверах

One Identity

Эффективность доступа

- **Active Roles** – автоматизация рутиных процессов в AD, Exchange. «Облегченный» вариант IDM для MS среды
- **Password Manager** – Самостоятельный сброс паролей и разблокировка учетных записей пользователями.
- **Defender** – двухфакторная аутентификация. Soft и Hard токены.
- **Cloud Access Manager** – система единой точки входа для Web-приложений. Технология Reverse proxy.
- **Enterprise Single Sign-on** - система единой точки входа для любых приложений

Привилегированный доступ

- **Safeguard for Privileged Passwords** – Решение для выдачи административных паролей. Защищенный аплаенс.
- **Safeguard for Privileged Sessions**– выдача и запись административных сессий. Защищенный аплаенс.
- **Privileged Access Suite for Unix** - Аутентификация в UNIX/Linux через AD, управление Unix/Linux через групповые политики AD, делегирование полномочий, Расширение SUDO, контроль доступа, логирование ввода с клавиатуры.

Что такое IAM?

Аутентификация

“Кто я?”

Авторизация

“Что я могу делать?”

Администрирование

“Как все настроить правильно. Желательно автоматизировать?”

Аудит

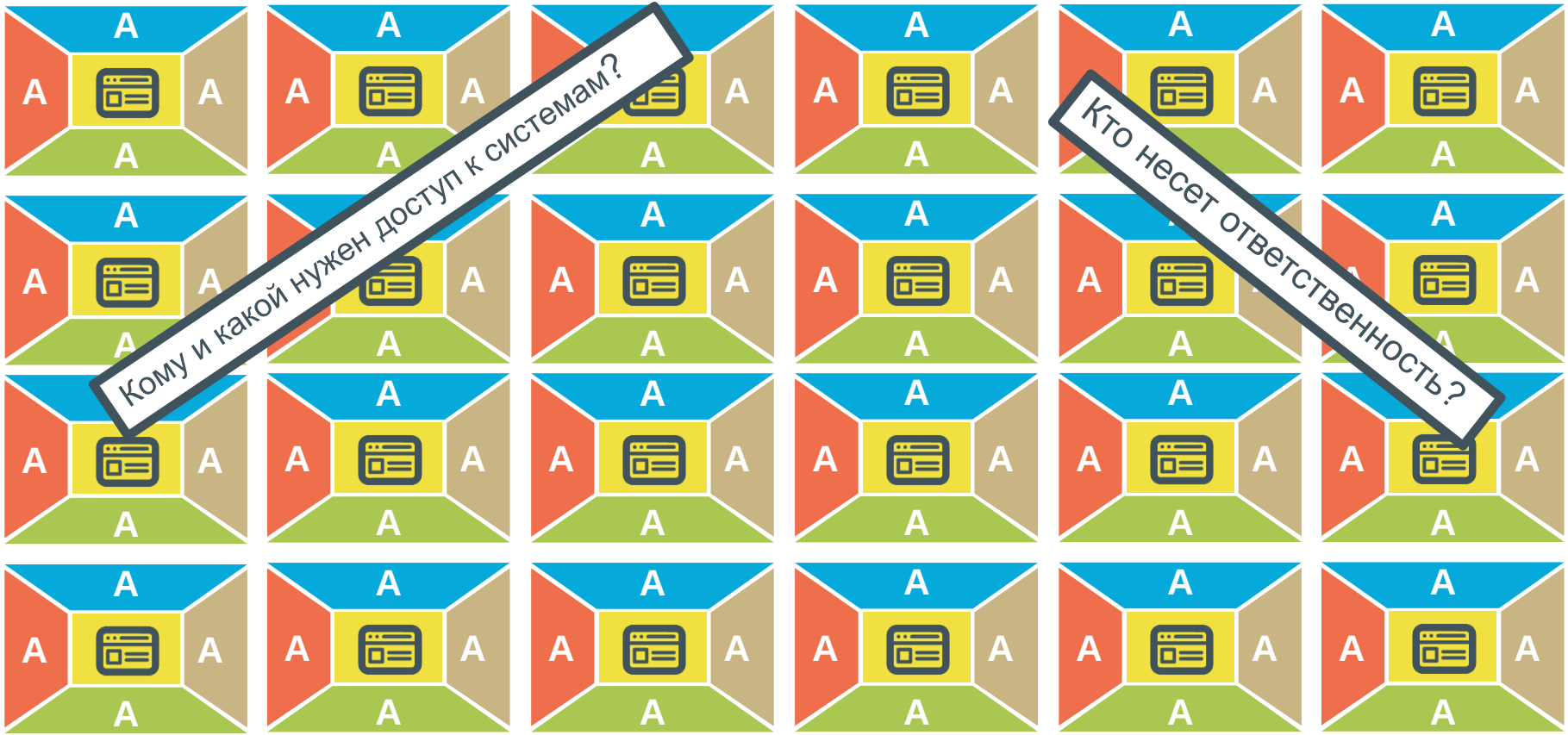
“Как убедиться, что все работает по правилам?”

Это нужно делать для каждой ИС и ресурса…

Кому предоставить права доступа к системам?

Кто несет ответственность?

В компаниях десятки систем….



Предпосылки. Операционные факторы

В среднем сотрудник имеет доступ к X различным приложениям*

1.5 дня

В среднем занимает процесс первоначального предоставления прав*

> 2 дней

В среднем занимает отзыв доступа*

Рядовой пользователь компании имеет минимум X паролей к системам компании*

* Источник: Aberdeen Group Research

- Сотрудники слишком долго ожидают предоставления прав доступа
- Администраторы перегружены задачами по предоставлению доступа
- В службу поддержки поступает слишком много запросов на сброс пароля

Предпосылки. Информационная безопасность

- Высокая трудоёмкость сбора данных о правах доступа сотрудников, об их согласовании и изменении
- После переводов по должности накапливаются избыточные права доступа
- Незаблокированные учётные записи уволенных сотрудников
- В информационных системах есть пользователи с несогласованными правами доступа
- Сотрудники имеют больше прав доступа, чем им необходимо
- Конфликты разделения ответственности при назначении полномочий

The New York Times

World Business

French Bank Says Rogue Trader Lost $7 Billion

By NICOLA CLARK and DAVID JOLLY
Published: January 25, 2008

Correction Appended

PARIS — A French bank announced Thursday that it had lost $7.2 billion, not because of complex subprime loans, but the old-fashioned way — because a 31-year-old rogue trader made bad bets on stocks and then, in trying to cover up those losses, dug himself deeper into a hole.

TWITTER
LINKEDIN
SIGN IN TO E-MAIL
PRINT
SINGLE PAGE
REPRINTS
SHARE

BROOKLYN
NOVEMBER 4
WATCH TRAILER

Jérôme Kerviel, 31, was a low-level bank employee.

Société Générale, one of France's largest and most respected banks, said an unassuming midlevel employee who made about 100,000 euros ($147,000) a year — identified by others as Jérôme Kerviel — managed to evade multiple layers of computer controls and audits for as long as a year, stacking up 4.9 billion euros in losses for the bank.

Unlike many of his high-level trading colleagues, Mr. Kerviel graduated not from one of France's elite

Bloomberg Our Company | Professional | Anywhere

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE TECH POLITICS SUSTAINABILI

Societe Generale Reports EU4.9 Billion Trading Loss (Update8)

France's Societe Generale Reports Biggest Trading Loss Ever by a Bank — Bloomberg

Societe Generale, France's second-largest bank by market value, said unauthorized bets on stock-index futures by an unidentified employee caused a 4.9 billion-euro, or $7.2 billion trading loss, the largest in banking history.

The graphic on the right lists some the biggest and most notable losses by rogue traders.

Company (Country): Year		Cause of loss
Societe Generale (France): 2008	$7.2 billion	Stock-index futures
Amaranth Advisors (U.S.): 2006	$6.6 billion	Natural-gas futures
Sumitomo (Japan): 1996	$2.6 billion	Copper futures
Barings (U.K.): 1995	$1.8 billion	Asian futures
Allied Irish Banks (Ireland): 2002	$691 million	Currency options

By Gregory Viscusi and Anne-Sylvaine Chassany - January 24, 2008 15:29 EST

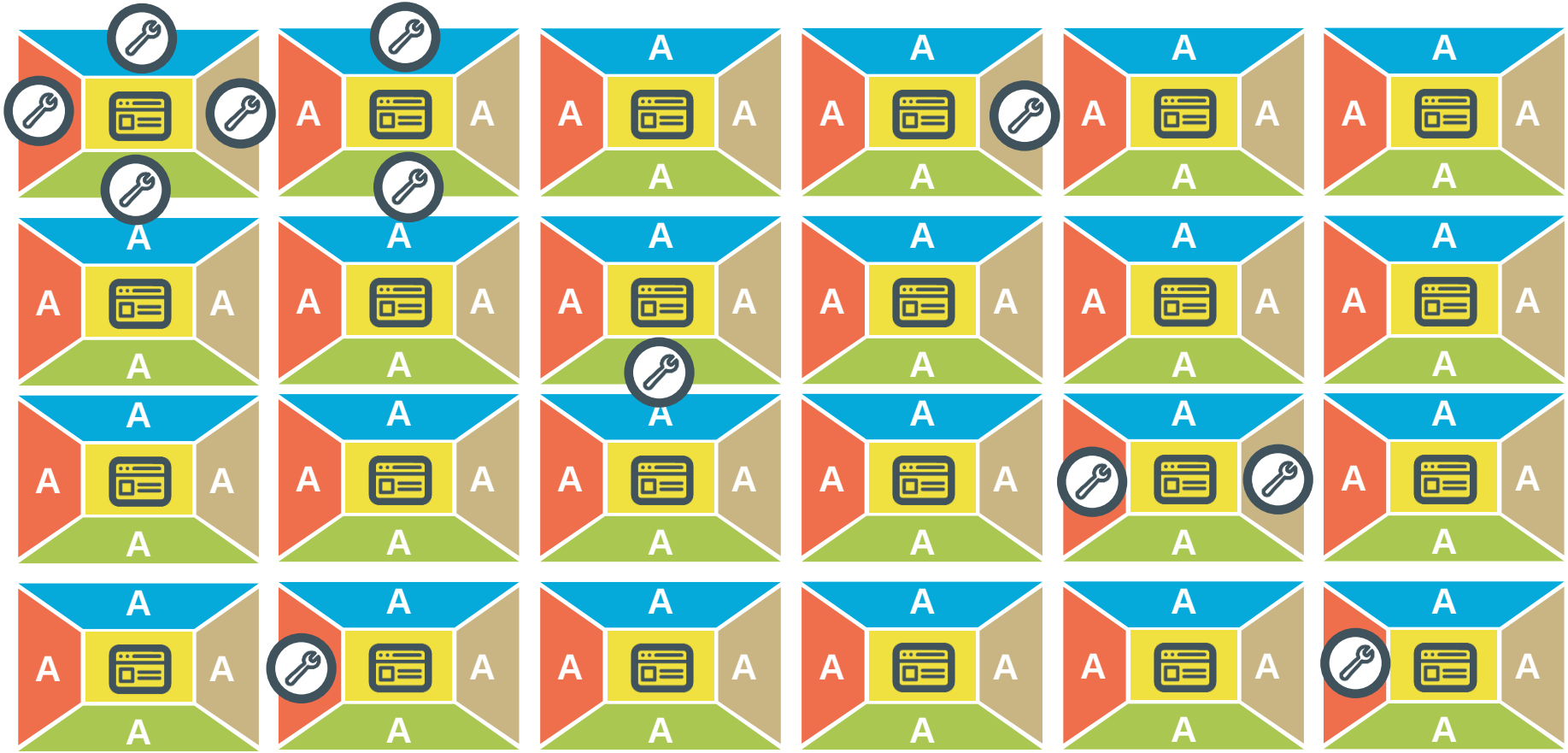
ONE IDENTITY

Предпосылки. Требования стандартов и аудиторов

- *Должно контролироваться создание, изменение и удаление идентификационных данных (PCI DSS n.8.5.1)*
- *Предоставление полномочий должно быть согласованным, контролируемым (PCI DSS n.7.1.3, ISO 27001 n.11.2.2)*
- *Права доступа должны незамедлительно отзываться при увольнении сотрудника, пересматриваться при переводе по должности (PCI DSS n.8.5.4)*
- *Руководство должно осуществлять периодически пересмотр прав доступа пользователей, используя формальный процесс (ISO 27001 n.11.2.4)*
- *Обязанности и области ответственности должны быть разграничены (ISO 27001 n.10.1.3)*

Выбор компании

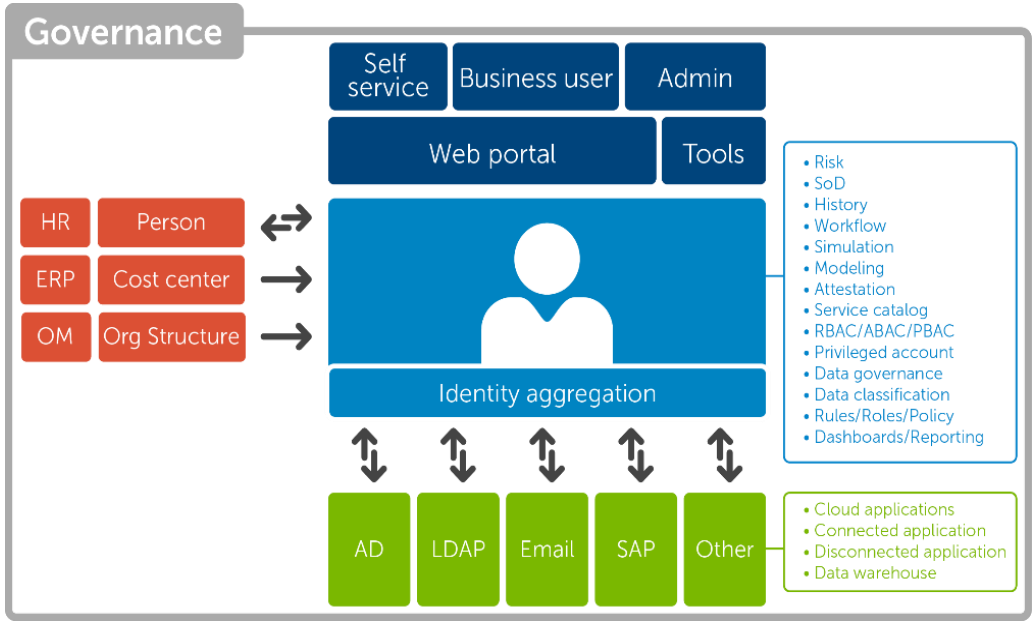
- Оставить все как есть
- Разрозненные иструменты для разных задач
- Централизованная платформа IAM



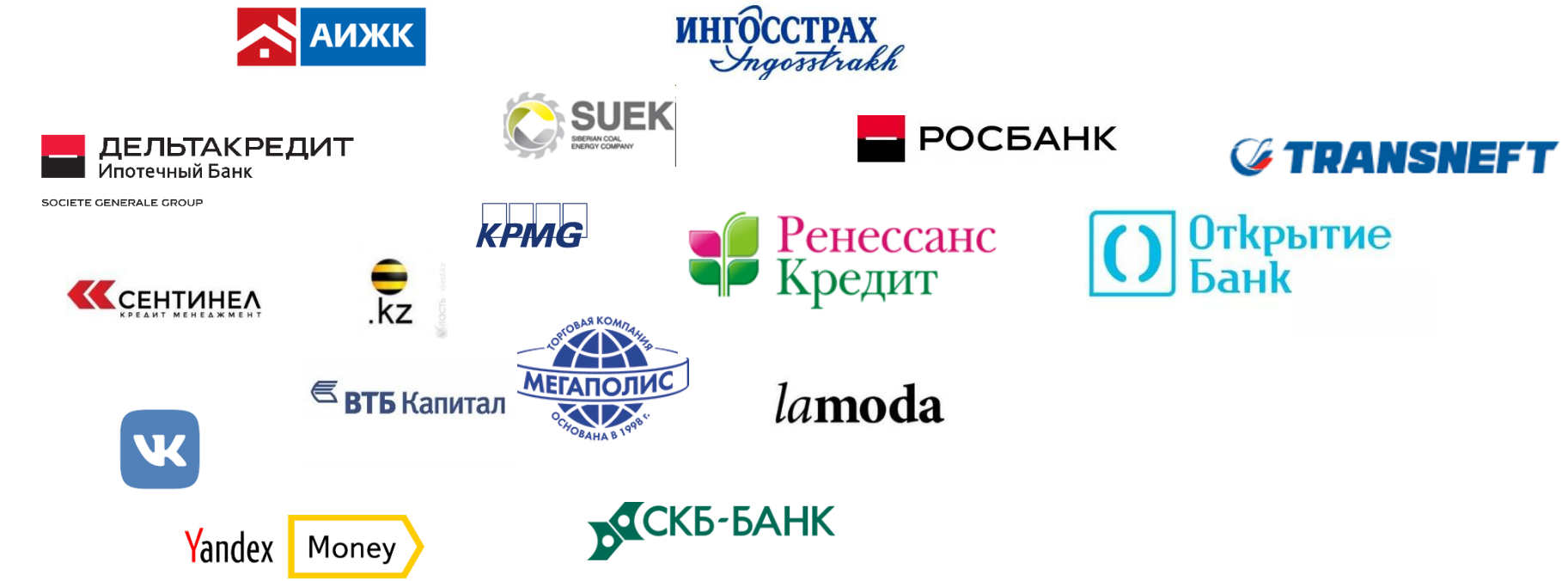
…Унификация IAM по всем системам…

Комплексное управление доступом, построенное как единое решение – One Identity Manager (1IM)

- Жизненный цикл информации о сотруднике и доступе
- Ролевая модель доступа
- Заявки и согласование доступа
- Сертификация доступа
- Контроль доступа и анализ рисков
- Разделение полномочий
- Отчетность и аналитика



Логотипы клиентов One Identity Manager в СНГ



Количество пользователей

500+ **1000+** **10 000+** **20 000+**

ONE IDENTITY

Логотипы некоторых клиентов One Identity в мире

Количество пользователей

2 000- **10 000+** **20 000+** **350 000+**

ONE IDENTITY

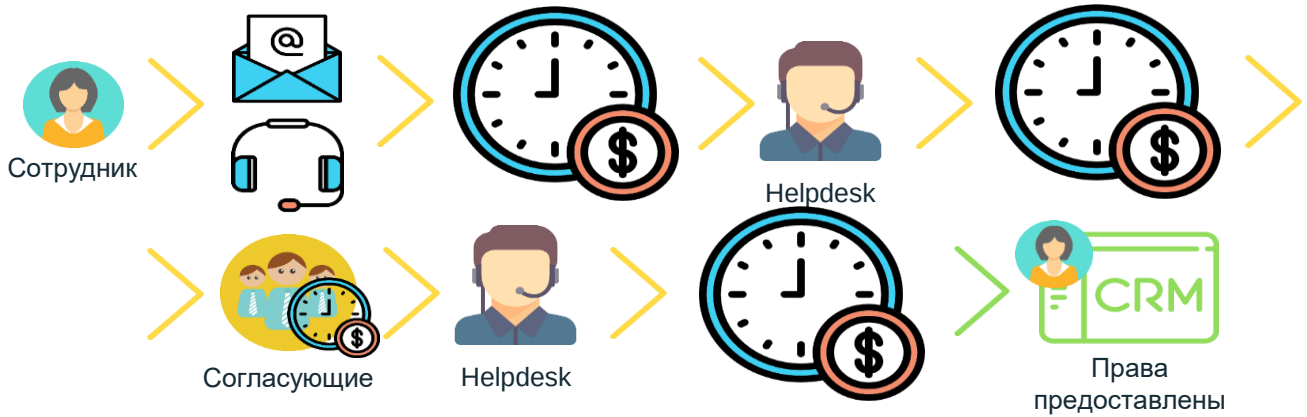
Внедрение 1IM в ПАО «СКБ-банк» г Екатеринбург

One Identity

Предпосылки к внедрению системы класса IDM/IGA

СКБ-БАНК

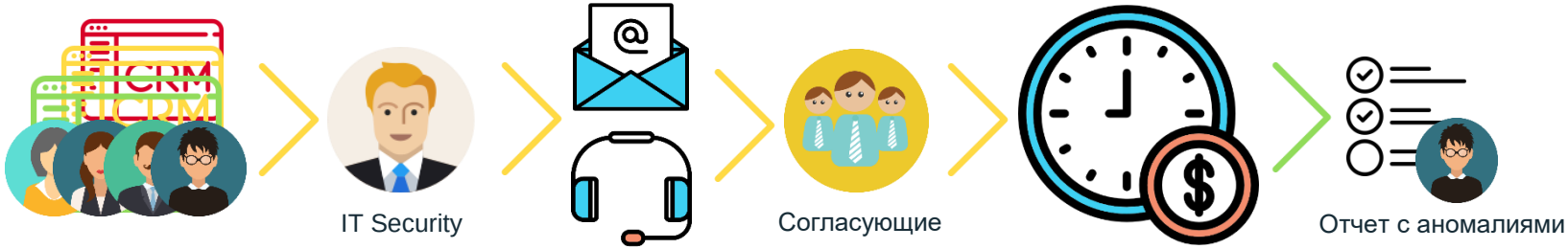
1. Ожидание доступа при устройстве составляло **1-2 дня**. Бумажные заявки, согласование, назначение



2. Затраты ИТ-специалистов на предоставление прав доступа можно было оценить в **3 ФОТ**

Предпосылки к внедрению системы класса IDM/IGA

3. Требовался контроль и прозрачность. Возможность быстрого аудита



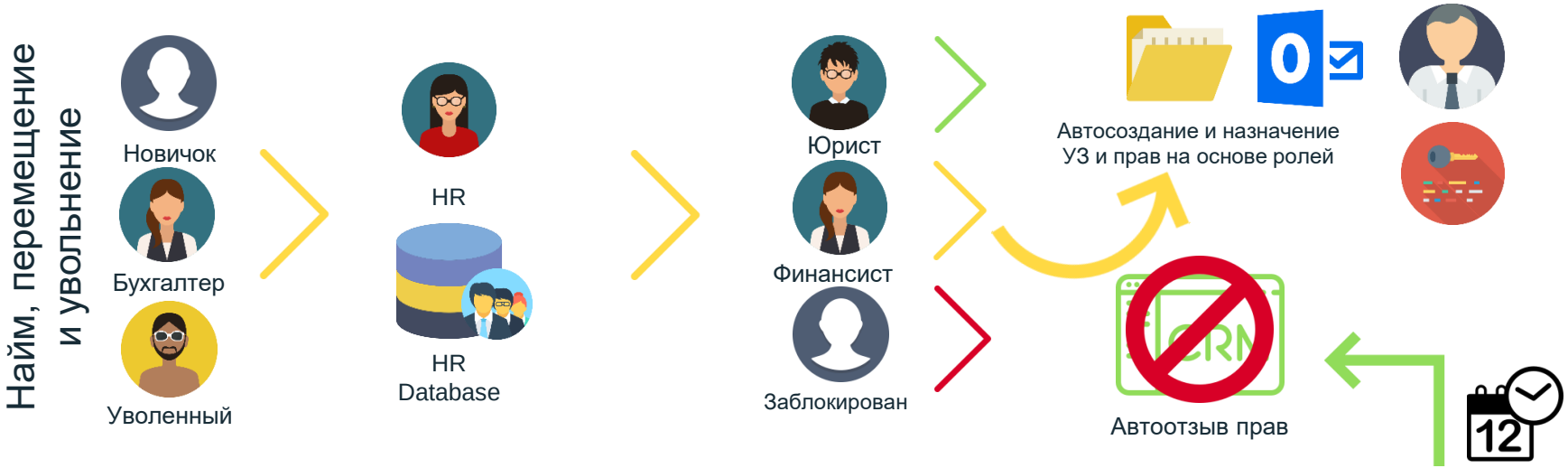
4. Процессс восстановления забытого пароля к системе через Service Desk иногда занимал **4-5 часов**

Результаты внедрения IGA/IDM проекта

СКБ-БАНК

1. Время назначения прав при кадровых событиях сократилось до **пары минут**
2. ИТ-специалисты переорентировались на более интересные задачи. **~~3 ФОТ~~**

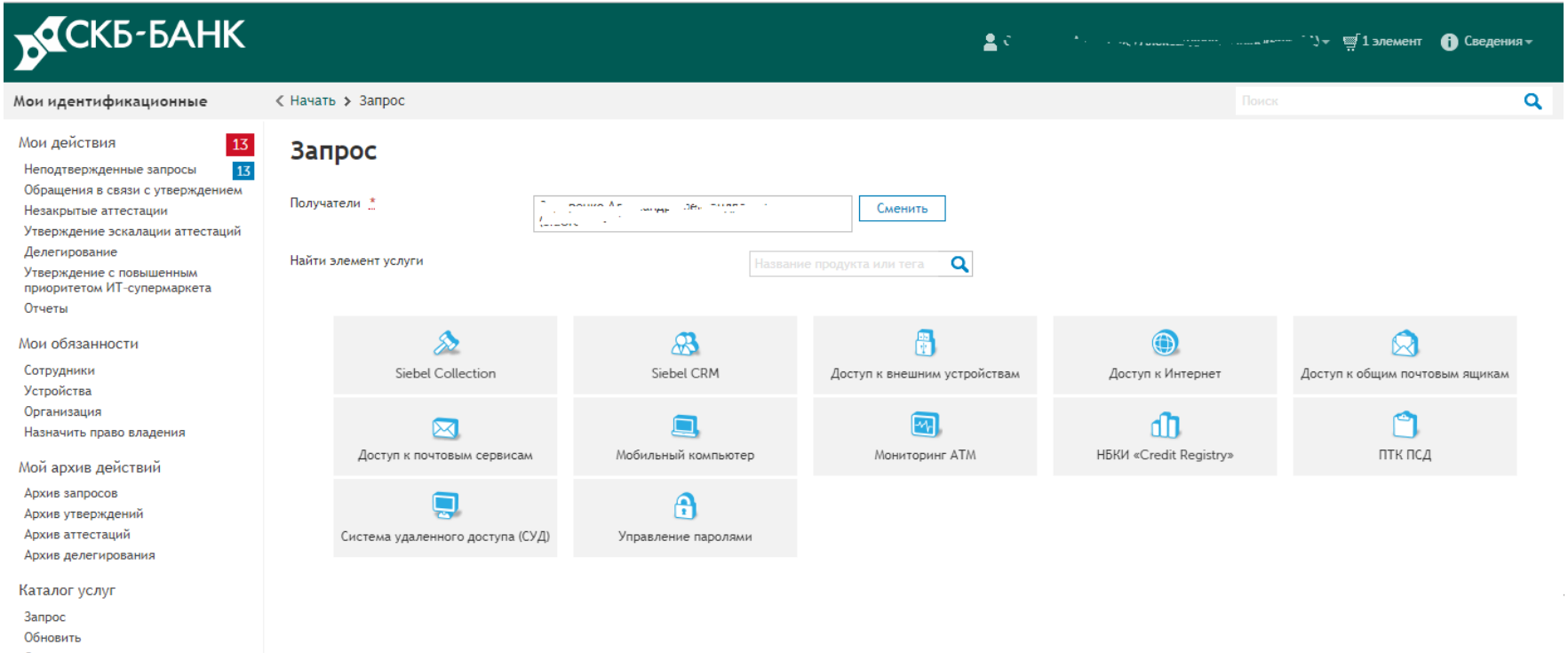
(Пример: почтовый ящик создается по правилам на нужном сервере, определенного объма)



ONE IDENTITY

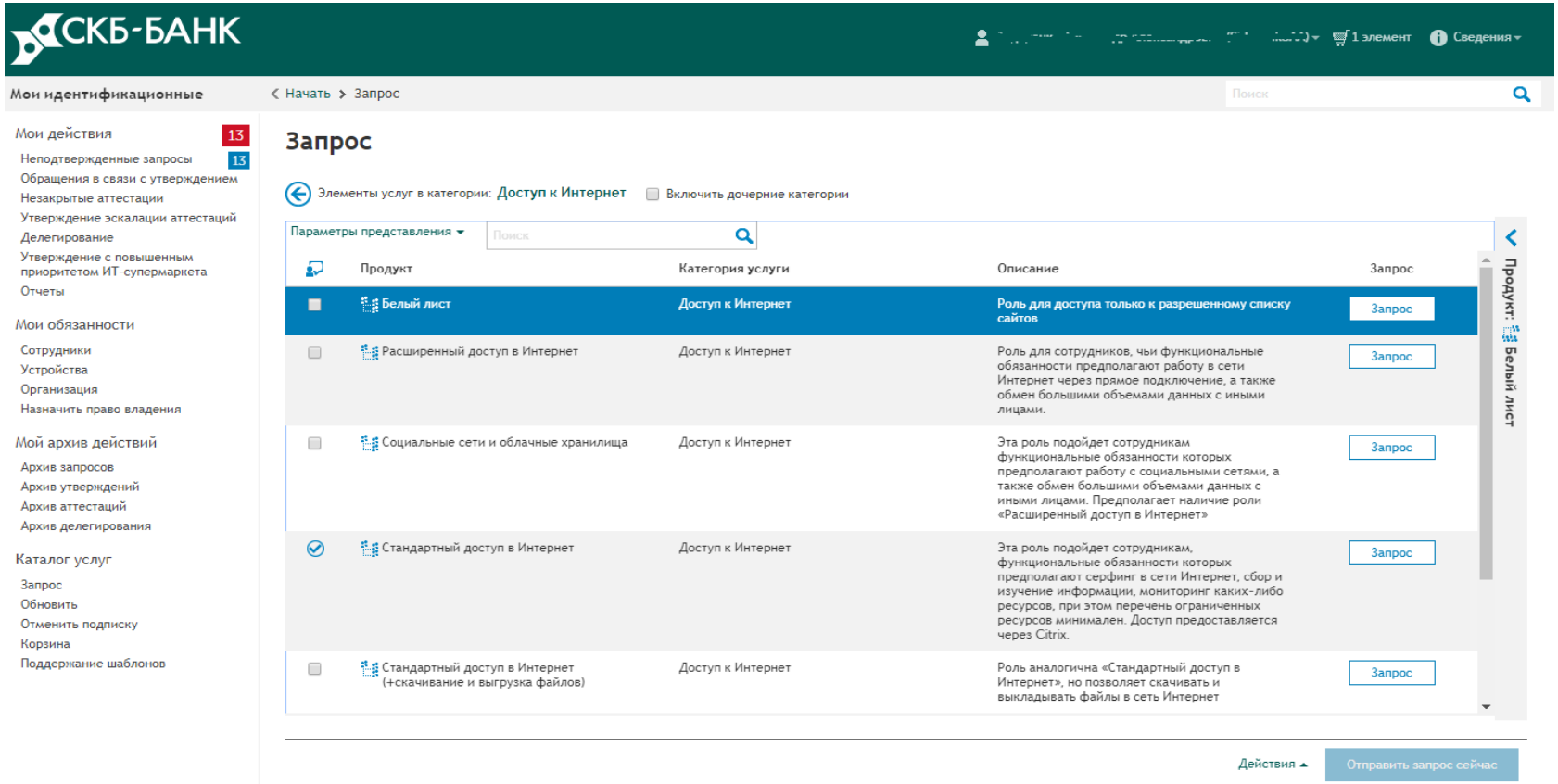
Результаты внедрения IGA/IDM проекта

3. Создается ролевая модель → Количество заявок уже снизилось до **300 заявок** в неделю
4. Развитие портала самообслуживания. Пользователи активны.
5. Самостоятельный сброс пароля – **5 мин**



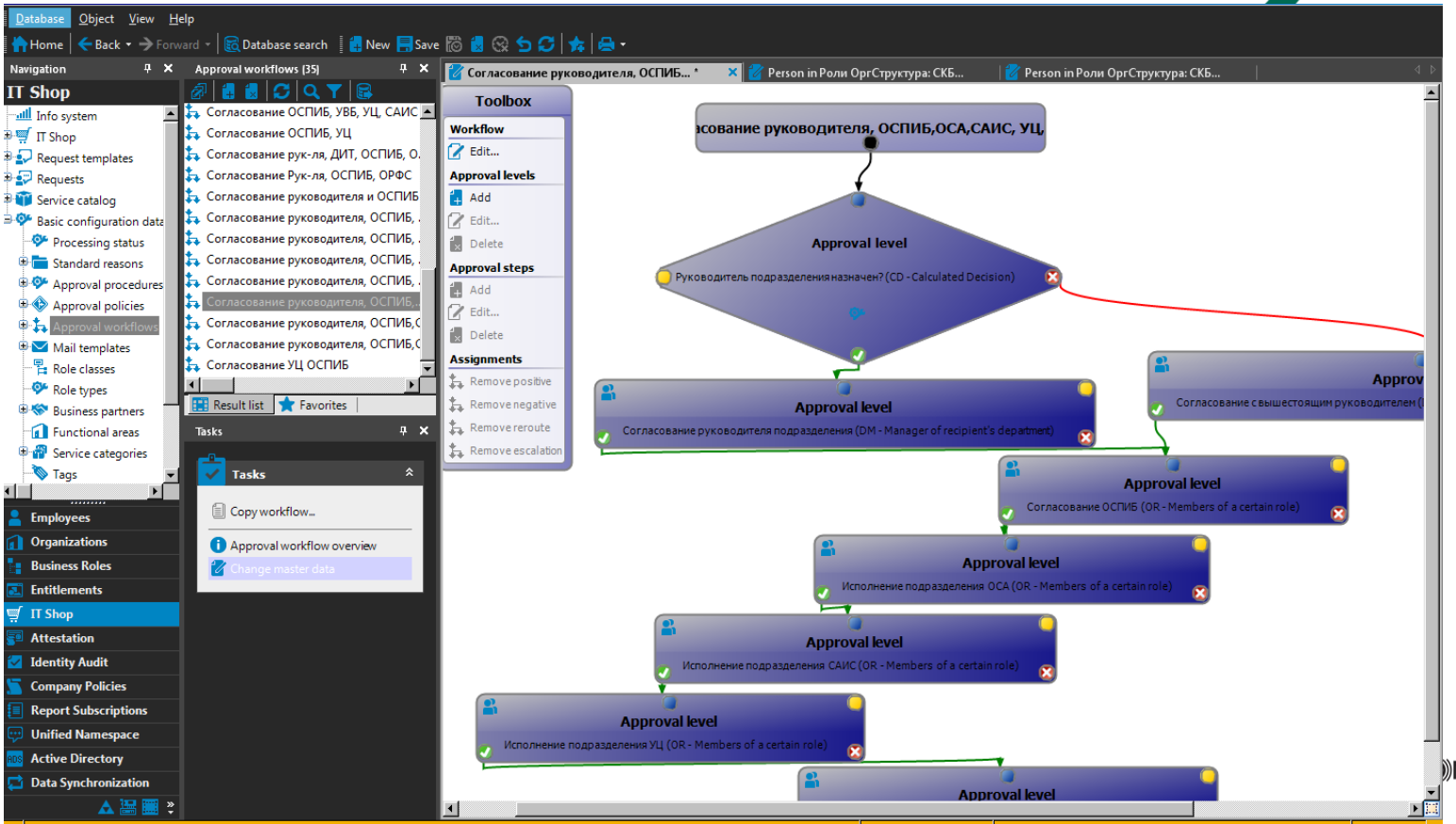
Результаты внедрения IGA/IDM проекта

Описание на понятном бизнесу языке



Пример настройки цепочки согласования

Интерфейс manager для инженерных настроек



Результаты внедрения IGA/IDM проекта

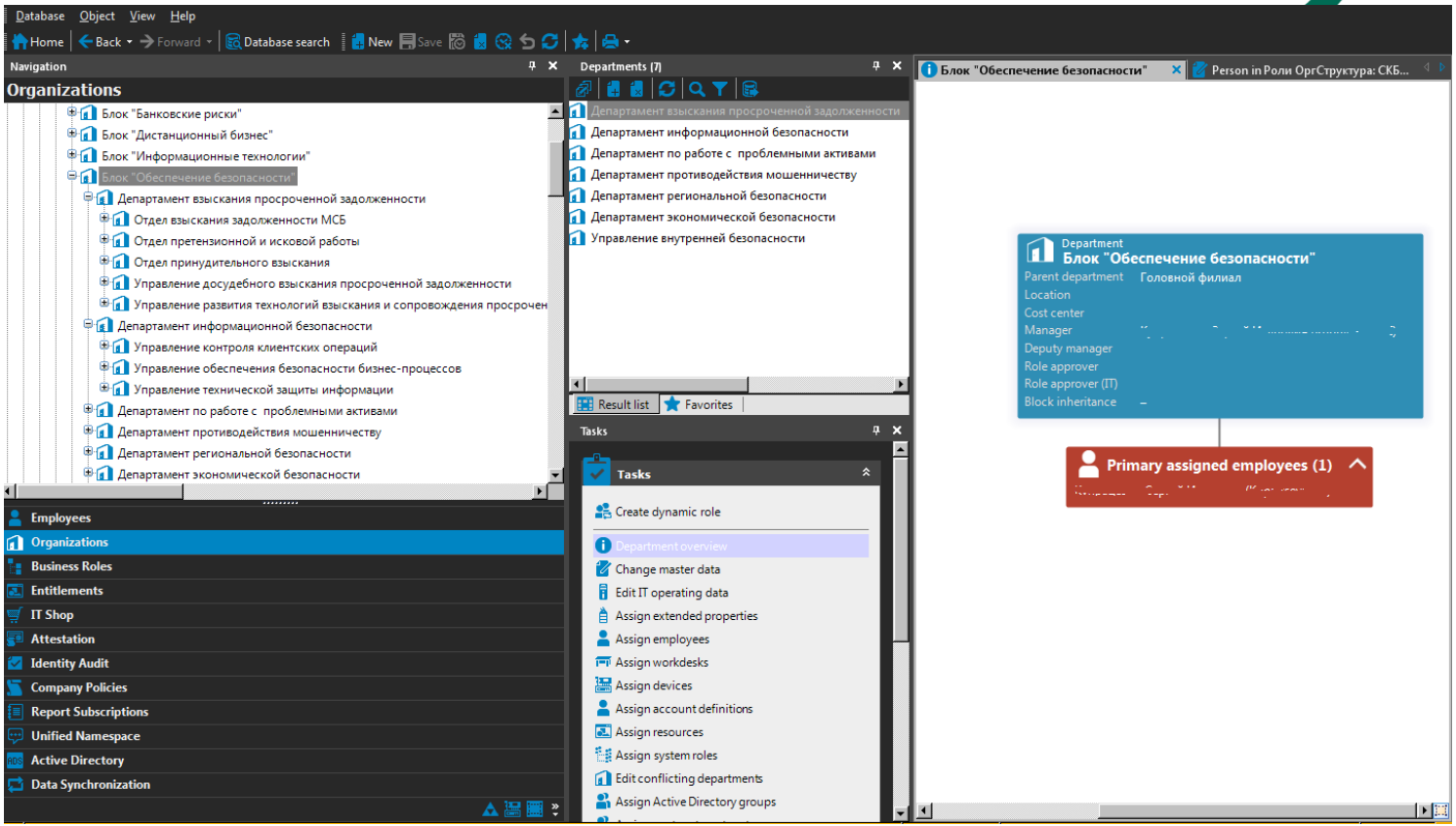
6. ИБ-отдел постепенно реализует задачу польного контроля над доступом в компании. Кто? Куда имеет доступ? Почему? В какой момент времени? Кто согласовал? Не конфликтуют ли доступы?

Инвентаризация AD с Кадрами позволила выявить **несколько сотен** бесхозных учеток без владельца

Пример обзора сотрудника на 360

Использование оргструктуры в IDM

Интерфейс manager для инженерных настроек



Оповещения по почте

От: idm@skbbank.ru
Кому:
Копия:
Тема: IDM | Запрос на предоставление доступа отклонен

Добрый день!

Запрос на предоставление доступа, оформленный на портале «Управление доступом к системам», не согласован и был отклонен.

Наименование доступа: Мобильный компьютер. Удаленный доступ

Автор заявки:
Получатель доступа:

Обоснование запроса: тест

Информация о последнем этапе согласования запроса:

Причина отказа: .....

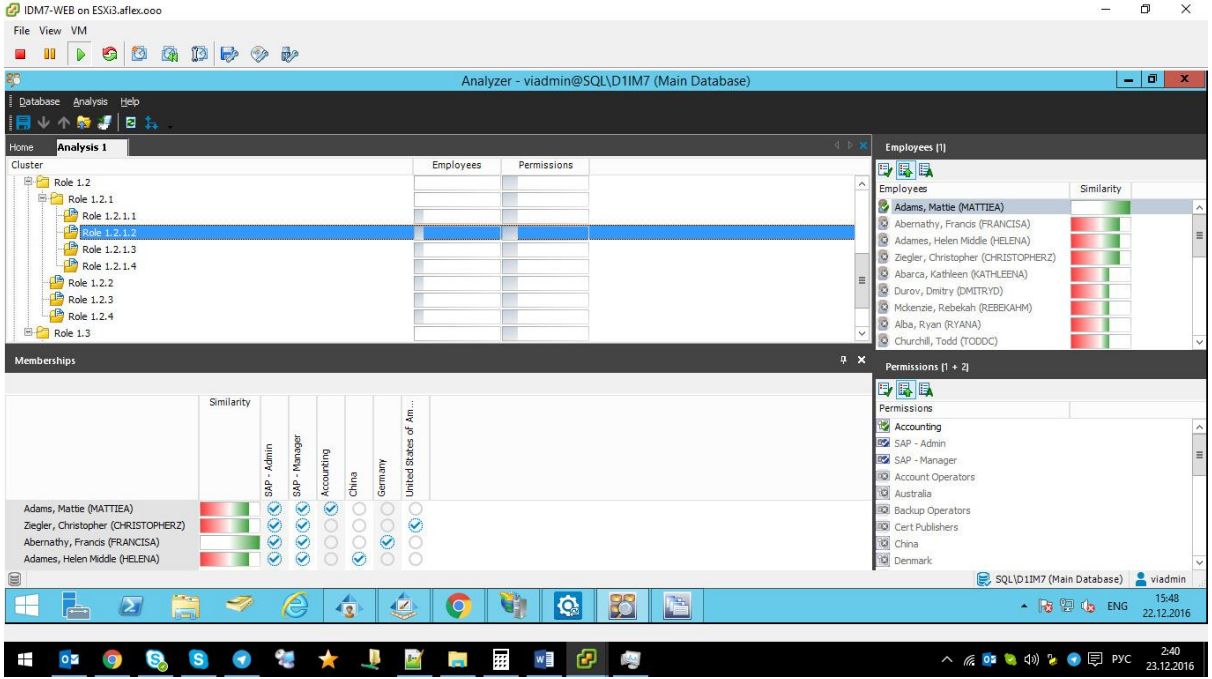
Вы можете перейти на Управление доступом к системам для просмотра истории согласования запроса.

ВНИМАНИЕ!!! Данное письмо автоматически сгенерировано системой. Отвечать на него не нужно.

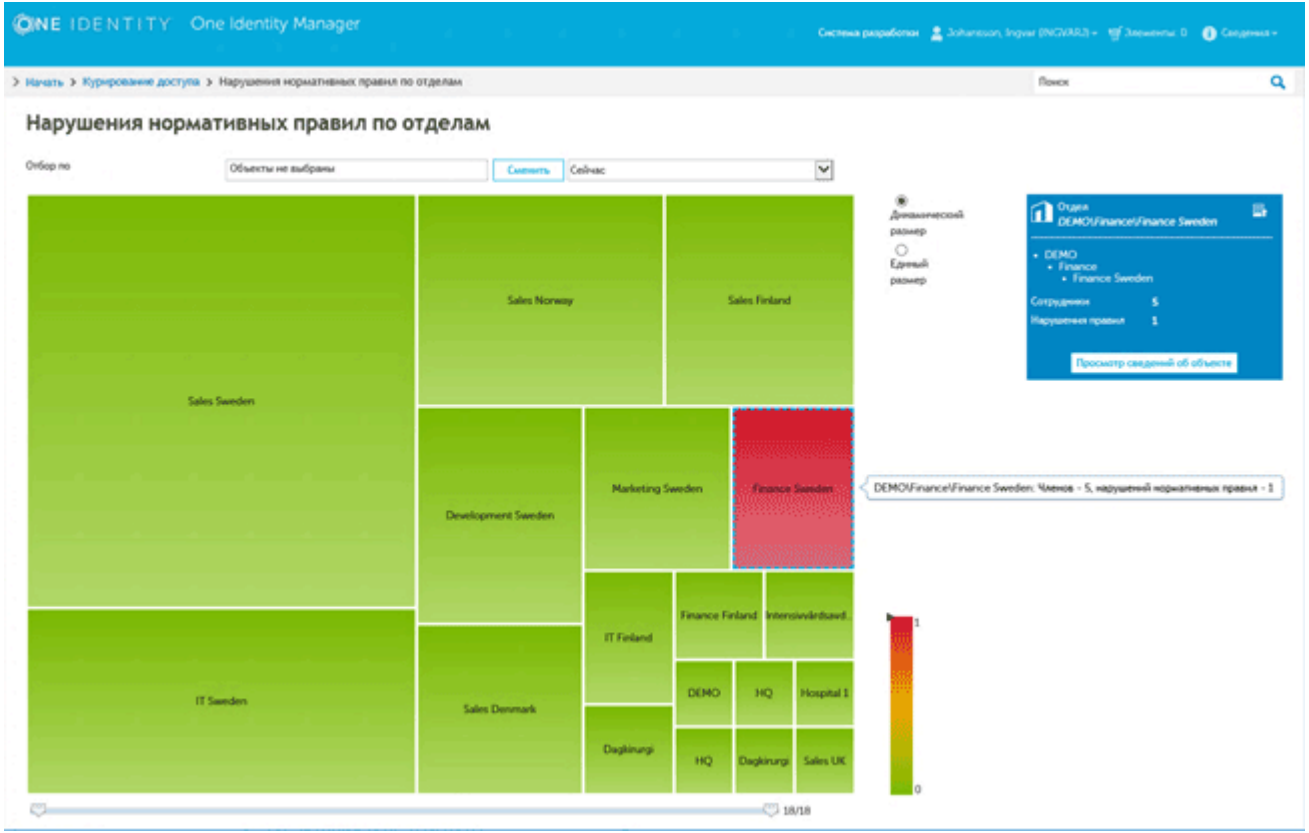
Некоторые другие возможности 1IM

One Identity

Конструктор ролей – Analyzer

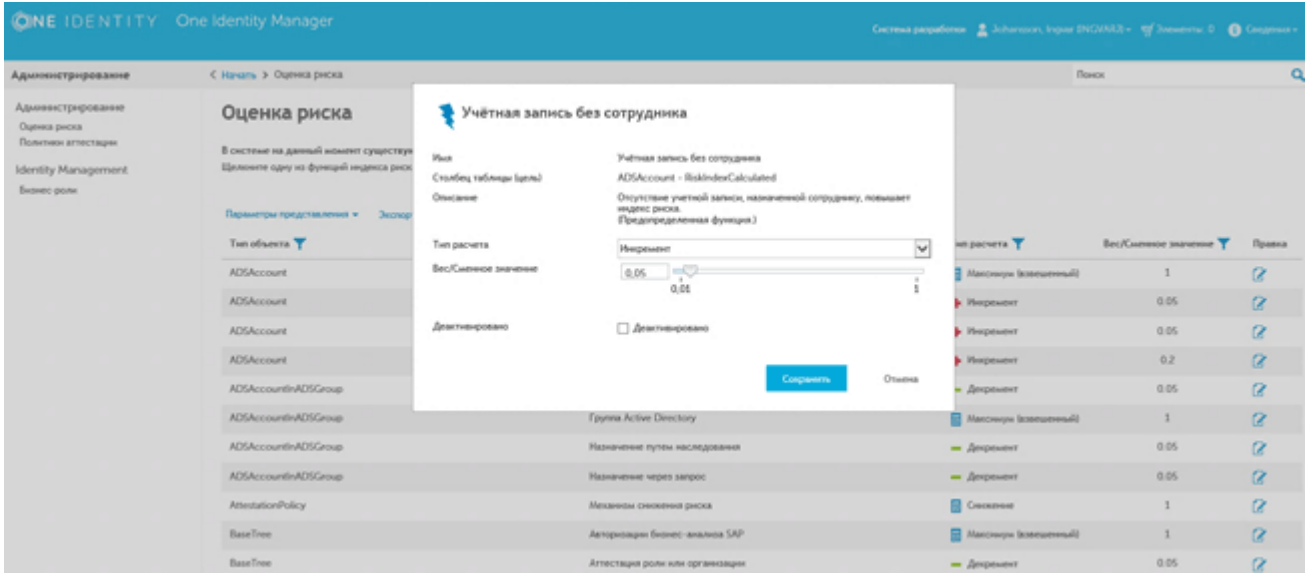


Карта самых проблемных мест в нарушении политик



Настройки правил расчёта индекса риска

Тонкая настройка повышающих и понижающих коэффициентов индекса риска



Рекомендации при выборе IDM/IGA

- Не доверять сравнительным таблицам
- Демо не достаточно
- Делать POC и тестировать ключевые сценарии
- Обязательно сходить на референс
- Возможность самостоятельно развивать решение
- Зрелость решения и количество внедрений
- Локальная команда вендора
- Разбить внедрение на этапы
- Не заниматься долгим предпроектным консалтингом, а начинать внедрение


ONE IDENTITY™