



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



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

\$260М 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



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



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



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 неструктурированных данных на файловых серверах

One Identity

Эффективность доступа

- **Active Roles** - автоматизация рутинных 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
ответствен
ность?

В компаниях десятки систем....



Предпосылки. Операционные факторы

27

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*

6

* 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.

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



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

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

BROOKLYN
NOVEMBER 4
[WATCH TABLE]

Bloomberg Our Company | Professional | Anywhere

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE TECH POLITICS SUSTAINABILITY

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

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

Company (Country): Year	Loss	Cause of loss
Societe Generale (France): 2008	\$7.2 billion	Stock-index futures
Amaranth Advisors (U.S.): 2006	\$6.6 billion	Natural-gas futures
Somitema (Japan): 1996	\$2.6 billion	Copper futures
Barings (U.K.): 1995	\$1.8 billion	Asian futures
Allied Irish Banks (Ireland): 2002	\$993 million	Currency options

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

By Gregory Viscusi and Anne-Sylvaine Chassagny - January 24, 2008 15:20 EST

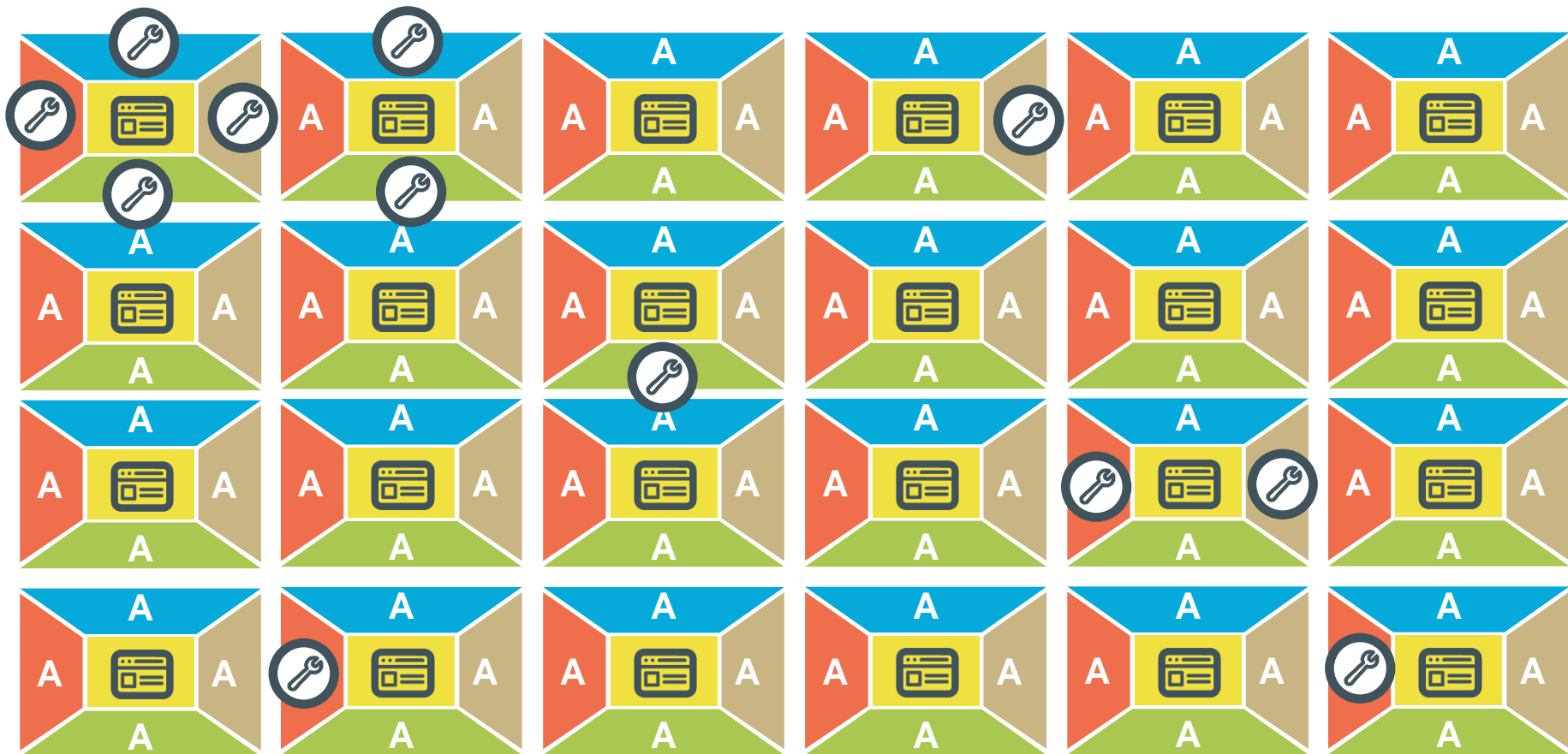
Предпосылки. Требования стандартов и аудиторов



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

Выбор компании

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

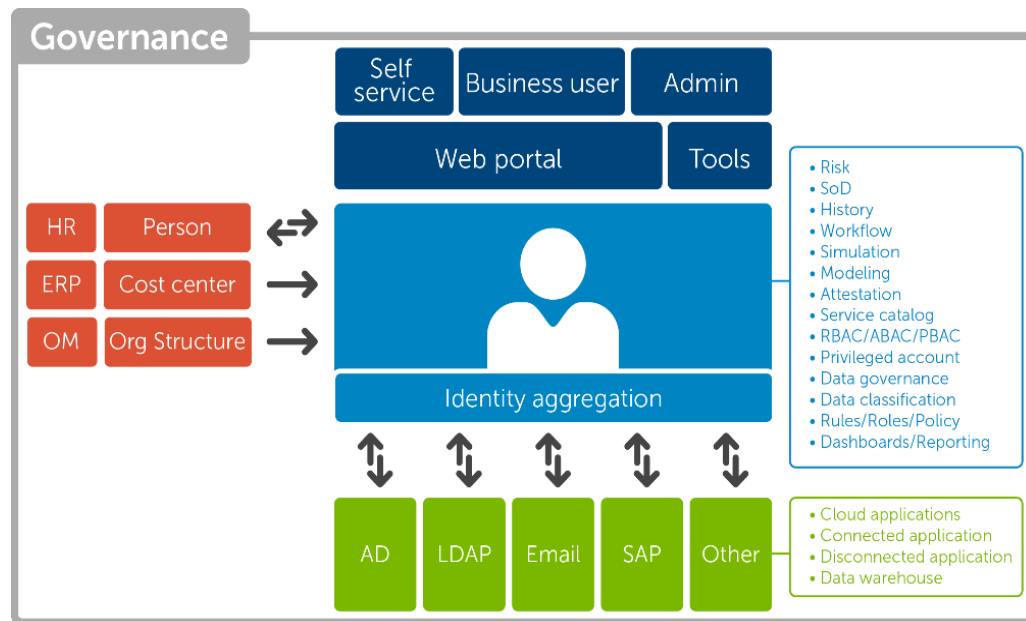


...Унификация IAM по всем системам...



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



SOCIETE GENERALE GROUP



Количество пользователей

500+

1000+

10 000+

20 000+

Логотипы некоторых клиентов One Identity в мире

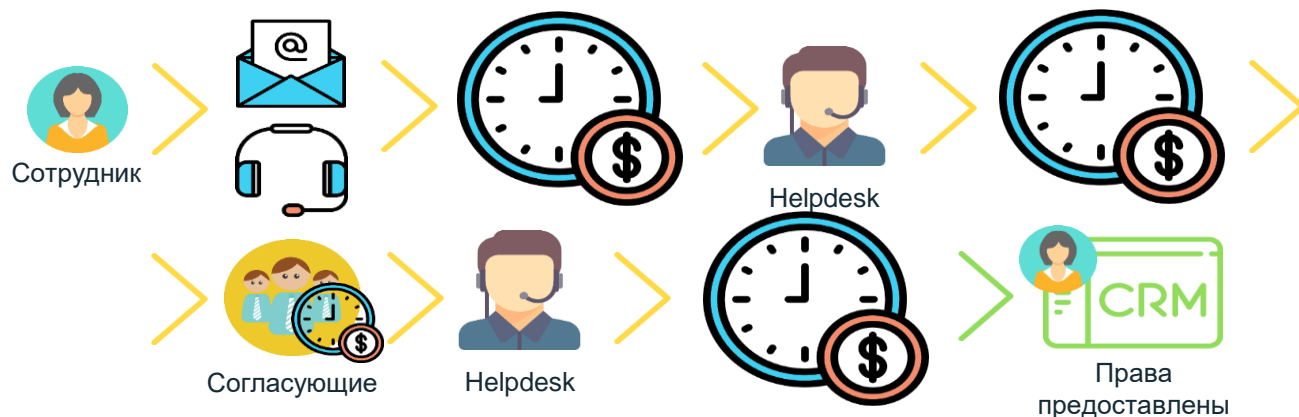


Внедрение 1ИМ в ПАО «СКБ-банк» г Екатеринбург

Предпосылки к внедрению системы класса IDM/IGA



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

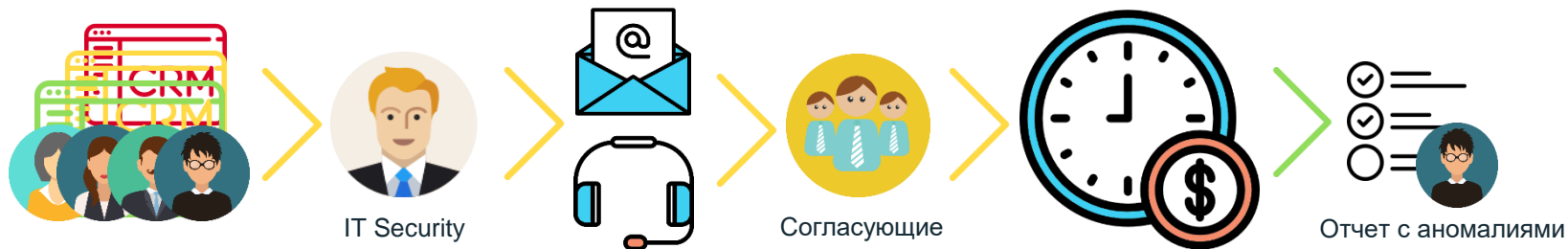


2. Затраты ИТ-специалистов на предоставление прав доступа можно было оценить в 3 ФОТ

Предпосылки к внедрению системы класса IDM/IGA



3. Требовался контроль и прозрачность. Возможность быстрого аудита

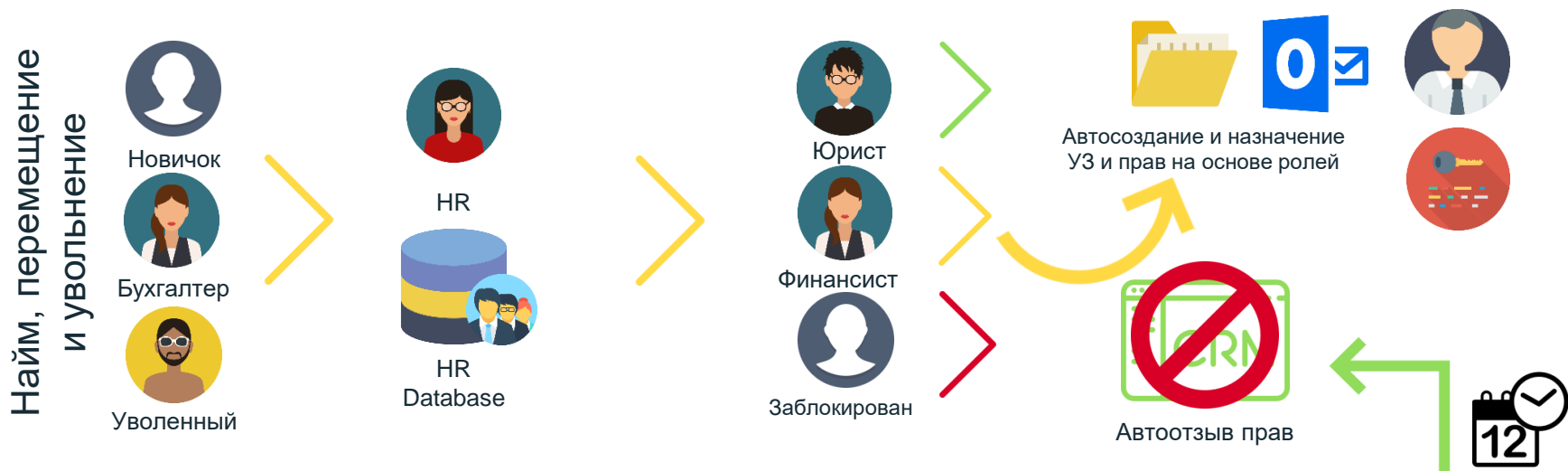


4. Процесс восстановления забытого пароля к системе через Service Desk иногда занимал 4-5 часов

Результаты внедрения IGA/IDM проекта



1. Время назначения прав при кадровых событиях сократилось до **пары минут**
2. ИТ-специалисты переориентировались на более интересные задачи. **3 ФОТ**
(Пример: почтовый ящик создается по правилам на нужном сервере, определенного объема)




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**

The screenshot displays the user interface of the Sberbank self-service portal. At the top, the Sberbank logo and name are visible on the left, and user account information and a search bar are on the right. The main navigation bar includes 'Мои идентификационные' and 'Запрос'. The 'Запрос' section is active, showing a search bar for 'Получатели' and a 'Сменить' button. Below this is a search bar for 'Найти элемент услуги'. The main content area features a grid of service tiles, each with an icon and a label: Siebel Collection, Siebel CRM, Доступ к внешним устройствам, Доступ к Интернет, Доступ к общим почтовым ящикам, Доступ к почтовым сервисам, Мобильный компьютер, Мониторинг АТМ, НБКИ «Credit Registry», ПТК ПСД, Система удаленного доступа (СУД), and Управление паролями. A left sidebar contains navigation links for 'Мои действия' (with a red '13' badge), 'Мои обязанности', 'Мой архив действий', and 'Каталог услуг'.

Результаты внедрения IGA/IDM проекта

Описание на понятном бизнесу языке

1 элемент Сведения

Мои идентификационные < Начать > Запрос

Мои действия

- Неподтвержденные запросы 13
- Обращения в связи с утверждением 13
- Незакрытые аттестации
- Утверждение эскалации аттестаций
- Делегирование
- Утверждение с повышенным приоритетом ИТ-супермаркета
- Отчеты

Мои обязанности

- Сотрудники
- Устройства
- Организация
- Назначить право владения

Мой архив действий

- Архив запросов
- Архив утверждений
- Архив аттестаций
- Архив делегирования






Каталог услуг

- Запрос
- Обновить
- Отменить подписку
- Корзина
- Поддержание шаблонов

Запрос

← Элементы услуг в категории: **Доступ к Интернет** Включить дочерние категории

Параметры представления

Продукт	Категория услуги	Описание	Запрос
<input checked="" type="checkbox"/>  Белый лист	Доступ к Интернет	Роль для доступа только к разрешенному списку сайтов	<input type="button" value="Запрос"/>
<input type="checkbox"/>  Расширенный доступ в Интернет	Доступ к Интернет	Роль для сотрудников, чьи функциональные обязанности предполагают работу в сети Интернет через прямое подключение, а также обмен большими объемами данных с иными лицами.	<input type="button" value="Запрос"/>
<input type="checkbox"/>  Социальные сети и облачные хранилища	Доступ к Интернет	Эта роль подойдет сотрудникам функциональные обязанности которых предполагают работу с социальными сетями, а также обмен большими объемами данных с иными лицами. Предполагает наличие роли «Расширенный доступ в Интернет»	<input type="button" value="Запрос"/>
<input checked="" type="checkbox"/>  Стандартный доступ в Интернет	Доступ к Интернет	Эта роль подойдет сотрудникам, функциональные обязанности которых предполагают серфинг в сети Интернет, сбор и изучение информации, мониторинг каких-либо ресурсов, при этом перечень ограниченных ресурсов минимален. Доступ предоставляется через Citrix.	<input type="button" value="Запрос"/>
<input type="checkbox"/>  Стандартный доступ в Интернет (+скачивание и выгрузка файлов)	Доступ к Интернет	Роль аналогична «Стандартный доступ в Интернет», но позволяет скачивать и выкладывать файлы в сеть Интернет	<input type="button" value="Запрос"/>

Действия

22

Пример настройки цепочки согласования

Интерфейс manager для инженерных настроек



The screenshot displays the configuration interface for approval workflows. On the left, a navigation pane shows the 'Approval workflows' section. The main area shows a workflow diagram with the following steps:

- Task: **Согласование руководителя, ОСПИБ, ОСА, САИС, УЦ**
- Decision: **Approval level** (Condition: **Руководитель подразделения назначен? (CD - Calculated Decision)**)
- Task: **Approval level** (Condition: **Согласование руководителя подразделения (DM - Manager of recipient's department)**)
- Task: **Approval level** (Condition: **Согласование с вышестоящим руководителем**)
- Task: **Approval level** (Condition: **Согласование ОСПИБ (OR - Members of a certain role)**)
- Task: **Approval level** (Condition: **Исполнение подразделения ОСА (OR - Members of a certain role)**)
- Task: **Approval level** (Condition: **Исполнение подразделения САИС (OR - Members of a certain role)**)
- Task: **Approval level** (Condition: **Исполнение подразделения УЦ (OR - Members of a certain role)**)

The interface also includes a 'Toolbox' with options for 'Workflow', 'Approval levels', 'Approval steps', and 'Assignments'. The 'Tasks' pane at the bottom left shows options like 'Copy workflow...', 'Approval workflow overview', and 'Change master data'.

Результаты внедрения IGA/IDM проекта



6. ИБ-отдел постепенно реализует задачу полного 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

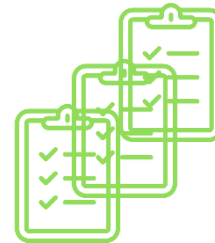
контроли ИБ



Аналитик
ИБ



IAM Web-Portal



Отчеты об
аномалиях,
нарушения,
аналитика, карты
рисков

Пример обзора сотрудника на 360



Использование оргструктуры в IDM

Интерфейс manager для инженерных настроек



The screenshot displays the IDM Manager interface with the following components:

- Navigation Panel (Left):** Shows a tree view of Organizations. The selected path is: **Блок "Обеспечение безопасности"** > **Департамент экономической безопасности**. Other visible organizations include "Банковские риски", "Дистанционный бизнес", and "Информационные технологии".
- Organizations Panel (Top Left):** Lists the selected organization and its sub-departments: **Департамент взыскания просроченной задолженности**, **Отдел взыскания задолженности МСБ**, **Отдел претензионной и исковой работы**, **Отдел принудительного взыскания**, **Управление досудебного взыскания просроченной задолженности**, **Управление развития технологий взыскания и сопровождения просроченной задолженности**, **Департамент информационной безопасности**, **Управление контроля клиентских операций**, **Управление обеспечения безопасности бизнес-процессов**, **Управление технической защиты информации**, **Департамент по работе с проблемными активами**, **Департамент противодействия мошенничеству**, **Департамент региональной безопасности**, and **Департамент экономической безопасности**.
- Departments Panel (Top Middle):** Shows a list of departments for the selected organization, including: **Департамент взыскания просроченной задолженности**, **Департамент информационной безопасности**, **Департамент по работе с проблемными активами**, **Департамент противодействия мошенничеству**, **Департамент региональной безопасности**, **Департамент экономической безопасности**, and **Управление внутренней безопасности**.
- Tasks Panel (Bottom Middle):** Lists available actions for the selected department: **Create dynamic role**, **Department overview** (highlighted), **Change master data**, **Edit IT operating data**, **Assign extended properties**, **Assign employees**, **Assign workdesks**, **Assign devices**, **Assign account definitions**, **Assign resources**, **Assign system roles**, **Edit conflicting departments**, and **Assign Active Directory groups**.
- Department Overview Panel (Right):** Displays details for the selected department: **Блок "Обеспечение безопасности"**. Fields include: **Parent department** (Головной филиал), **Location**, **Cost center**, **Manager**, **Deputy manager**, **Role approver**, **Role approver (IT)**, and **Block inheritance** (set to -).
- Primary assigned employees (1) Panel (Bottom Right):** Shows a list of employees assigned to the department.
- Bottom Panel:** Contains a list of system-wide settings: **Employees**, **Organizations** (selected), **Business Roles**, **Entitlements**, **IT Shop**, **Attestation**, **Identity Audit**, **Company Policies**, **Report Subscriptions**, **Unified Namespace**, **Active Directory**, and **Data Synchronization**.

Оповещения по почте



От: idm@skbbank.ru
Кому: [redacted]
Копия: [redacted]
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: [redacted]

Получатель доступа: [redacted]

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

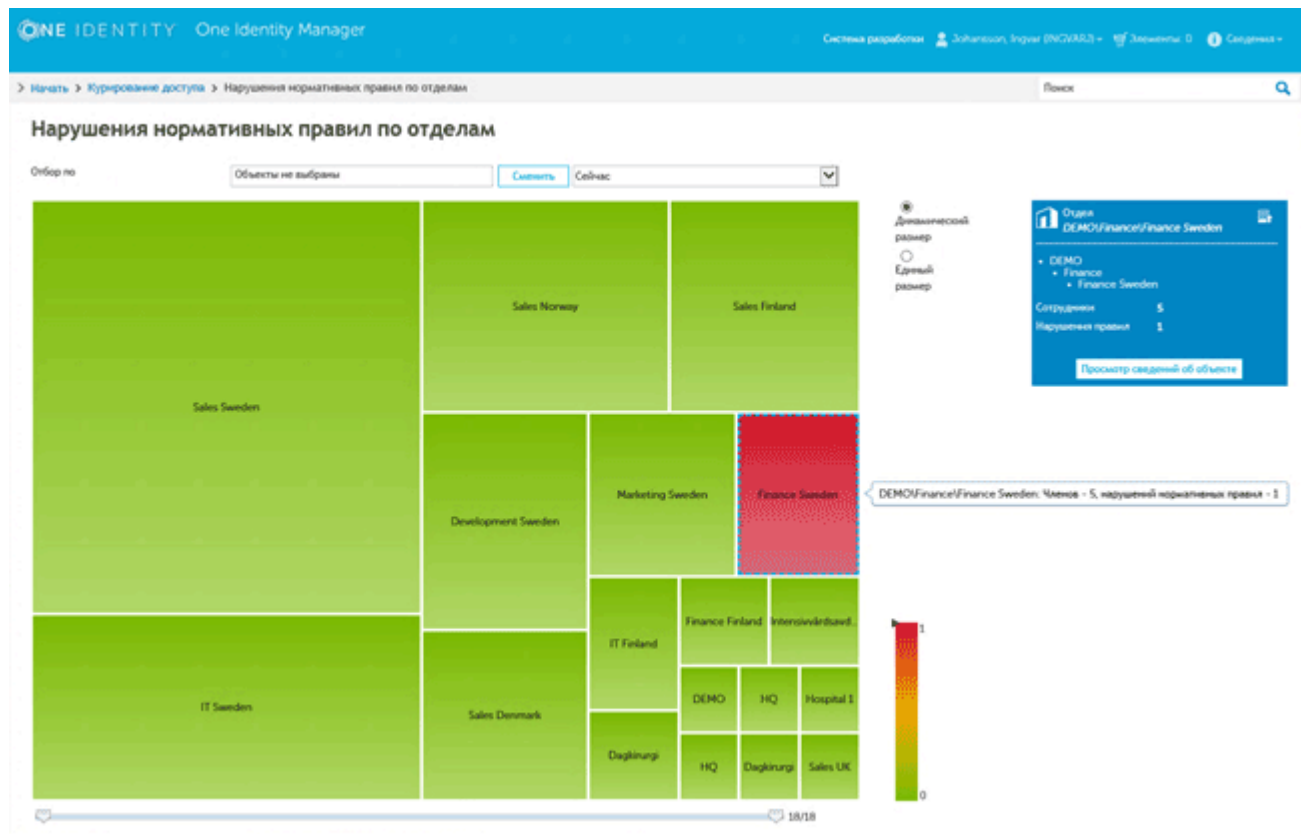
Конструктор ролей – Analyzer

The screenshot displays the Analyzer application interface, titled "Analyzer - viadmin@SQLD11M7 (Main Database)". The interface is divided into several sections:

- Cluster:** A tree view on the left shows a hierarchy of roles, with "Role 1.2.1.2" selected. A table to the right lists "Employees" and "Permissions" for the selected role.
- Memberships:** A table at the bottom left shows membership details for "Adams, Mattie (MATTIEA)", "Ziegler, Christopher (CHRISTOPHERZ)", "Abernathy, Francis (FRANCISA)", and "Adames, Helen Middle (HELENA)". It includes columns for "Similarity" and various categories like "SAP - Admin", "SAP - Manager", "Accounting", "China", "Germany", and "United States of Am...".
- Employees [1]:** A table on the right lists employees with their names and similarity scores, represented by green and red bars.
- Permissions [1 + 2]:** A list of permissions on the right, including "Accounting", "SAP - Admin", "SAP - Manager", "Account Operators", "Australia", "Backup Operators", "Cert Publishers", "China", and "Denmark".

The Windows taskbar at the bottom shows the system time as 15:48 on 22.12.2016, and the taskbar at the very bottom shows 2:40 on 23.12.2016.

Карта самых проблемных мест в нарушении политик



Настройки правил расчёта индекса риска

Тонкая настройка повышающих и понижающих коэффициентов индекса риска

Учётная запись без сотрудника

Имя: Учётная запись без сотрудника
Ссылка таблицы (цели): ADSAccount - RiskIndexCalculated
Описание: Отсутствие учетной записи, назначенной сотруднику, повышает индекс риска. (Предопределенная функция.)

Тип расчета: Итерировать
Вес/Сильное значение: 0,05 (range 0,05 to 1)

Дезактивировано: Дезактивировано

Сохранить Отмена

Тип расчета	Вес/Сильное значение	Права
Максимум (взвешенный)	1	?
Итерировать	0.05	?
Итерировать	0.05	?
Итерировать	0.2	?
Детерминат	0.05	?
Максимум (взвешенный)	1	?
Детерминат	0.05	?
Детерминат	0.05	?
Сложение	1	?
Максимум (взвешенный)	1	?
Детерминат	0.05	?

Рекомендации при выборе IDM/IGA

- Не доверять сравнительным таблицам
- Демо не достаточно
- Делать РОС 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™