



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

4 ОКТЯБРЯ 2018
КРАСНОЯРСК

#CODEIB



Внедрение IDM-решения в СУЭК Рекомендации при подготовке и внедрении

Яков Фишелев

Руководитель представительства One Identity в России и СНГ

Багаев Максим Сергеевич

Советник по информационной безопасности компании СУЭК



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



PAM, Behaviour Analytics

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
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?”

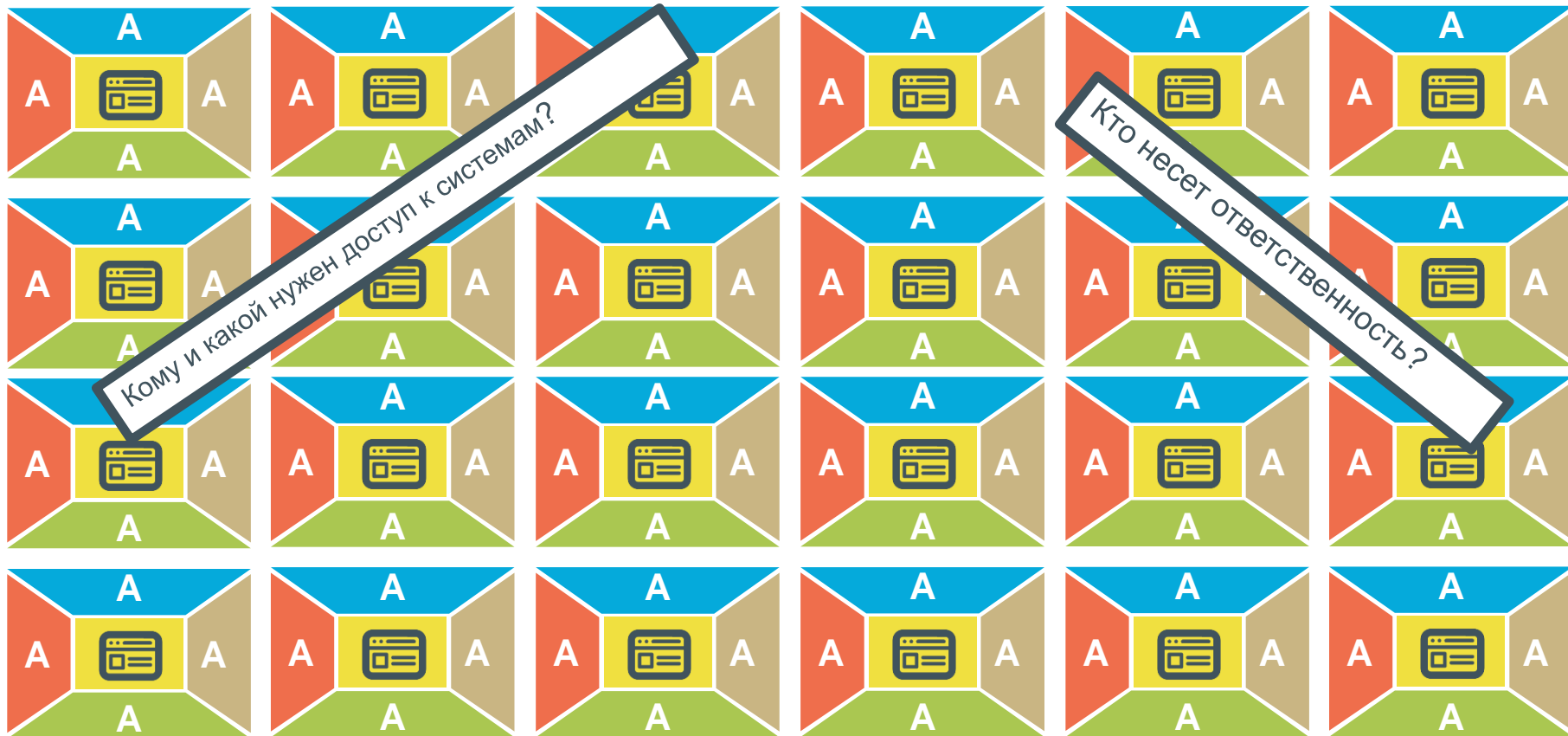
Это нужно делать для каждой ИС и ресурса...

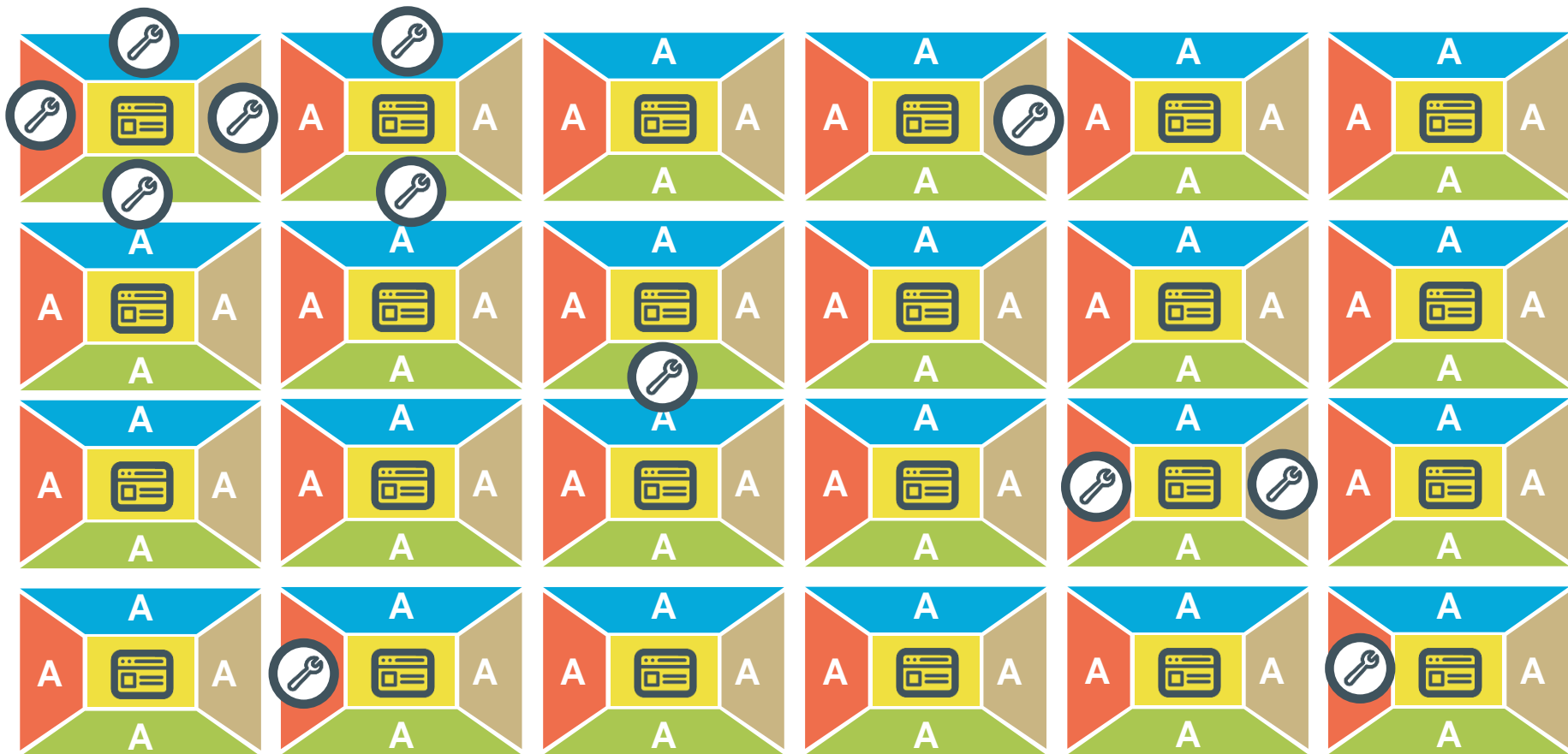
Кому
предоставить
права доступа к
системам?



Кто несет
ответственность?

В компаниях десятки систем....



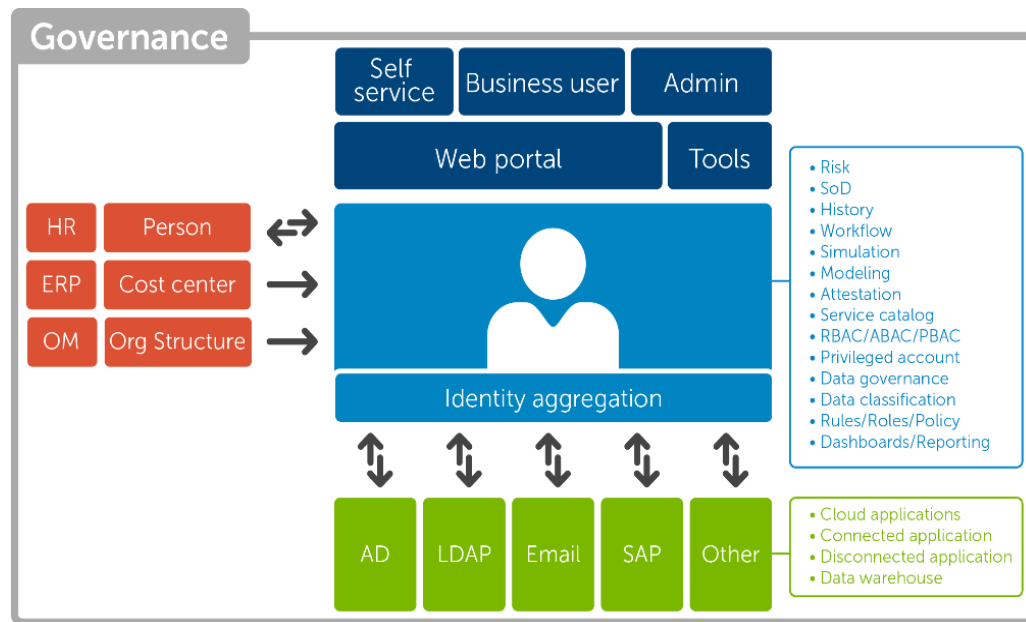


...Унификация IAM по всем системам...



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



Функционал 1ИМ на примерах наших клиентов

Заявка на доступ на портале IDM



Меню навигации

1 элемент

Сведения

Мои идентификационные

< Начать > Запрос

Поиск



Мои действия

13

Неподтвержденные запросы

13

Обращения в связи с утверждением

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

Получатели

Сменить

Найти элемент услуги

Название продукта или тега



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)



Управление паролями

Заявка на доступ на портале IDM



Мои идентификационные

Начать > Запрос

Поиск



Мои действия

13

- Неподтвержденные запросы
- Обращения в связи с утверждением
- 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
- Поддержка шаблонов

Запрос

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

Параметры представления	Поиск	Продукт	Категория услуги	Описание	Запрос
<input 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"/>

Продукт: Белый лист

Действия

Отправить запрос сейчас

Просмотр цепочки согласования заявки

One Identity Manager

Система разработки - Обновления в ожидании | Рягин Николай Анатольевич | Элементы: 2 | Сведения

Мои идентификационные < Начать > Архив утверждений

Поиск

Руководство пользователя

Мои действия **8**

- Неподтвержденные запросы
- Обращения в связи с утверждением
- Делегирование
- Незакрытые аттестации **8**

Мои обязанности

- Люди

Мой архив действий

- Архив запросов
- Архив утверждений
- Архив делегирования

Каталог услуг

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

Отчеты

Мой пароль

- Управление моими паролями
- Редактировать "Мой профиль вопрос-ответ"
- Редактировать "Мои оповещения"

Архив утверждений

На этой странице отображен архив принятых вами решений по утверждению. Более детальный поиск доступен с помощью кнопки «Расширенный поиск».

Расширенный поиск

Параметры представления | Дополнительные столбцы | Экспортировать представление | Поиск

Продукт	Статус	Дата запроса	Получатель	Нет.
Почтовые сервисы	Отклонено	час.назад		148
USB (Корпоративный)	Назначено	5 дней назад		140
Общение с внешними участниками	Прервано	19 дней назад	Игоревич	122
Общение с внешними участниками	Прервано	20 дней назад	Л	115
Общение с внешними участниками	Прервано	20 дней назад	Лот	113
Общение с внешними участниками	Прервано	20 дней назад	Юрьевич	112
Общение с внешними участниками	Прервано	20 дней назад	Евса	111
Общение с внешними участниками	Нет подписки	20 дней назад	Игоревич	110
Общение с внешними участниками	Назначено	20 дней назад	Игоревич	108
Общение с внешними участниками	Назначено	20 дней назад	Иванлович	109
Тестовая папка - Новый общий ресурс файловой системы	Отклонено	25 дней назад	Пользователь Тестовый	86
Совместная работа	Назначено	25 дней назад		78
USB (Корпоративный)	Прервано	26 дней назад	Александрович	55

Продукт: **USB (Корпоративный)** Статус: **Назначено**

Информация | **Процедура** | Нормоконтроль

Запрос - 5 дней назад

По	М	Ирина В
Дата создания	19.07.2017 12:00:29	

Предоставить - Подтверждение руководителя - час.назад

Обоснование принятого решения: Не указана причина

По	Климук Л	
Процедура утверждения	СМ - Менеджер получателя	
Дата создания	24.07.2017 12:04:36	

Предоставить - Подтверждение офицера информационной безопасности - 14 минут назад

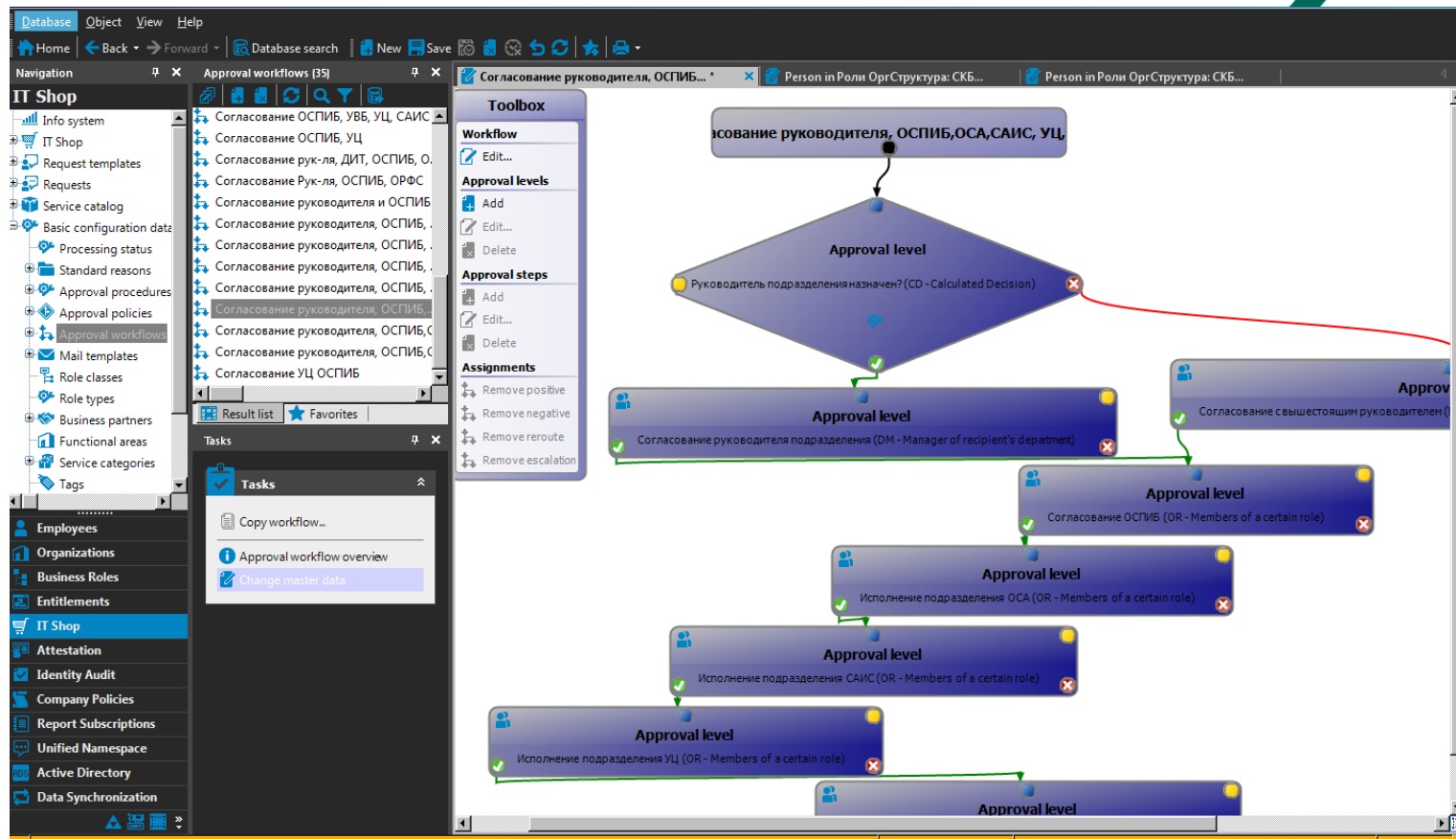
Обоснование принятого решения: Не указана причина

По	Рягин Николай Анатольевич	
Процедура утверждения	OR - Члены конкретной роли	
Дата создания	24.07.2017 13:14:11	

16

Пример настройки цепочки согласования

Интерфейс manager для инженерных настроек



Пример обзора сотрудника на 360

Info system | **Рягин Николай Анатольевич**

Access to shops (3)
Requests for all
Requests for DGE
Requests for DIBT

One Identity Manager application roles (9)
Base roles\Bright Assignments
Base roles\Employee Managers
Base roles\Everyone (Change)
Base roles\Everyone (Lookup)
Custom Managers
Data Governance Admins
Identity Management\Employee
Identity Management\Employee Admins

Technique roles (AP)
Additinally assigned to business role

Basic roles (BAZOVNIE)
Additinally assigned to business role
Доступ к сетевому ресурсу
Доступ к сетевому ресурсу
Классификация
Ученая запись Active Directory
Ученая запись Skype

Employee: Рягин Николай Анатольевич
Form of address: Mr.
Full name: Рягин Николай Анатольевич
Phone: 26
Mobile phone: +7999
Fax:
Building:
Floor:
Room:
Central user account: nryagin
Default email address: nryagin@deltacredit.ru
Primary location: Москва
Primary department: Отдел информационной безопасности ИТ
Primary cost center:
Primary business role:
Manager: C B C
VIP: -
Disabled permanently: -
External: -
Identity: Primary Identity

One Identity Manager accountability (2)
IT Shop Approver
Responsible Department: Делта Кредит Тестовые подразделения

Account definitions (3)
AD\Account
BIC\Hmailbox
SKYP\Account

Active Directory user account: nr
Domain: deltaxcredit
Login name (pre-Win2000): nr
Home directory:
Email address: nr_n@deltacredit.ru
Manage level:
User account is disabled: -

Active Directory user account: Ryagin Nikolay
Domain: deltaxcredit
Login name (pre-Win2000): nr
Home directory:
Email address: n_n@deltacredit.ru
Manage level: Full managed
User account is disabled: -

Mailbox: nryagin
Alias: nr
Simple display:
Active Directory account: Ryagin Nikolay
Exchange organization: Deltacredit
Do not display in address list: -
Account definition: BIC\Hmailbox
Manage level: Full managed

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 List (Top Left):** A list of departments under the selected block, including: "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 просрочен", "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 (7) Panel (Top Middle):** A list of departments for the selected block, 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):** A list of tasks for the selected department, including: "Create dynamic role", "Department overview", "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):** A detailed view of the "Блок 'Обеспечение безопасности'" department. It shows: Parent department: Головной филиал; Location; Cost center; Manager; Deputy manager; Role approver; Role approver (IT); and Block inheritance: -. Below this is a section for "Primary assigned employees (1)".

Оповещения в почту

IT | ИНФОРМАЦИОННАЯ
SECURITY | БЕЗОПАСНОСТЬ

Для внутреннего пользования (C1 - Internal)

Уважаемый руководитель, Рягин Николай Анатольевич!

Новая учетная запись была создана для вашего подчиненного. Пароль к учетной записи будет выслан отдельным письмом. Распечатайте данную информацию и передайте вашему подчиненному.

Работник	Волков Н В
Управляемые системы	Рабочий компьютер Электронная почта Skype For Business
Учетная запись	DELTA CREDIT\involkov_ext

Внедрение 1ИМ в компании СУЭК

Багаев Максим Сергеевич

Советник по информационной безопасности компании СУЭК

One Identity

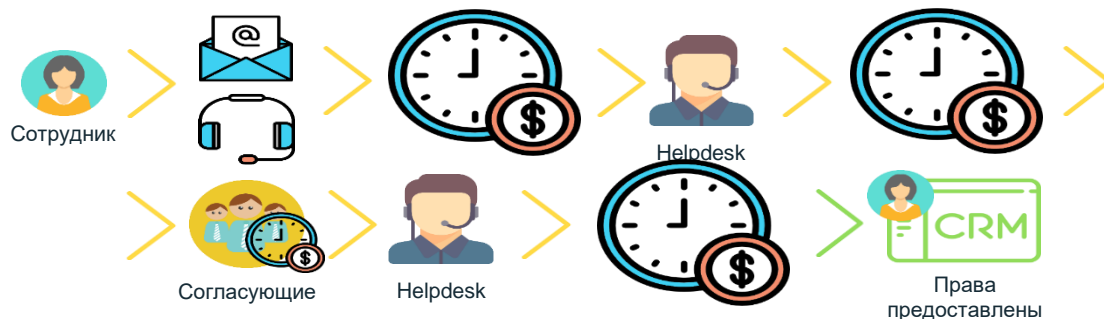
Задачи проекта IDM



1. Необходимость управлять доступом в SAP

- получать данные о текущих полномочиях
- управлять жизненным циклом доступа в SAP-системах
- Контролировать SOD-конфликты (разделение полномочий)

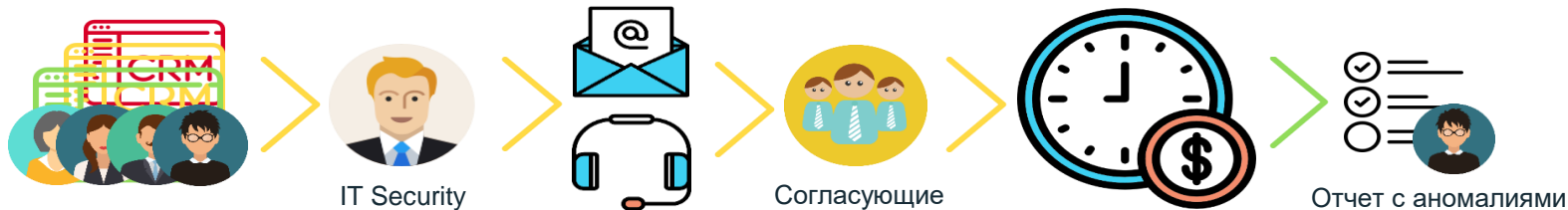
2. Сократить процесс согласования доступа с дней до минут. Согласования и ручная работа



Задачи проекта IDM



3. Сократить затраты ИТ-специалистов на предоставление прав доступа вручную
4. Несвоевременные блокировки
 - 7 незаблокированных УЗ в месяц в SAP-системах
 - 30 незаблокированных УЗ в месяц в AD
5. Сократить время восстановления забытого пароля к системам. Через Service Desk иногда занимает 2 дня
6. Возможность быстрого аудита. Подготовки отчетов для выполнения стандартов



Почему One Identity Manager



- Сертифицированный коннектор для SAP
- Позволяет реализовать полноценный SOD до уровня транзакций SAP

- Комплексное решение Enterprise уровня,
- Лидер Gartner и других аналитиков

- Управление сетевыми шарами

SAP GRC vs One Identity

- ✓ Дорого
- ✓ Только SAP
- ✓ Только через подрядчика

- Можно внедрить самостоятельно
- Визарды и иные инструменты помощи для внедрения

Наличие большого количества референсов в России и мире

- Зрелое решение
- Много коннекторов «из коробки» к ключевым системам

- Полноценно решается задача нескольких должностей для одной персоны



Рекомендации при выборе IDM/IGA



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

 ONE IDENTITY™