КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | Красноярск

29.02.2024

Владимир Ковалев

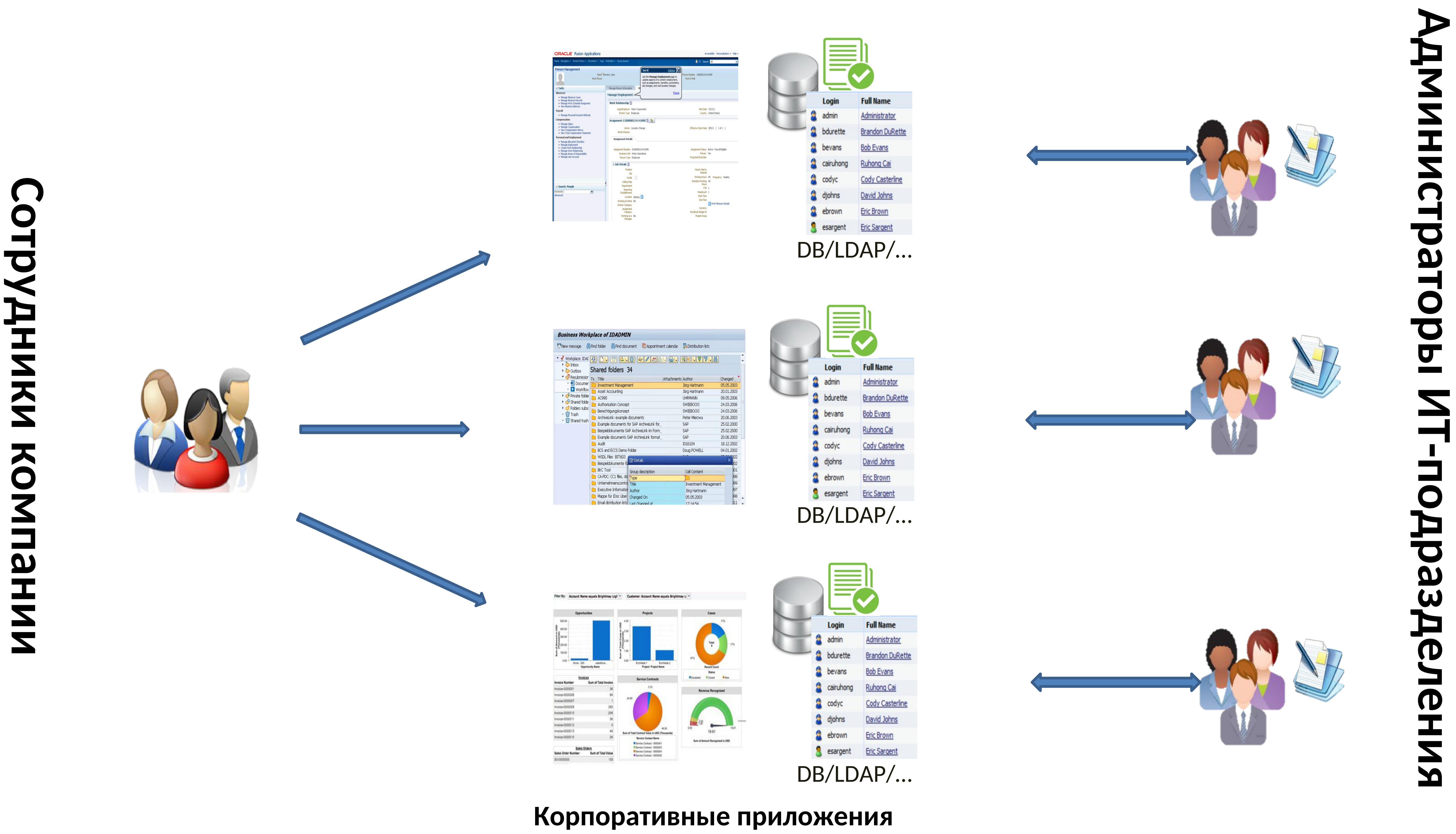
- От админа, до Java разработчика
- От 1С программиста, до начальника отдела ИТ и руководителя проектов внедрения западных ERP систем
- От замдиректора завода по ИТ и… обратно к администву и руководству проектами

Identity and Access management – фундамент ИБ в организации

Зачем?

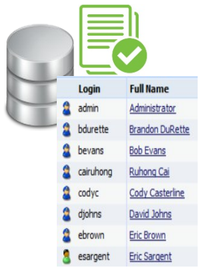
- Проблема «мертвых душ»
- Стандартизация и контроль выполняемых администраторами ИС операций
- Длительные сроки выдачи и отзыва ролей и прав в ИС
- Высокая сложность аудита прав пользователей

Классическая схема управления

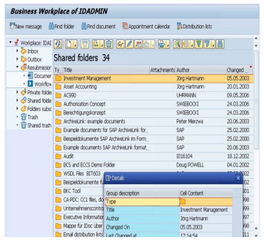


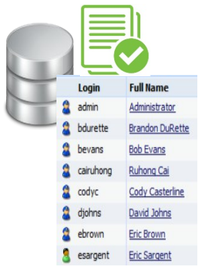
После внедрения IdM системы

Сотрудники компании

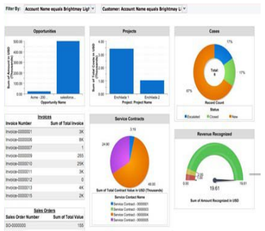


DB/LDAP/...





DB/LDAP/...



DB/LDAP/...

Корпоративные приложения

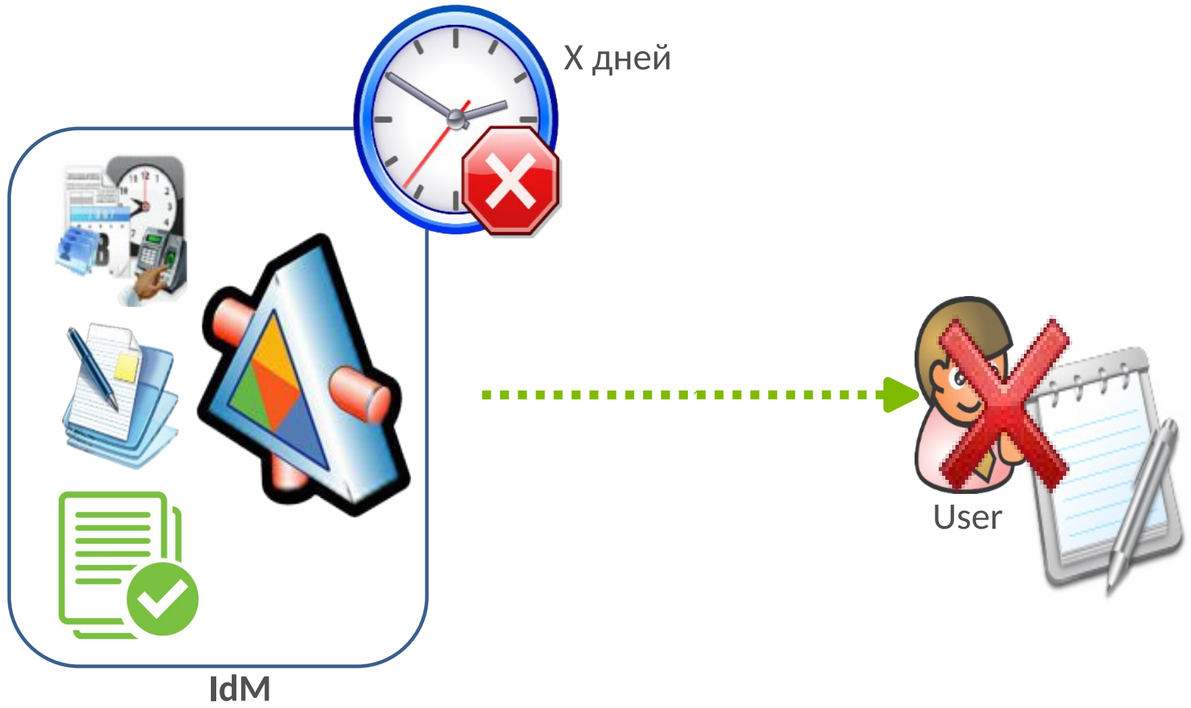
HR-системы

IdM

Администраторы ИТ-подразделения

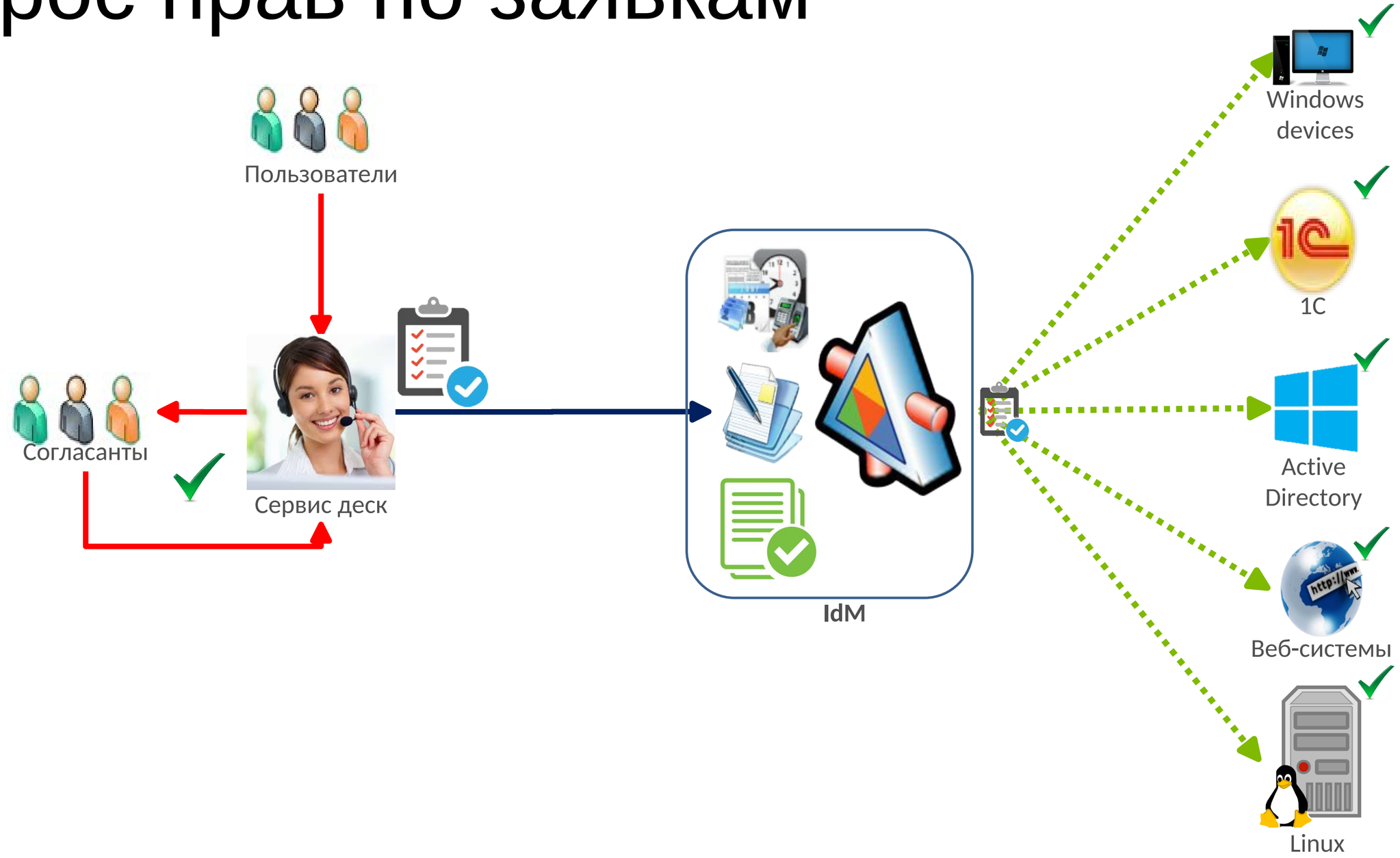
Контроль учеток уволенных сотрудников

Контроль неактивных учетных записей

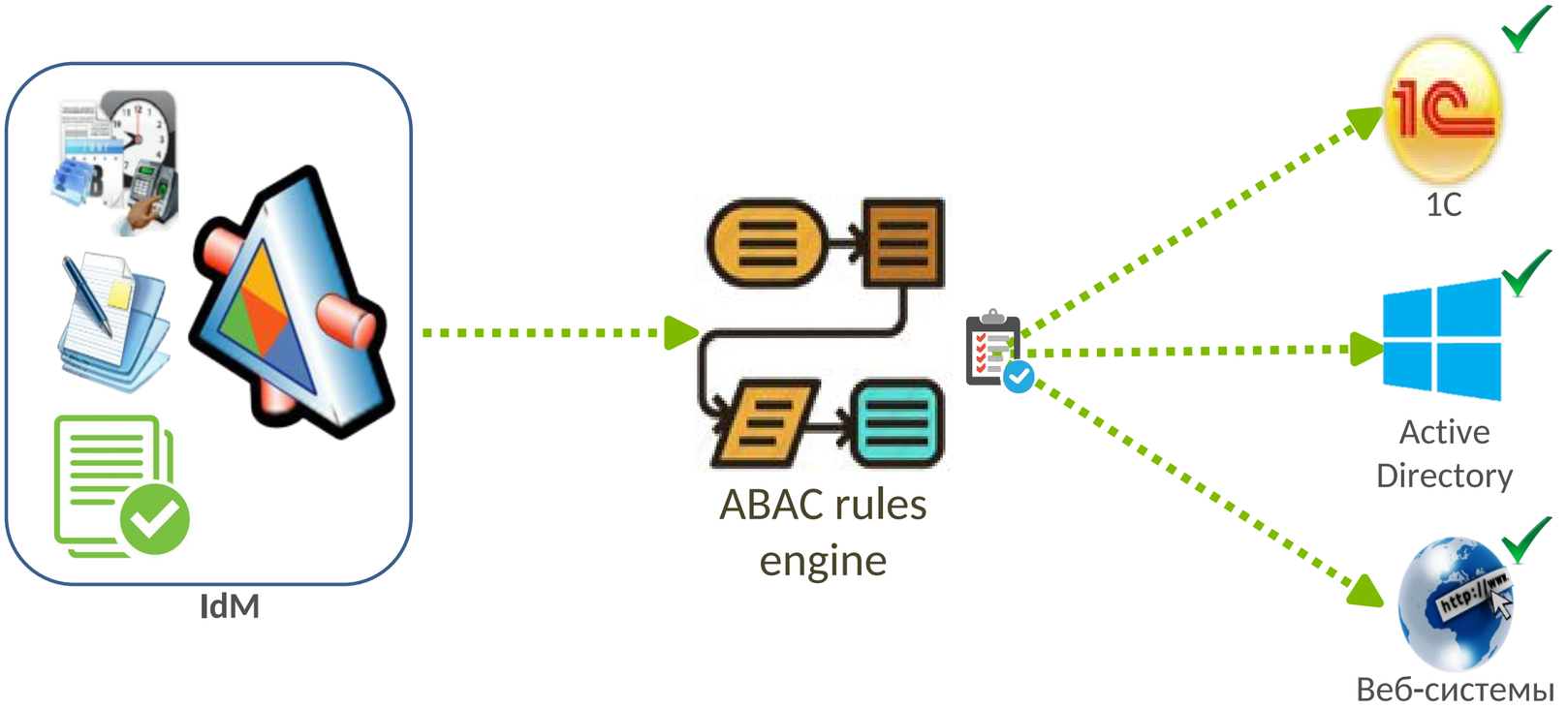


Пересмотр прав доступа

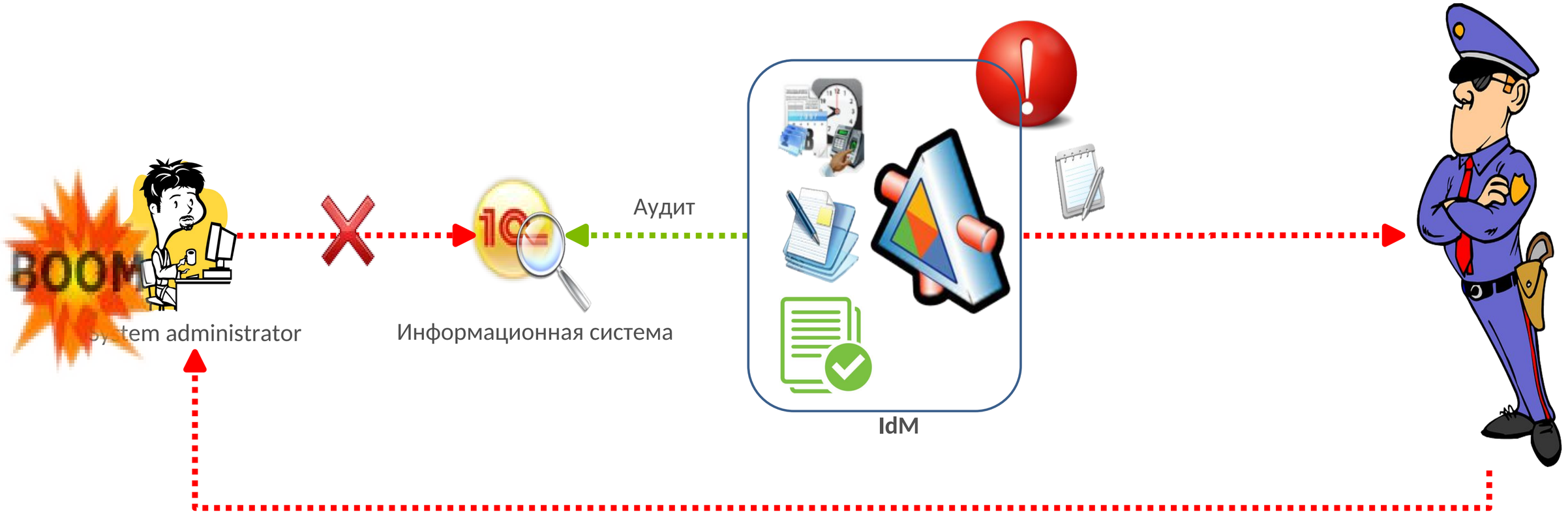
Запрос прав по заявкам



Атрибутивное управление правами



Аудит неавторизованных изменений

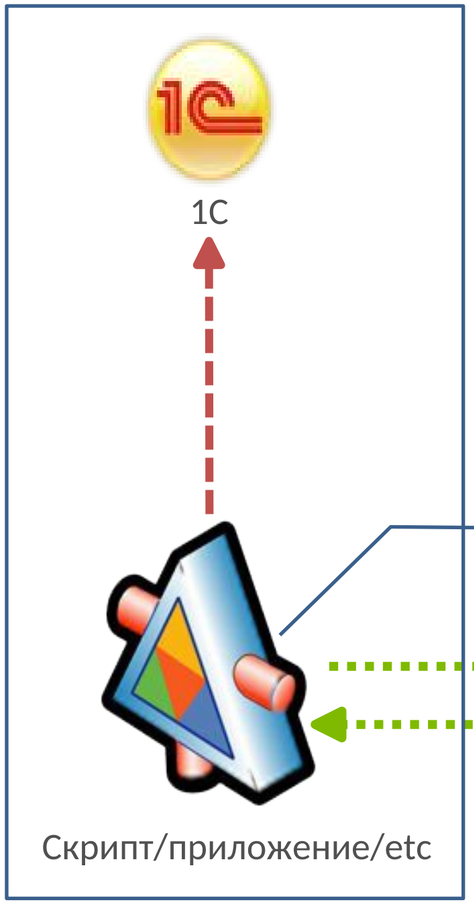


System administrator

Информационная система

Управление жизненным циклом специальных УЗ

App2App password management




```
…
$user = "учетная запись"
$pass = "aGjSAv23jh%agj!^%@"
# использование учетки
…
```

App2App password management

Пример скрипта на PowerShell

Было

```
…
$user = ‘учетная запись'
$pass = 'kajsghdjhsagj!^%@^"
# использование учетки
…
```

Стало:

```
…
# получение учетных данных в память по токену
$apiURI = https://IdM.domain.local/API/App2App/getCredential
$cred = Invoke-RestMethod -Method POST -Uri $apiURI -Body "5cb38847-1bb4-4669-af99-bebbe75f832b" # использование учетки
…
```

IdM-система: комплексные выгоды

- Снижение затрат на ИТ
- Уменьшение времени простоев
- Оптимизация бизнес-процессов
- Сквозной контроль использования доступов
- Предотвращение повышения привилегий
- Снижение количества ошибок
- Автоматизация рутинных операций
- Выполнение требований регуляторов
- И т.д. и т.п.

Наш опыт

Ноябрь 2014 – старт проекта

- Microsoft Forefront Identity manager (ныне это Microsoft Identity Manager)
- Свой портал управления, свое API поверх FIM
- Консолидируем данные из 14 кадровых источников
- Подключаем одну ИС – MS Active Directory и 4 завода к марту 2015

И тут мы поняли, насколько сильно ошиблись

Сентябрь 2015 – рестарт проекта

- Полностью свое ядро
- Полнотекстовый поиск объектов
- API для создания коннекторов к ИС
- API для интеграции с прочими системами

К декабрю 2016

- Консолидируем данные из 120+ кадровых источников в 17 городах
- Подключаем три ИС:
  - MS Active Directory – 2 шт (суммарно 22.5 тысячи учеток)
  - АСУ ЖДЦ – 1300+ учеток

2017… – подключение прочих систем

- Релиз интеграции с SAP, 1C, Citrix XenApp, VMWare airwatch
- Интеграция с СервисДеск
- Подключение прочих систем
- Атрибутивное управление правами
- SoD контроль
- Управление пользовательскими устройствами и серверами Windows (агент)
- Сбор security логов с DC и прочих приложений
- Конструктор отчетов
- Расширенные парольные политики AD
- …

Управление устройствами

Инструмент сотрудников техподдержки, администраторов и ИБ

- Управление жизненным циклом учетных записей типа **Computer** в AD
- Включение/выключение/рестарт устройства
- Удаленные операции ping/tracert/telnet
- Доступ к журналам Windows
- Доступ к локальным файлам
- Управление локальными сервисами (create/delete/start/stop/restart/change account and password)
- Управление локальными учетками и группами
- Инвентаризация железа и софта
- Сбор информации по фактам входа на устройства
- Журналирование всех операций с пользовательским устройством

Февраль 2024 – текущее состояние

- Кадровые данные из 286 источников, более 113 тысяч сотрудников и подрядчиков из 163 городов
- 5 доменов AD – 100+ тыс учеток
- 261 приложение 1С – 120+ тыс учеток
- 3 SAP/R3 – 21 тыс+ учеток
- 27 прочих приложений, 12 типов
- Более 800 пользователей, 50+ интеграций с другими системами

Время исполнения заявок сократилось с дней до секунд

PAM – расширение IdM системы

- Широкая география компании
- Большое число привилегированных пользователей и оборудования
- Необходимость контроля выполняемых работ со стороны ИТ, ИБ и бизнес-заказчиков

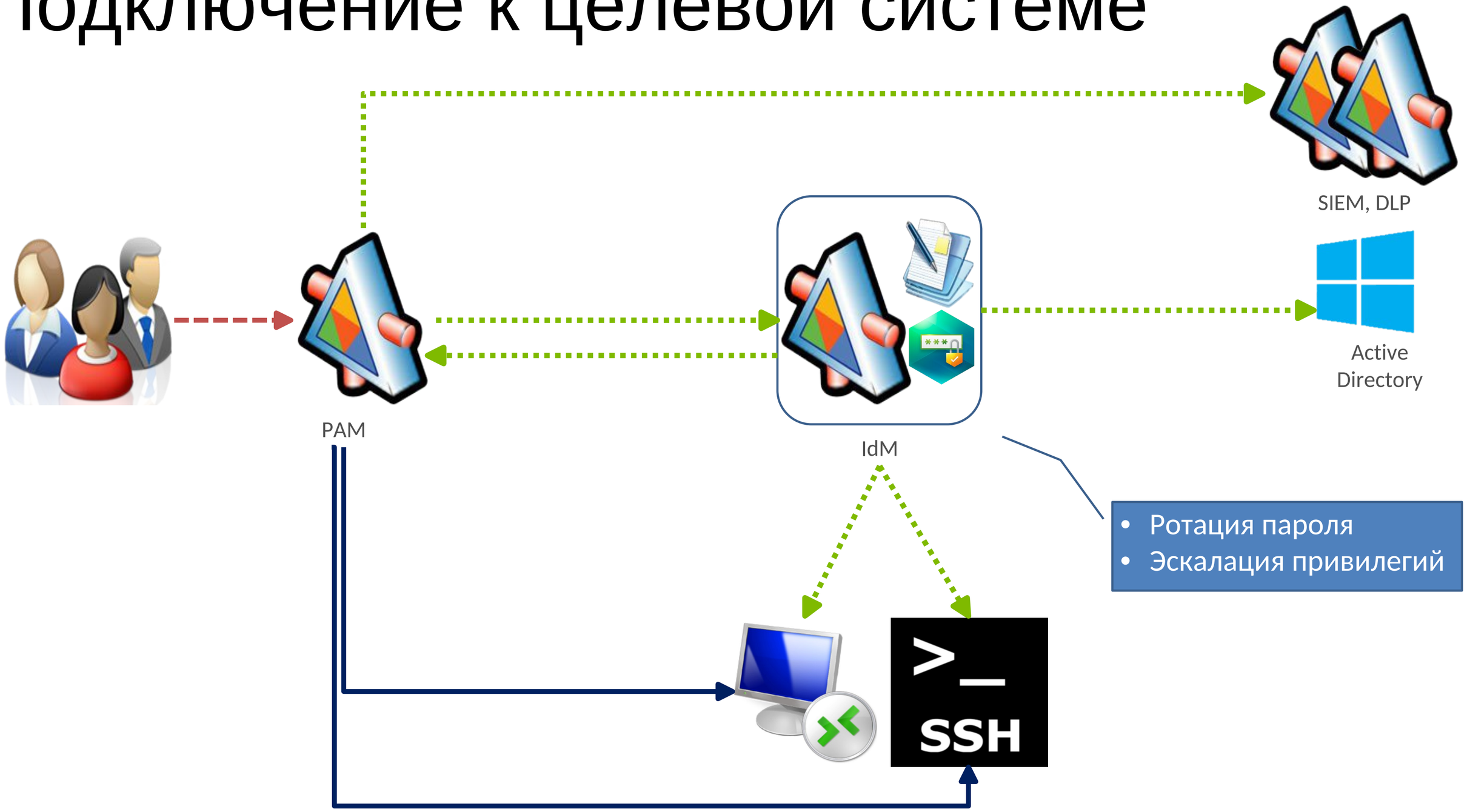
Классическая схема подключения
После внедрения PAM системы

- Видео запись сессии
- Перехват клавиатуры
- Перехват буфера обмена и передачи файлов (отправляем в DLP систему)

+ (с агентом):

- Информация о процессах и их контроль(start process, change active window, etc)
- Эскалация привилегий по требованию

Подключение к целевой системе



Февраль 2024 – текущее состояние

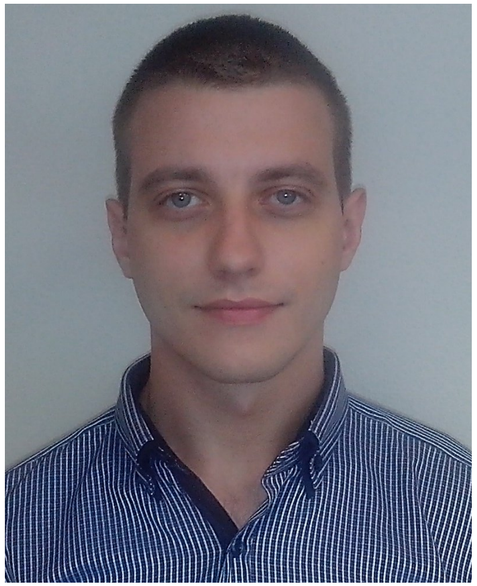
- 18 площадок
- Более 700 пользователей
- 44тыс+ часов сессий
- 310Гб хранилище

Что было самым сложным

- Консолидация кадровых данных
- Тестирование, тестирование и ЕЩЕ РАЗ ТЕСТИРОВАНИЕ
- Обучение пользователей
- Оптимизация производительности

Команда проекта





Готов ответить
на ваши вопросы