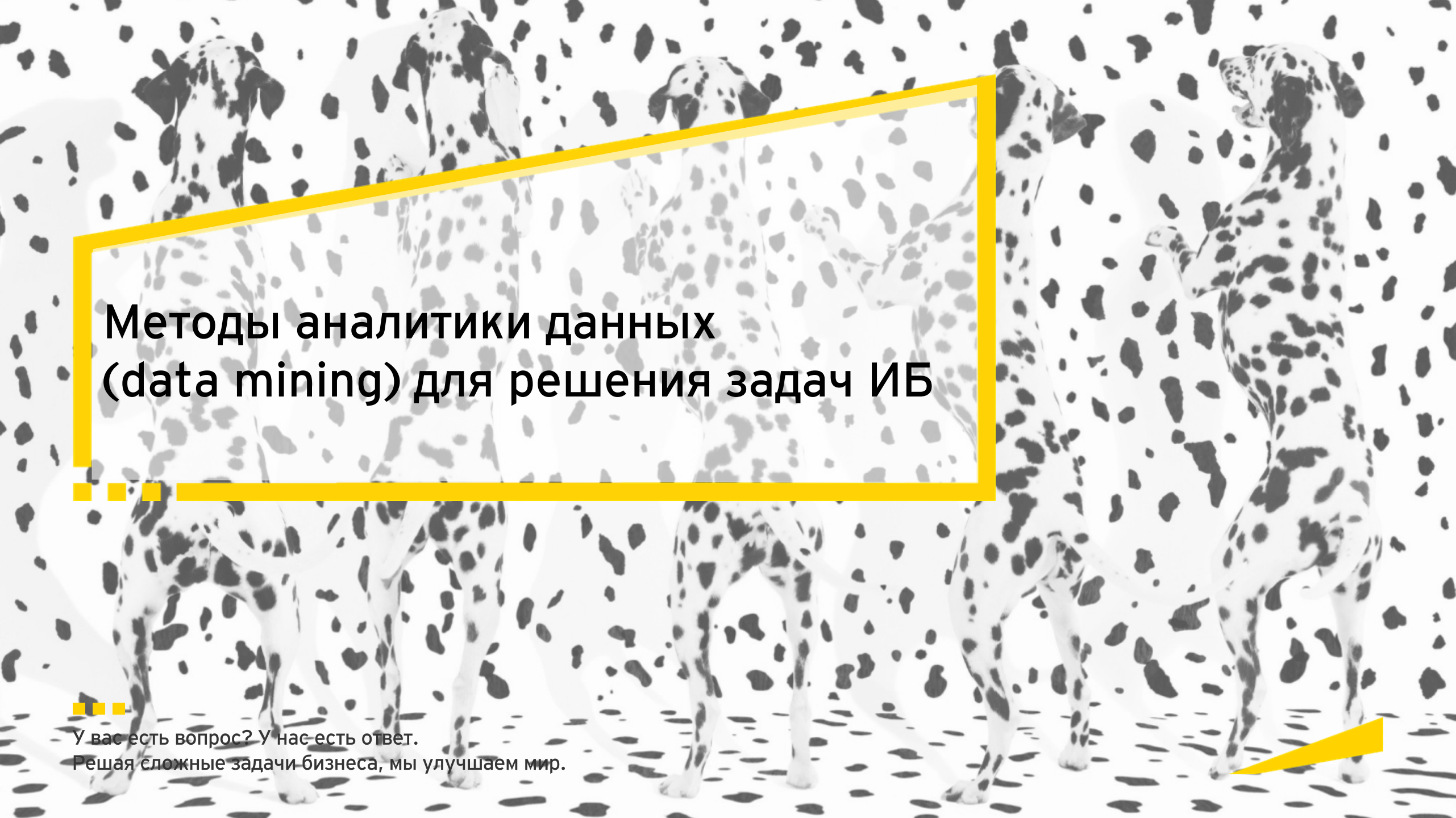
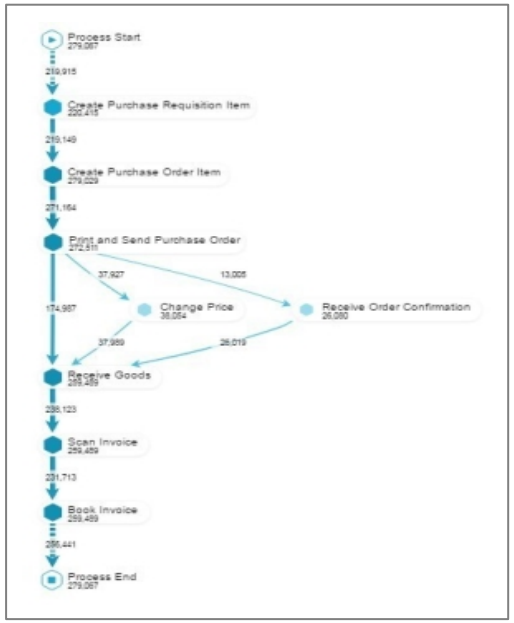


Методы аналитики данных (data mining) для решения задач ИБ

Для процессов, поддерживаемых ИТ-системами, с помощью технологий Process Mining возможен анализ процессов в реальном времени



Современная технология реконструкции и оценки сценариев поведения внутренних и внешних агентов.

Методы и инструменты Process Mining позволяют извлечь ценную информацию о процессах на основании данных ИТ-систем.

Преимущества Process Mining

- Обследование процесса основывается на объективных данных, а не мнениях интервьюируемых
- Достигается полная прозрачность выводов по анализу бизнес-процессов и обоснованность выводов фактами
- Сокращаются сроки, необходимые для проведения обследования
- Идентификация заранее неизвестных слабых мест процесса
- Инновационный инструмент, имеющий различные приложения в корпоративном секторе

Чего можно достичь с Process Mining?

- Единовременно или постоянно улучшать процессы
- Измерять эффективность контролей процессов
- Выявлять нарушения корпоративных политик
- Оптимизировать ресурсы
- Выявить возможности для автоматизации, в том числе с использованием RPA

Компании, уже использующие Process Mining

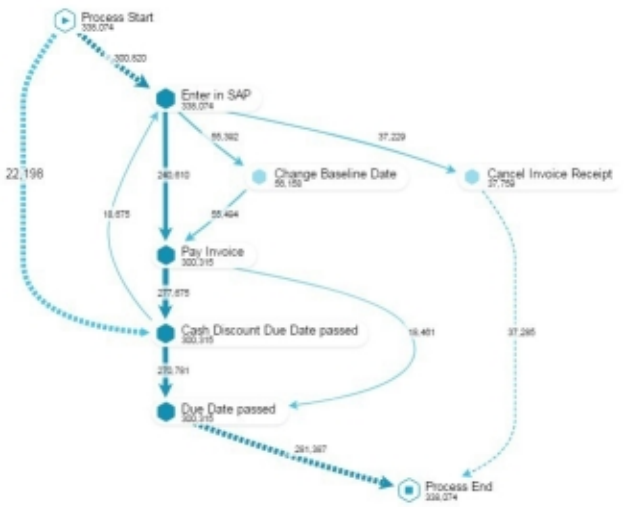
Источник: Celonis, 2016

Process Miningиспользует информацию о событиях, регистрируемых в ИБ-системах для реконструкции и анализа бизнес-процессов

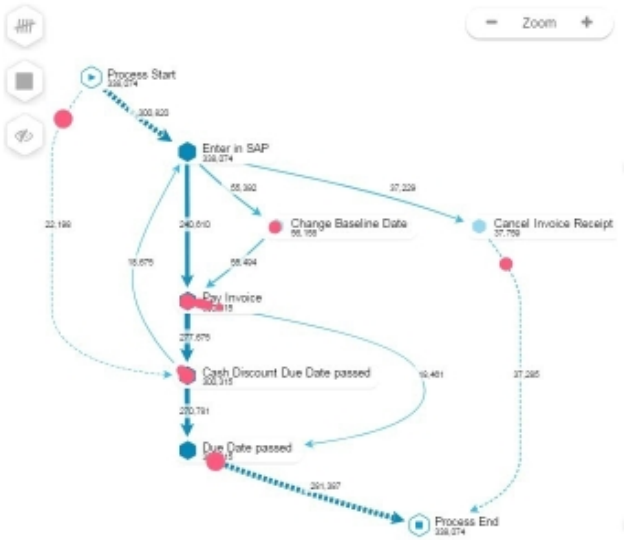
Источником информации являются журналы событий – таблицы, выгружаемые из ИТ-систем и включающие, как минимум: дату и время события; описание события; идентификатор экземпляра процесса

Ro...	T:concept:name	E:concept:name	E:time:timestamp	T:responsible
1	case-10011	Confirmation of receipt	Oct 11, 2011 3:45:40 PM MSK	Resource21
2	case-10011	T02 Check confirmation of receipt	Oct 12, 2011 10:26:25 AM MSK	Resource21
3	case-10011	T03 Adjust confirmation of receipt	Nov 24, 2011 6:36:51 PM MSK	Resource21
4	case-10011	T02 Check confirmation of receipt	Nov 24, 2011 6:37:16 PM MSK	Resource21
5	case-10017	Confirmation of receipt	Oct 18, 2011 3:46:39 PM MSK	Resource04
6	case-10017	T06 Determine necessity of stop advice	Oct 18, 2011 3:47:06 PM MSK	Resource04
7	case-10017	T02 Check confirmation of receipt	Oct 18, 2011 3:47:26 PM MSK	Resource04
8	case-10017	T03 Adjust confirmation of receipt	Oct 18, 2011 3:47:41 PM MSK	Resource04
9	case-10017	T02 Check confirmation of receipt	Oct 18, 2011 3:47:57 PM MSK	Resource04
10	case-10017	T10 Determine necessity to stop indication	Oct 18, 2011 3:48:15 PM MSK	Resource04
11	case-10017	T03 Adjust confirmation of receipt	Oct 18, 2011 3:48:30 PM MSK	Resource04
12	case-10017	T02 Check confirmation of receipt	Oct 18, 2011 3:51:01 PM MSK	Resource04
13	case-10017	T03 Adjust confirmation of receipt	Oct 18, 2011 3:56:57 PM MSK	Resource04
14	case-10024	Confirmation of receipt	Oct 18, 2011 5:53:19 PM MSK	Resource11
15	case-10024	T02 Check confirmation of receipt	Oct 18, 2011 5:53:38 PM MSK	Resource11
16	case-10024	T04 Determine confirmation of receipt	Oct 18, 2011 5:53:53 PM MSK	Resource11

С помощью алгоритмов Process Mining выполняется реконструкция реального процесса



На базе построенной модели выполняются различные виды анализа



Технологии process mining позволяют идентифицировать сценарии поведения с различной степенью детализации

Процесс из регламента: упрощённая модель

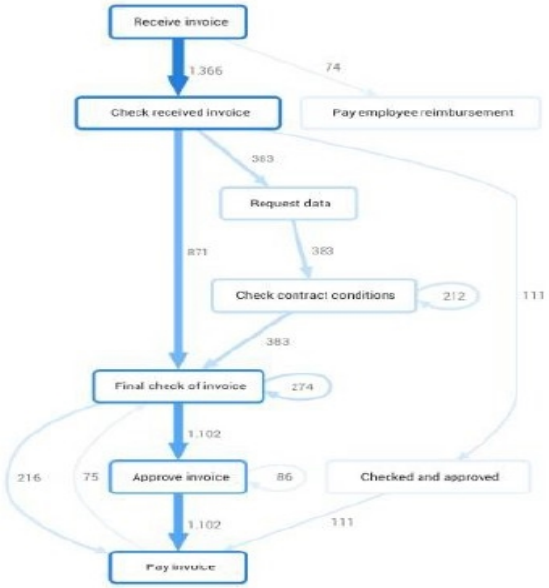
Покрытие вариантов: 20 %

Визуализация наиболее распространённого сценария исполнения процесса

Что знают люди, которые работают в процессе

Покрытие вариантов: 40 %

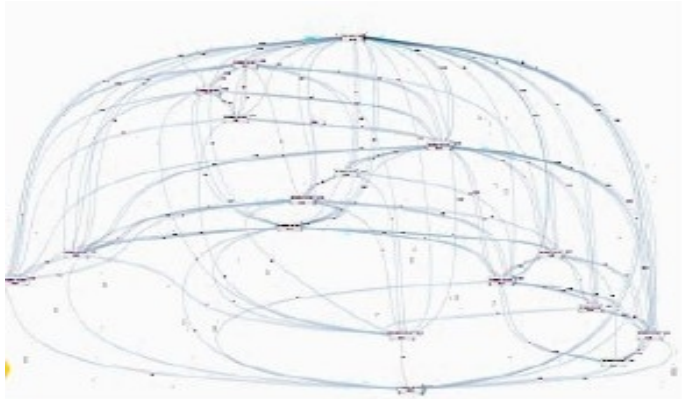
Отображены, в том числе, деятельности, которые исполняются реже. Идеально подходит для выявления аномалий и



Реальность: сложность, которая не может быть управляема без process mining

Покрытие вариантов: 100 %

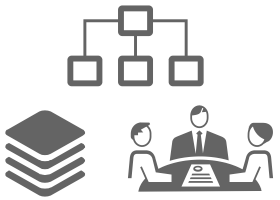
Полная картина, отображающая все варианты исполнения процесса. Подходит для выявления нетипичных вариантов или дефектов, которые в иных случаях оставались бы скрытыми



Process Miningдополняет классическийBPM*, работая в обратной последовательности

A. Проектирование процесса

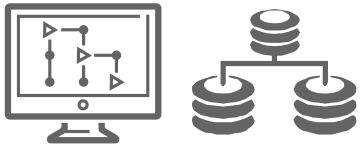
Разрабатывается высокоуровневая модель процесса



Конфигурирование

B. Реализация в ИТ-системе

Выполняется конфигурирование информационных систем автоматизации разработанного процесса



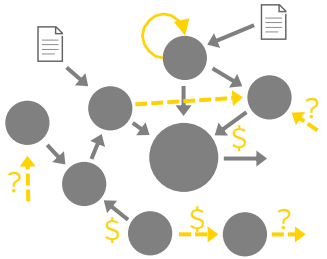
Исполнение

C. Люди и работа

ИБ-система координирует и поддерживает действия сотрудников при выполнении процесса

Классический BPM

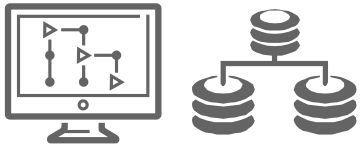
Process Mining



Реконструкция процесса

C. Process Mining

Реконструируется процесс «как есть», затем производится проверка соответствия и улучшение процесса



B. Информационные системы

Деятельность находит отражение в журналах ИТ-систем

Журналирование

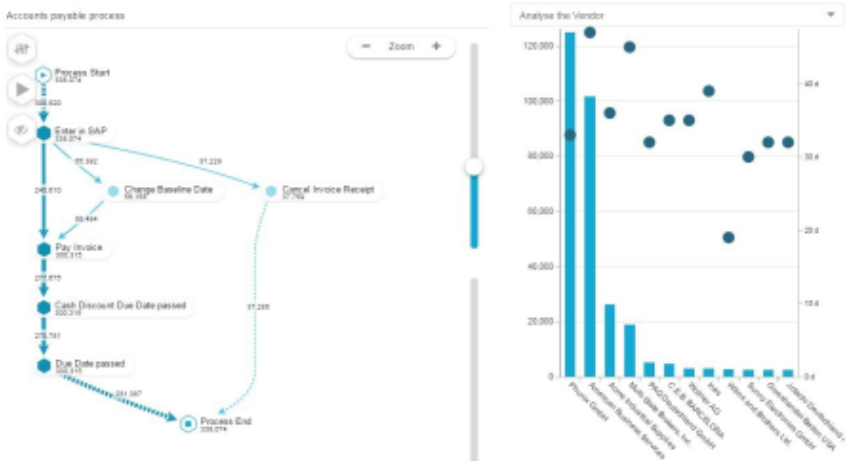
A. Люди и работа

В ходе работы сотрудники создают информацию о деятельности, которую они выполняют

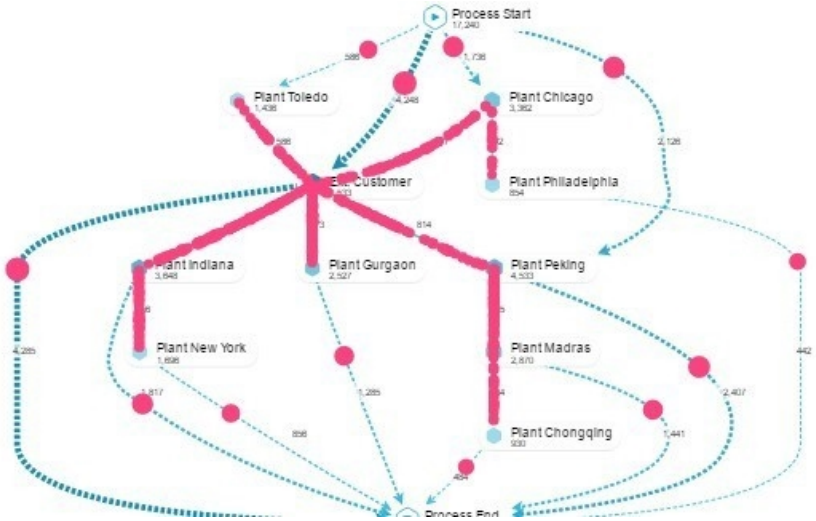
* BPM – Business Process Management, концепция процессного управления организацией

Варианты анализа процессов с использованием технологий Process Mining примеры вопросов, на которые можно ответить (1 из 3)

Реконструкция процесса и сравнительный анализ вариантов



Анализ динамики исполнения процесса (анимированное представление обработки объектов)



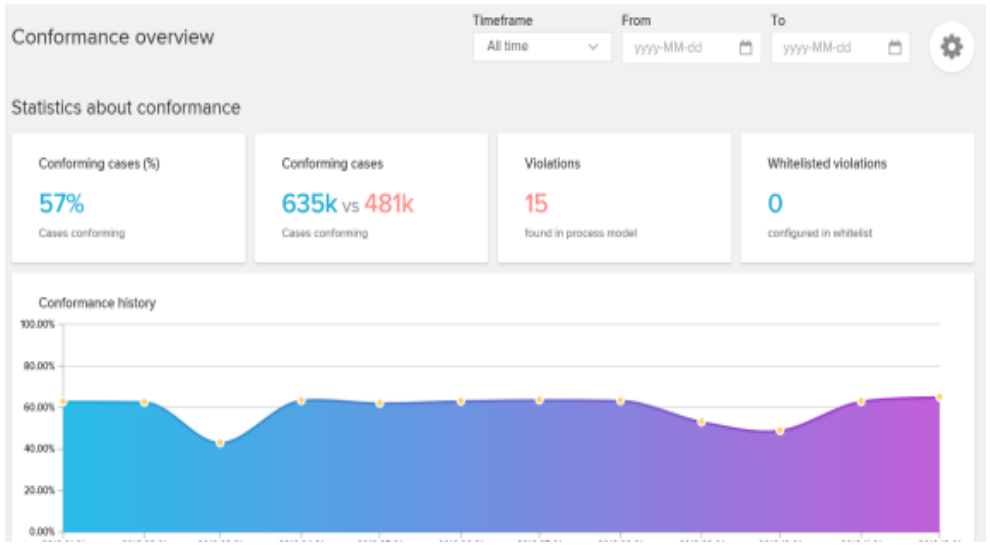
- Как выглядит процесс в реальности?
- В чём может быть причина задержек в исполнении процесса?
- Каковы часто исполняемые сценарии и исключения? В чём может быть причина исключений?
- На каких этапах процесса происходит накопление очереди задач, т.е. какие задачи являются «бутылочными горлышками»?
- Какие маршруты используются наиболее часто?

Варианты анализа процессов с использованием технологий Process Mining: примеры вопросов, на которые можно ответить (2 из 3)

Анализ трендов процесса во времени (например, продолжительность исполнения, динамика поступления объектов обработки)

- Как изменяются показатели процесса во времени?
- Есть ли цикличность процесса?
- Как влияет на производительность количество задач в работе?

Выявление степени соответствия исполнения процесса референтной модели



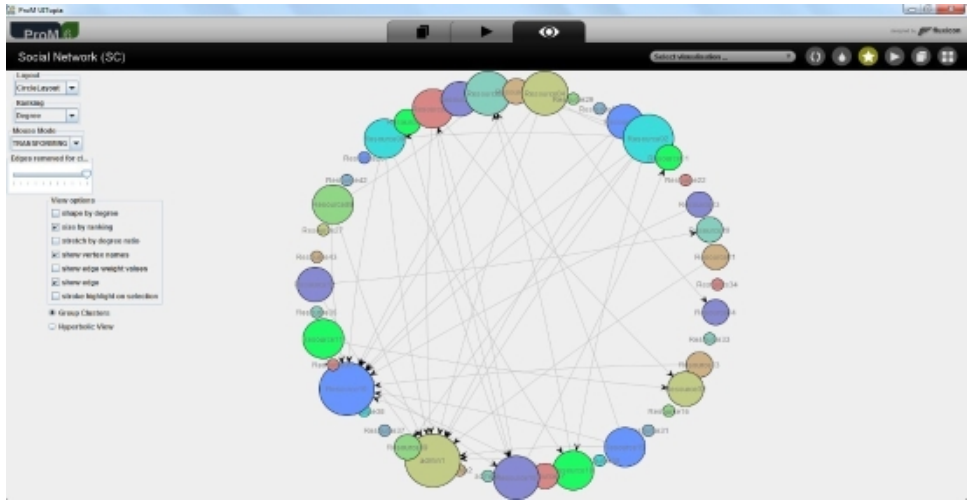
- Какие существуют типы отклонений фактического исполнения процесса от эталонной модели?

Варианты анализа процессов с использованием технологий Process Mining: примеры вопросов, на которые можно ответить (3 из 3)

Ресурсный анализ

- Какие задачи выполняются какими ресурсами?
- Существуют задачи, которые выполняются только одним или малым количеством ресурсов?
- Как происходит выполнение задач отдельными ресурсами во времени?

Анализ социальных связей процесса



- Соответствует ли исполнение задач сотрудников их должностным обязанностям?
- Какие сотрудники чаще всего передают работу другим, а какие - выполняют ряд задач самостоятельно?
- Как можно разделить сотрудников по группам?

Сценарии использования инструментария process mining в контексте информационной безопасности

1

Оптимизация процессов информационной безопасности

Постоянный мониторинг производительности процессов управления:

- Процесс управления инцидентами ИТ
- Процесс управления доступом

2

Мониторинг контролей процессов предприятия

- Соблюдение корпоративных политик
- Соблюдение принципа разграничения полномочий (SoD)

3

Проведение расследований инцидентов ИБ

Идентификация сценариев поведения пользователей и последовательности атаки

4

Исследования в целях соответствия законодательству по защите ПДн

Выявление фактов и сценариев реализации жизненного цикла ПДн

5

Углубленное исследование основных бизнес-процессов в рамках анализа воздействия на бизнес

Выявление основного сценария реализации процесса в целях разработки соответствующего плана восстановления

EY | Assurance | Tax | Transactions | Advisory

Краткая информация о компании EY

EY является международным лидером в области аудита, налогообложения, сопровождения сделок и консультирования.

Наши знания и качество услуг помогают укреплять доверие общественности к рынкам капитала и экономике в разных странах мира. Мы формируем выдающихся лидеров, под руководством которых наш коллектив всегда выполняет взятые на себя обязательства. Тем самым мы вносим значимый вклад в улучшение деловой среды на благо наших сотрудников, клиентов и общества в целом.

Название EY относится к глобальной организации и может относиться к одной или нескольким компаниям, входящим в состав Ernst & Young Global Limited, каждая из которых является отдельным юридическим лицом.

Ernst & Young Global Limited – юридическое лицо, созданное в соответствии с законодательством Великобритании, – является компанией, ограниченной гарантиями ее участников, и не оказывает услуг клиентам. Более подробная информация представлена на нашем сайте: ey.com.

Спасибо за внимание!

Александр Цимбалистов, PMP, ITIL Expert
Менеджер EY

Тел.: +7 (495) 755-9700

Моб.: +7 (903) 259-4067
E-mail:

Alexander.Tsimbalistov@ru.ey.com