

ITSEF

XIII ЦИФРОВОЙ ФОРУМ

Мониторинг бизнес-процессов с использованием Micro Focus Business Value Dashboard (BVD)

Евгений Горбачев

Ситуационный центр ДЗИ «Газпромбанк» (АО)

Наталья Попова

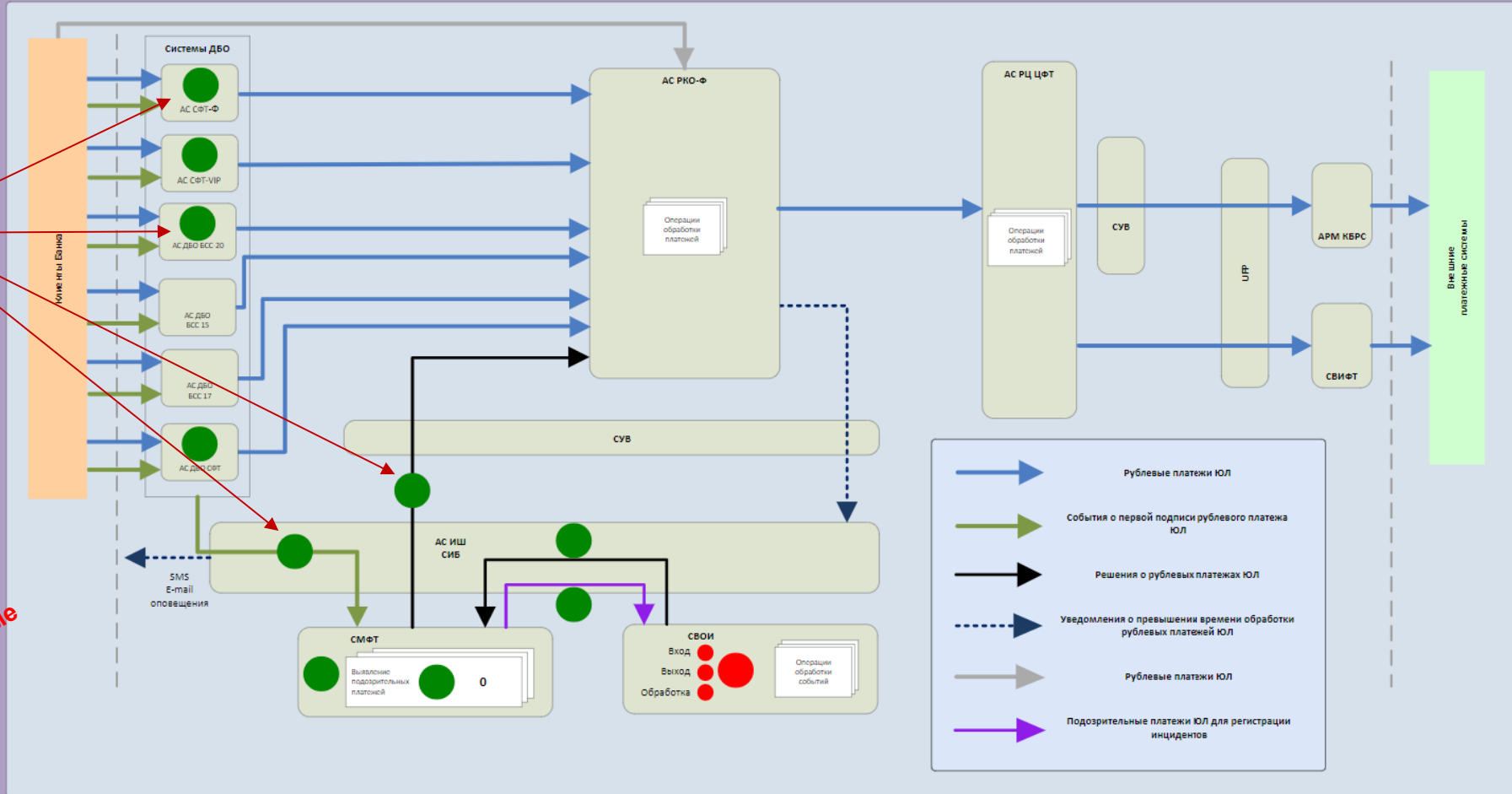
Группа систем управления ИТ-инфраструктурой ICL

Задачи системы

Система мониторинга банковского технологического процесса обработки рублевых платежей ЮЛ на основе Micro Focus Business Value Dashboard:

- Оперативный (текущее состояние) и аналитический (за интервал) мониторинг контролируемых ИС.
- Поддержка принятия решения для руководителей.
- Повышение прозрачности работы инфраструктуры.

Индикатор состояния обработки на отдельных системах/этапах



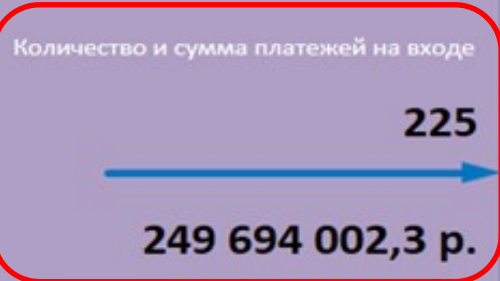
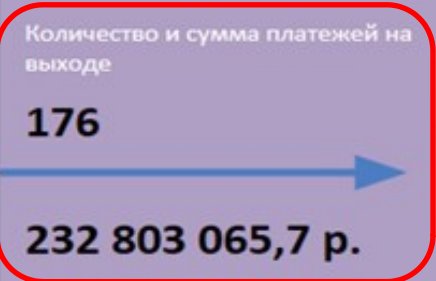
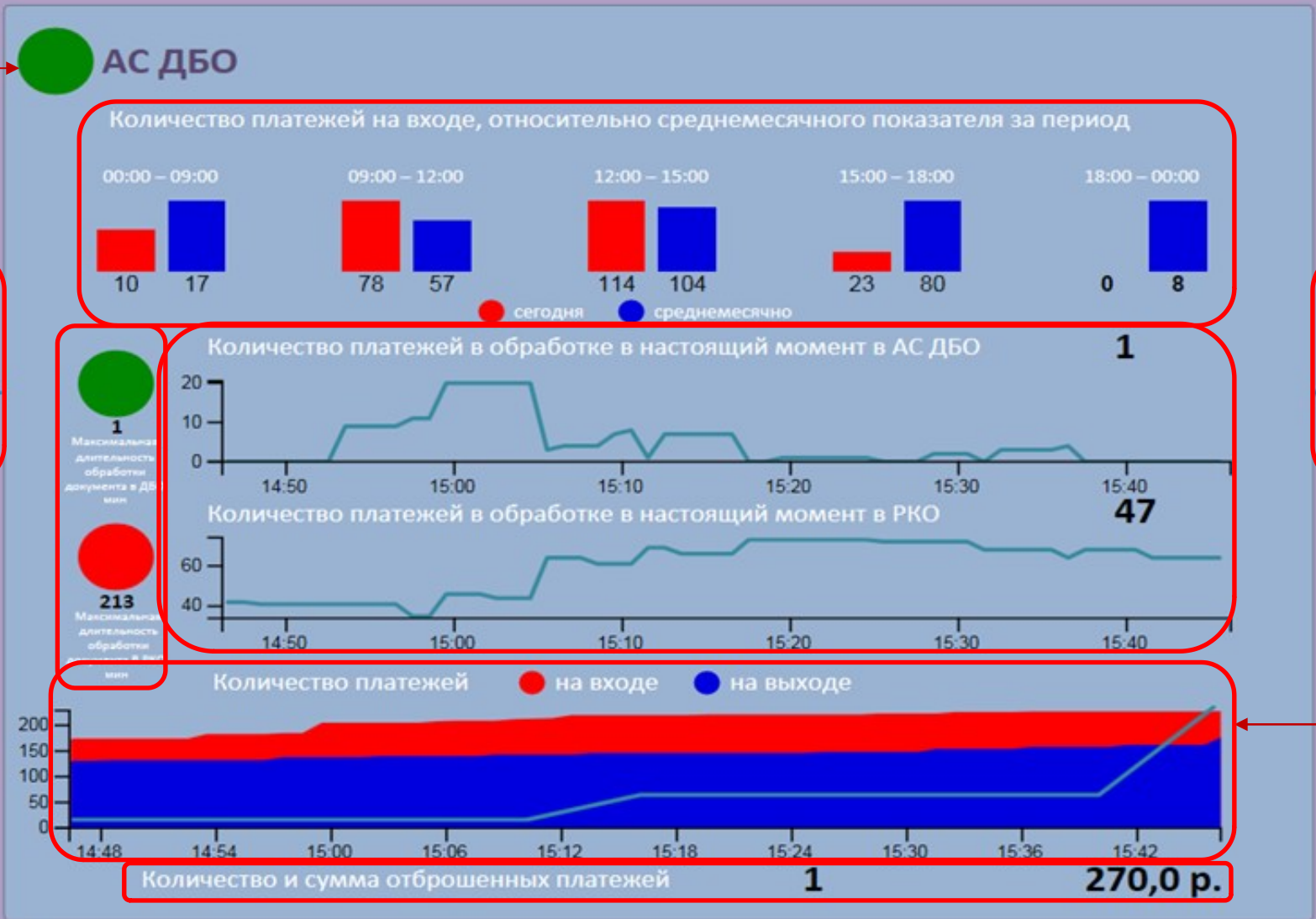
Это пример, а не реальные данные

(в течении опер. дня с 00:00 текущего дня до 00:00 следующего дня)

Мониторинг банковского технологического процесса обработки платежей ЮЛ



Индикатор отношения выхода ко входу:
 < 30 - зеленый
 >= 30 и < 40 - желтый
 >= 40 - красный



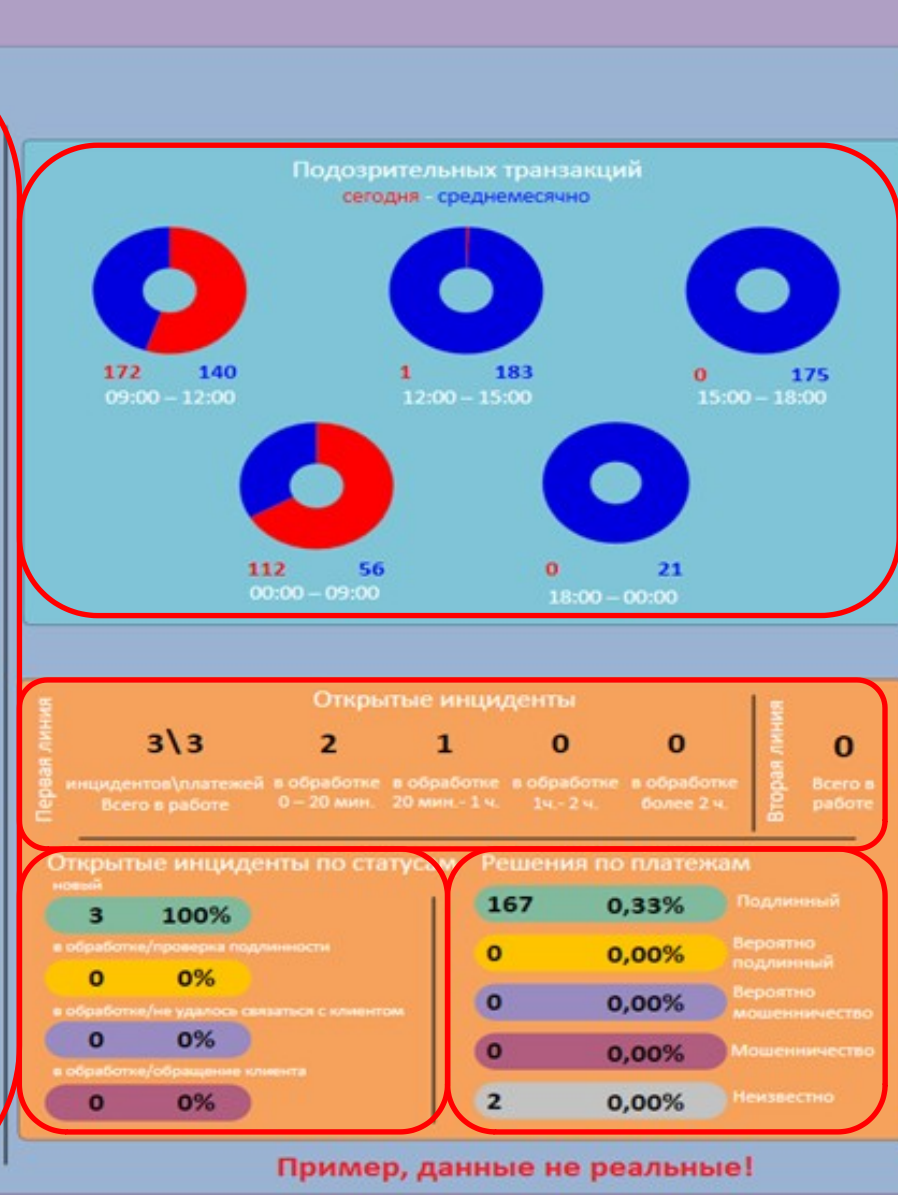
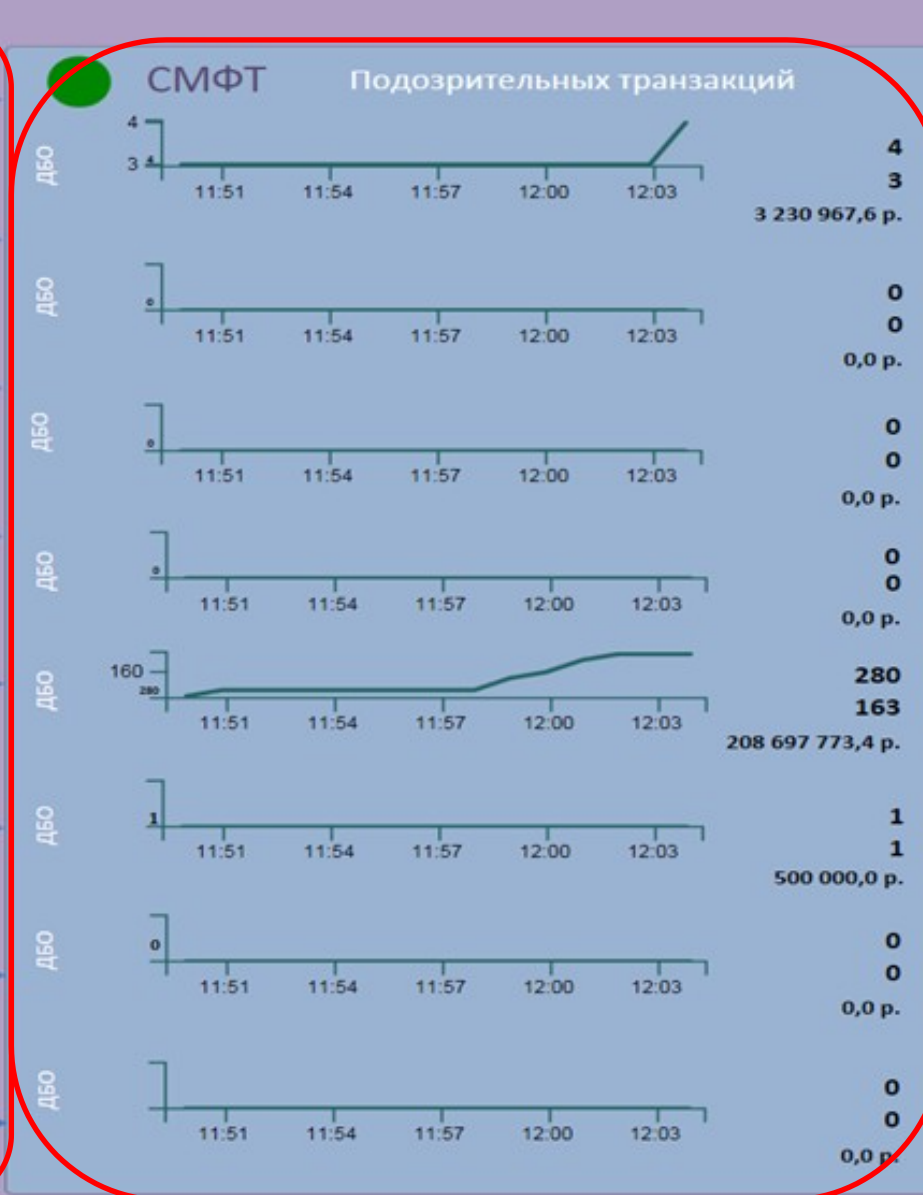
Это пример, а не реальные данные

График отношения количества платежей на выходе к количеству платежей на входе в процентах

Мониторинг системы Дистанционного Банковского Обслуживания (ДБО)



ДБО	
количество	2917
сумма	8 505 944 948,8 р.
клиентов	585
ДБО	
количество	33
сумма	83 698 135,8 р.
клиентов	13
ДБО	
количество	974
сумма	993 844 264,3 р.
клиентов	8
ДБО	
количество	141
сумма	9 297 897 891,7 р.
клиентов	3
ДБО	
количество	43274
сумма	46 634 005 630,9 р.
клиентов	4922
ДБО	
количество	2868
сумма	1 875 125 009,2 р.
клиентов	384
ДБО	
количество	0
сумма	0,0 р.
клиентов	0
ДБО	
количество	3
сумма	4 351,0 р.
клиентов	1



Передано подозрительных транзакций	
285	
Решений ДБО для РКО	2915
сумма	8 504 364 443,8 р.
клиентов	584
Решений ДБО для РКО	33
сумма	83 698 135,8 р.
клиентов	13
Решений ДБО для РКО	974
сумма	993 844 264,3 р.
клиентов	8
Решений ДБО для РКО	141
сумма	9 297 897 891 р.
клиентов	3
Решений ДБО для РКО	43160
сумма	46 576 277 505,4 р.
клиентов	4918
Решений ДБО для РКО	2868
сумма	1 875 125 009,2 р.
клиентов	384
Решений ДБО для РКО	0
сумма	0,0 р.
клиентов	0
Решений ДБО для РКО	3
сумма	4 351,0 р.
клиентов	1

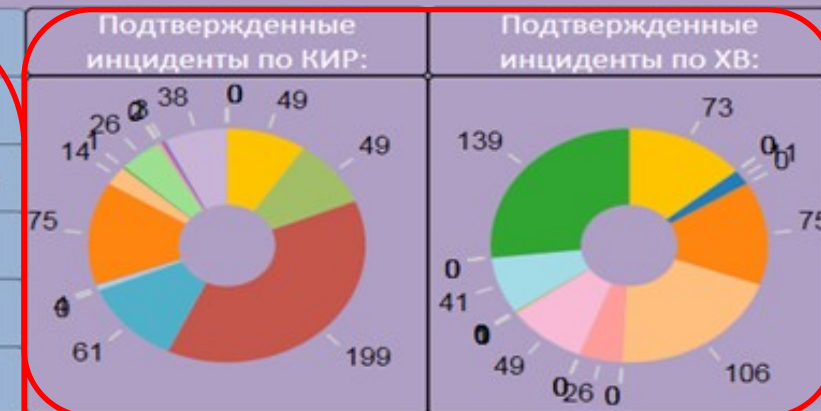
Пример, данные не реальные!

Мониторинг антифрод системы



Пример. Данные не реальные!

Уровни ТОС	Всего	Открыты	Закрты			
			Ложные	Подтверждены		
				Исключены	Дочерние	Уникальные
ТОС 7	1808	13	50	5	60	1680
ТОС 6	5274	26	169	21	98	4960
ТОС 5	0	0	0	0	0	0
ТОС 4	581	13	4	0	8	556
ТОС 3	513	0	47	2	31	433
ТОС 2	8	0	4	0	1	3
ТОС 1	541	2	21	0	25	493
Прочие	51	0	0	0	3	48
Итого	8776	54	295	28	226	8173

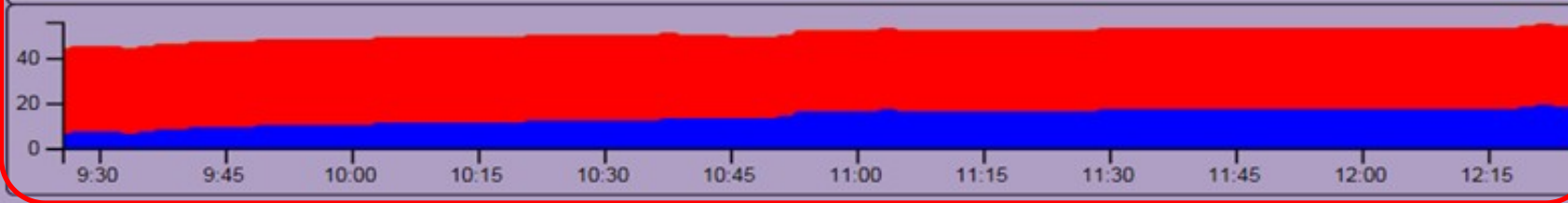


Самый «старый» незакрытый инцидент

IB73382	создан	10.03.2019 17:40:11
	изменен	12.03.2019 04:10:56



Открытые инциденты ИБ: **18** новых, **36** расследуются, **0** в ожидании, **0** решены.



Мониторинг обработки инцидентов ИБ



Зачем всё это нужно?

Владельцы бизнес процессов:

Как узнать - процесс сейчас «ок» или не очень?

Подразделение по защите информации:

Как определить и наглядно показать, что средства защиты не ухудшают состояние БТП?

Ответственные за ИТ-инфраструктуру:

Как определить и наглядно показать, какая АС выступает в качестве «тормоза»?

Реализация



Этап 1

- Формирование списка ключевых показателей бизнес-процесса
- Формирование графических панелей
- Определение списка АС-источников данных



Этап 2

- Настройка ПО для сбора данных
- Настройка функций для расчета ключевых показателей
- Настройка ПО для передачи данных на графические панели



Этап 3

- Отладка мониторинга, внесение правок и актуализация





Реализация: работа с процессом

Использование имеющихся описаний бизнес-процессов

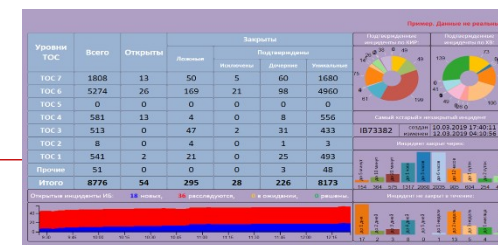
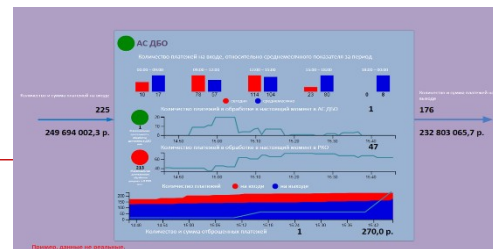
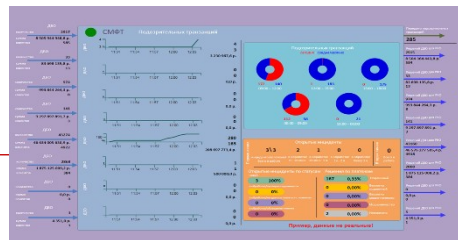
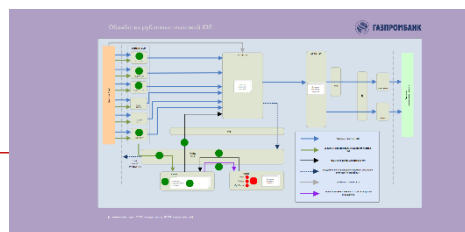
Описание бизнес-процесса с использованием методики:

- Определение активов («что обрабатывается бизнес-процессом»)
- Определение стадий обработки активов и условий перехода
- Определение АС в составе бизнес-процесса

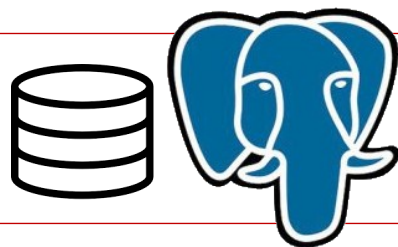
Подготовка списка метрик бизнес-процесса

- Количественные и качественные
 - По единицам измерения (количество, время, рубли и т.п.)
 - Оперативные и исторические
 - Типовой способ: «вход», «выход», «промежуточные стадии»
- 
- 

Реализация: настройка ПО



BVD - представление показателей на графических панелях



PostgreSQL

**Расчет и хранение
ключевых показателей**

ArcSight

ArcSight

ArcSight

ArcSight

ArcSight

ArcSight

**Сборщики
событий**

AC 1

AC 2

AC 3

AC N

**AC - источники
данных**



Реализация: сбор данных из АС

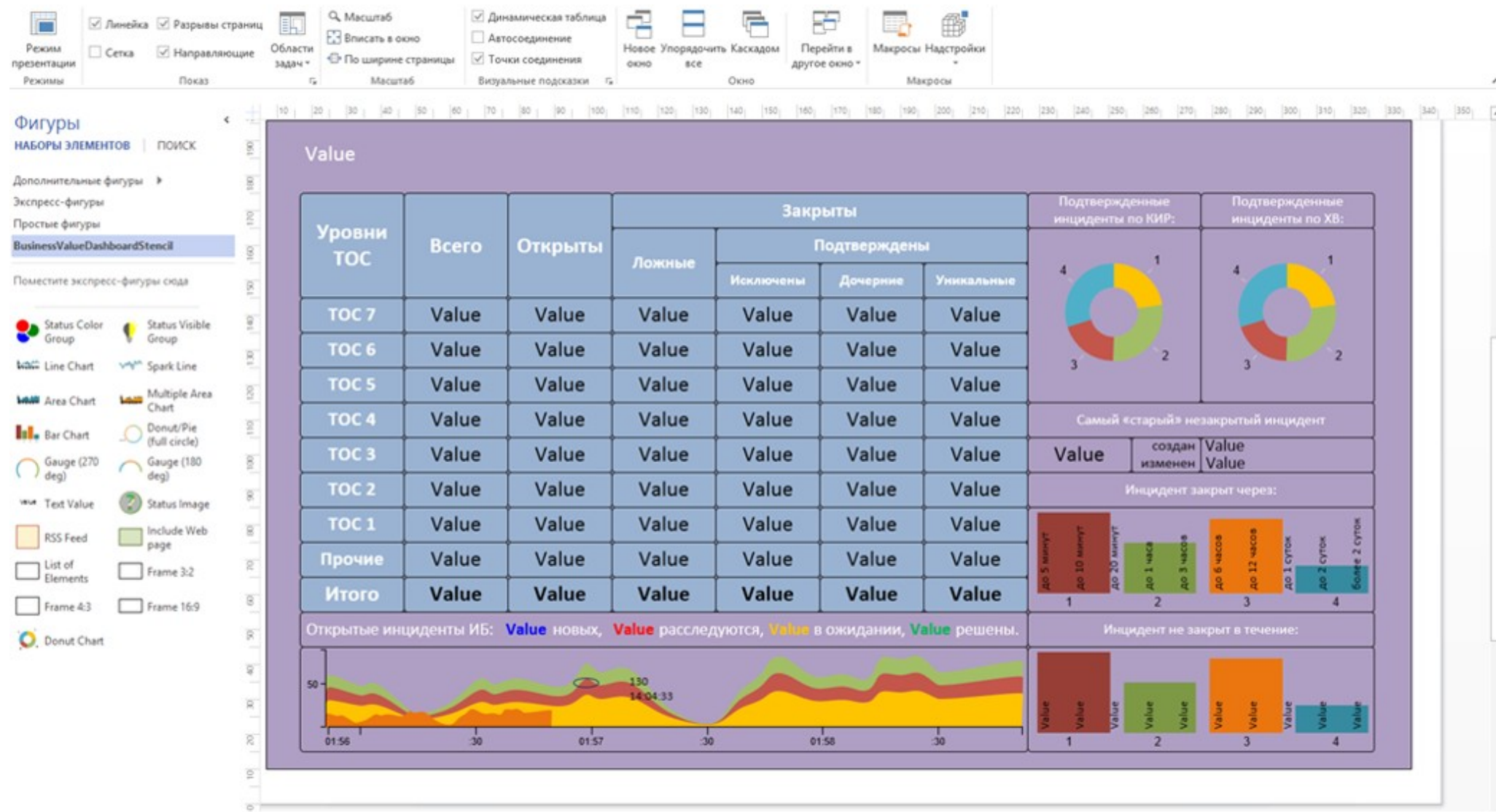
Использование сообщений о событиях обработки активов (вместо доступа к оперативным данным АС)

Используемый сборщик должен поддерживать алгоритмы обработки сообщений для выделения значений необходимых для расчета метрик

Используемый сборщик должен поддерживать все возможные форматы данных АС-источников (СУБД, текстовые файлы, syslog, XML, журналы Windows и т.д.)



Реализация: настройка панелей BVD



Реализация: настройка панелей BVD

OMi Business Value Dashboard Панели мониторинга

← Вернуться к свойствам панели мониторинга

Мини-приложение: group621 (Диаграмма с линиями/областями)

Свойства

Канал данных: SVOI, HPSM, Active

Поле данных: OpnNew, OpnWrk, OpnPnd, OpnSlv

Минимальное значение: 0

Максимальное значение: 0

Автоматическое масштабирование диаграммы:

Наведение указателя мыши:

Показать числовые значения на диаграмме:

Цвета диаграммы: #00B050;#FFC000;#FF0000;#0000FF

Период диаграммы в минутах: 180

Формат числа: не определено

Правило видимости: не определено

Гиперссылка: на другую панель мониторинга на URL-адрес

Сохранить Применить Отмена

Уровни ТОС	Всего	Открыты	Закреты				Подтвержденные инциденты по КИР:	Подтвержденные инциденты по ХВ:
			Ложные	Подтверждены				
				Исключены	Дочерние	Уникальные		
ТОС 7	Value	Value	Value	Value	Value	Value		
ТОС 6	Value	Value	Value	Value	Value	Value		
ТОС 5	Value	Value	Value	Value	Value	Value		
ТОС 4	Value	Value	Value	Value	Value	Value		
ТОС 3	Value	Value	Value	Value	Value	Value		
ТОС 2	Value	Value	Value	Value	Value	Value		
ТОС 1	Value	Value	Value	Value	Value	Value		
Прочие	Value	Value	Value	Value	Value	Value		
Итого	Value	Value	Value	Value	Value	Value		

Самый «старый» незакрытый инцидент

Value создан изменен Value Value

Инцидент закрыт через:

1 до 5 минут 2 до 10 минут 3 до 20 минут 4 до 30 минут 5 до 1 часа 6 до 3 часов 7 до 6 часов 8 до 12 часов 9 до 1 суток 10 до 2 суток 11 более 2 суток

Инцидент не закрыт в течение:

Открытые инциденты ИБ Value новых Value расследуются Value в ожидании Value решены.



Заключение

- Использование BVD позволяет обеспечить оперативный и аналитический (на глубину хранения) мониторинг работы контролируемых процессов.
- Метрики позволяют Заказчикам оперативно отслеживать «здоровье» своих процессов и своевременно реагировать на сбои.
- Графическое представление позволяет сравнивать метрики между собой и выявлять несоответствия или подозрительные расхождения



Вопросы и ответы

Наталья Попова

Руководитель группы управления ИТ-инфраструктурой

Тел: +7 843 567 57 57 (доп. 5424),
e-mail: Natalya.Popova@icl.kazan.ru