ITSF

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

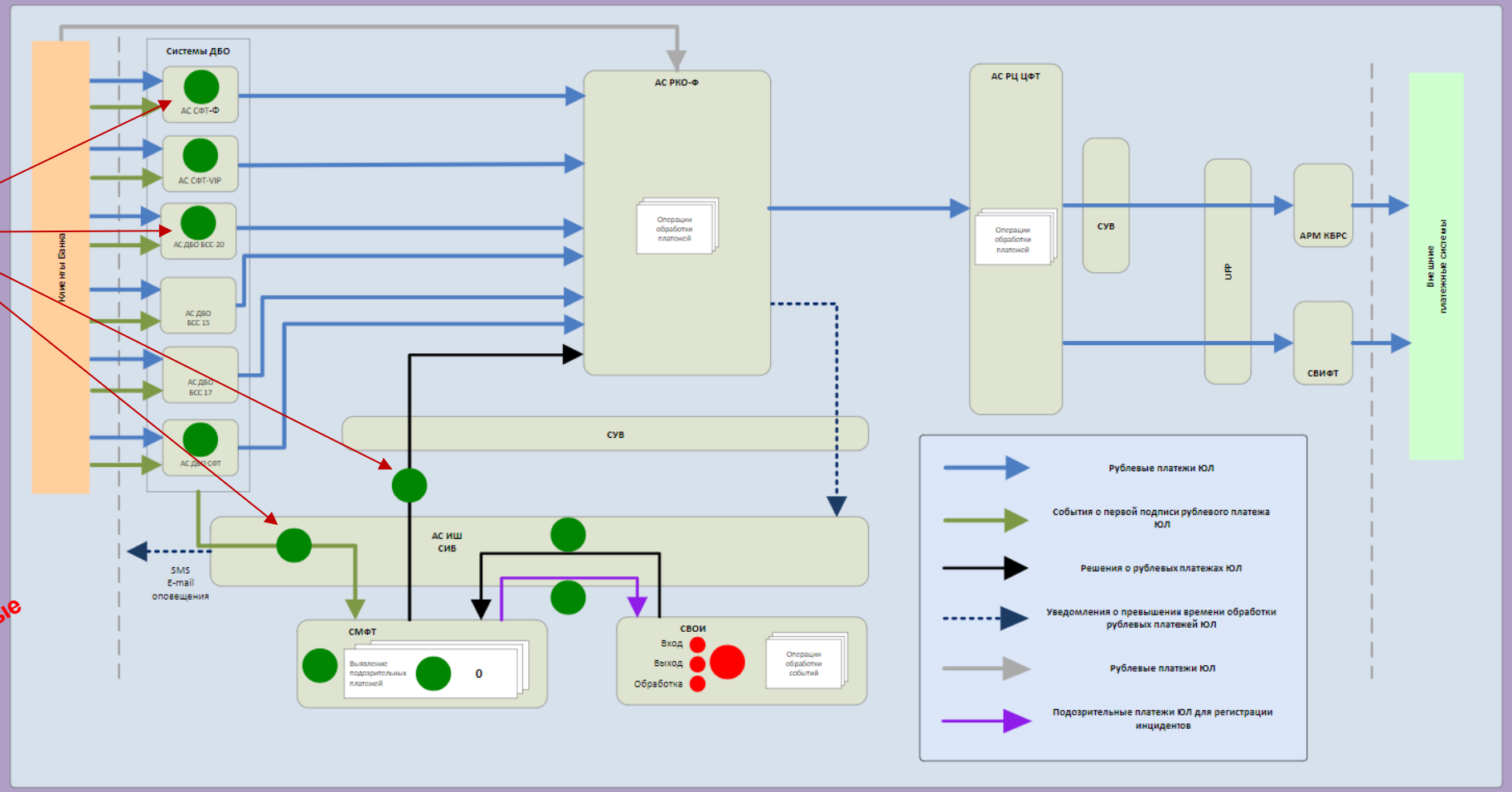
Задачи системы

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.

ГАЗПРОМБАНК

Индикатор состояния обработки на отдельных системах/этапах



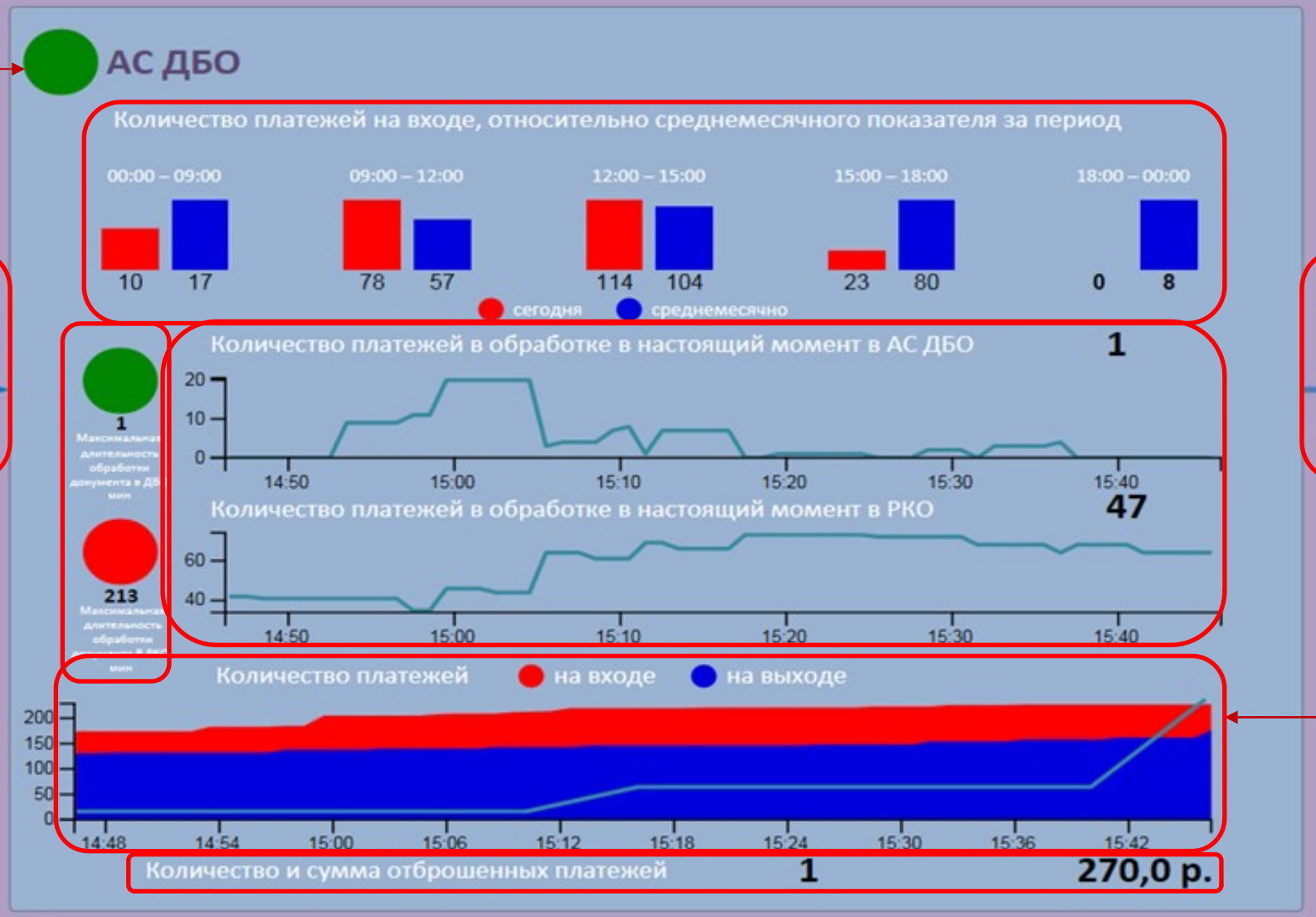
(в течении опер. дня с 00:00 текущего дня до 00:00 следующего дня)

Это пример, а не реальные данные

Мониторинг банковского технологического процесса обработки платежей ЮЛ

ITSF

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



Количество и сумма платежей на входе

225

249 694 002,3 р.

Количество и сумма платежей на выходе

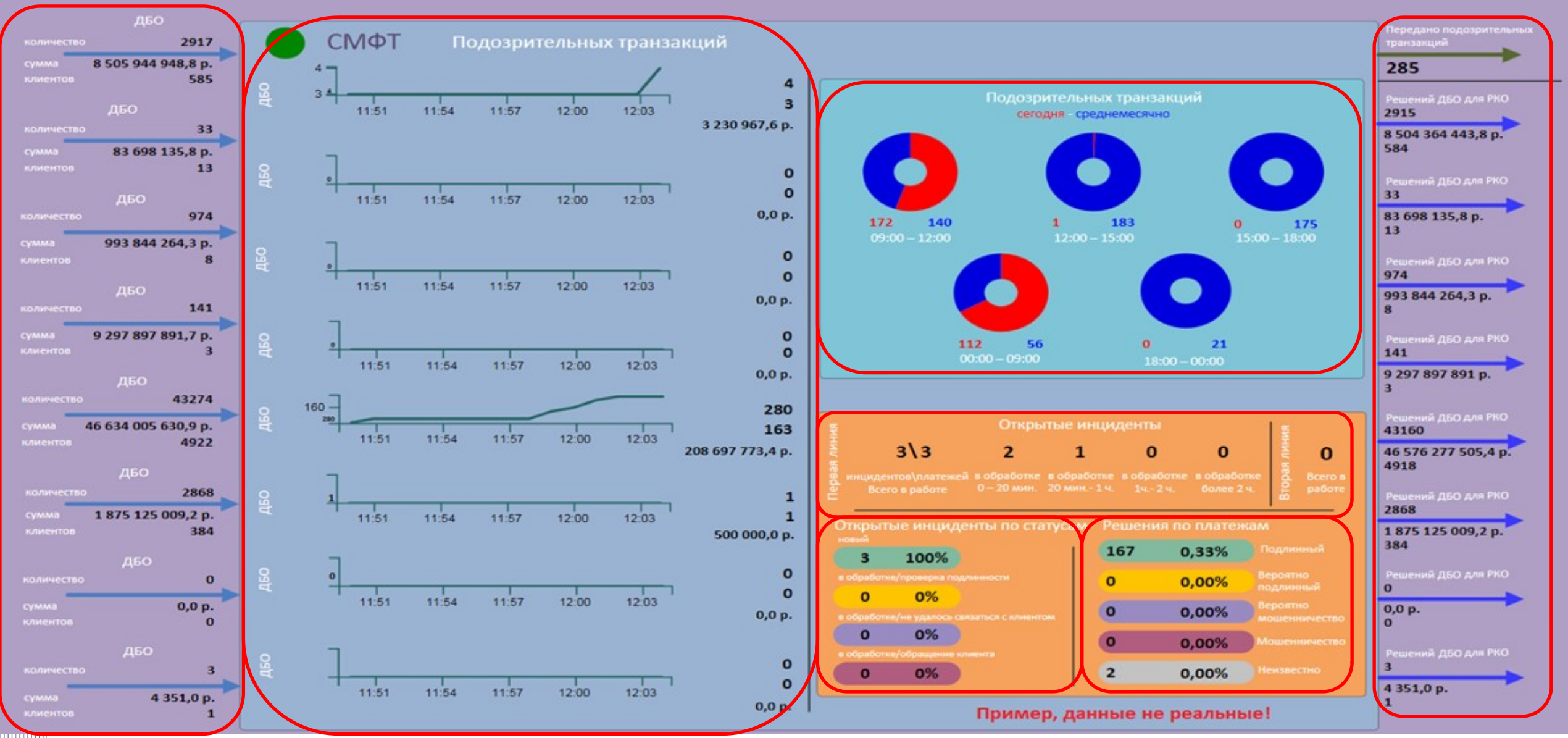
176

232 803 065,7 р.

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)

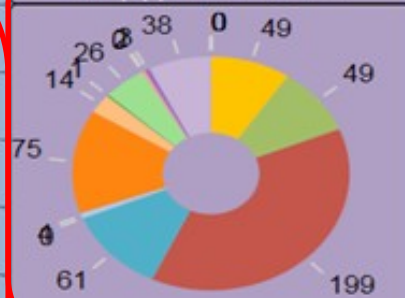


Мониторинг антифрод системы

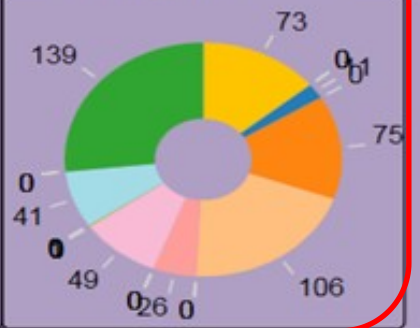
Пример. Данные не реальные!

Уровни ТОС	Всего	Открыты	Закрыты			
			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**

Подтвержденные инциденты по КИР:



Подтвержденные инциденты по ХВ:

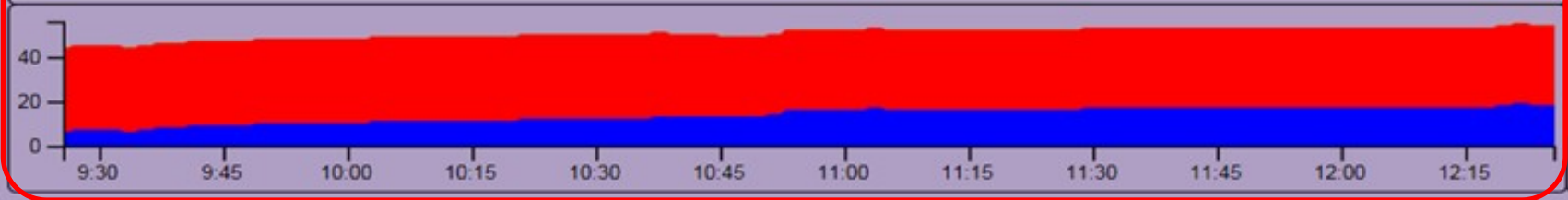


Самый «старый» незакрытый инцидент

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

Инцидент закрыт через:

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



Инцидент не закрыт в течение:

Мониторинг обработки инцидентов ИБ

Зачем всё это нужно?

Владельцы бизнес процессов:

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

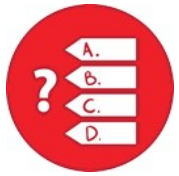
Подразделение по защите информации:

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

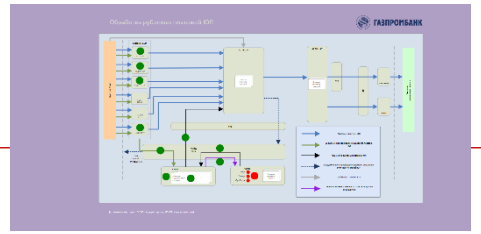
Описание бизнес-процесса с использованием методики:

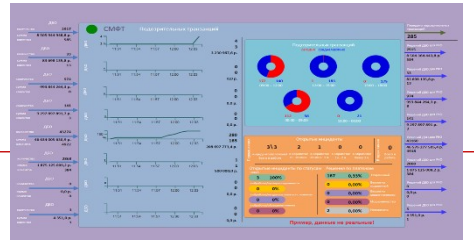
- Определение активов («что обрабатывается бизнес-процессом»)
- Определение стадий обработки активов и условий перехода
- Определение АС в составе бизнес-процесса

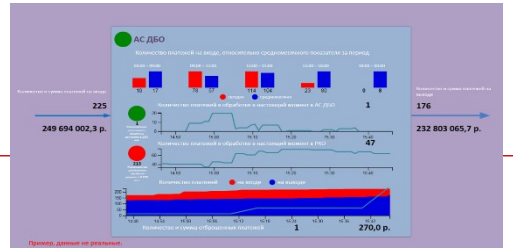
Подготовка списка метрик бизнес-процесса

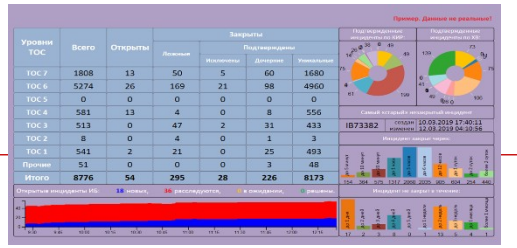
- Количественные и качественные
- По единицам измерения (количество, время, рубли и т.п.)
- Оперативные и исторические
- Типовой способ: «вход», «выход», «промежуточные стадии»

Реализация: настройка ПО









BVD - представление показателей на графических панелях

PostgreSQL

Расчет и хранение ключевых показателей

ArcSight ArcSight ArcSight ArcSight ArcSight ArcSight

Сборщики событий

АС 1 АС 2 TXT АС 3 ... АС N LOG

АС - источники данных

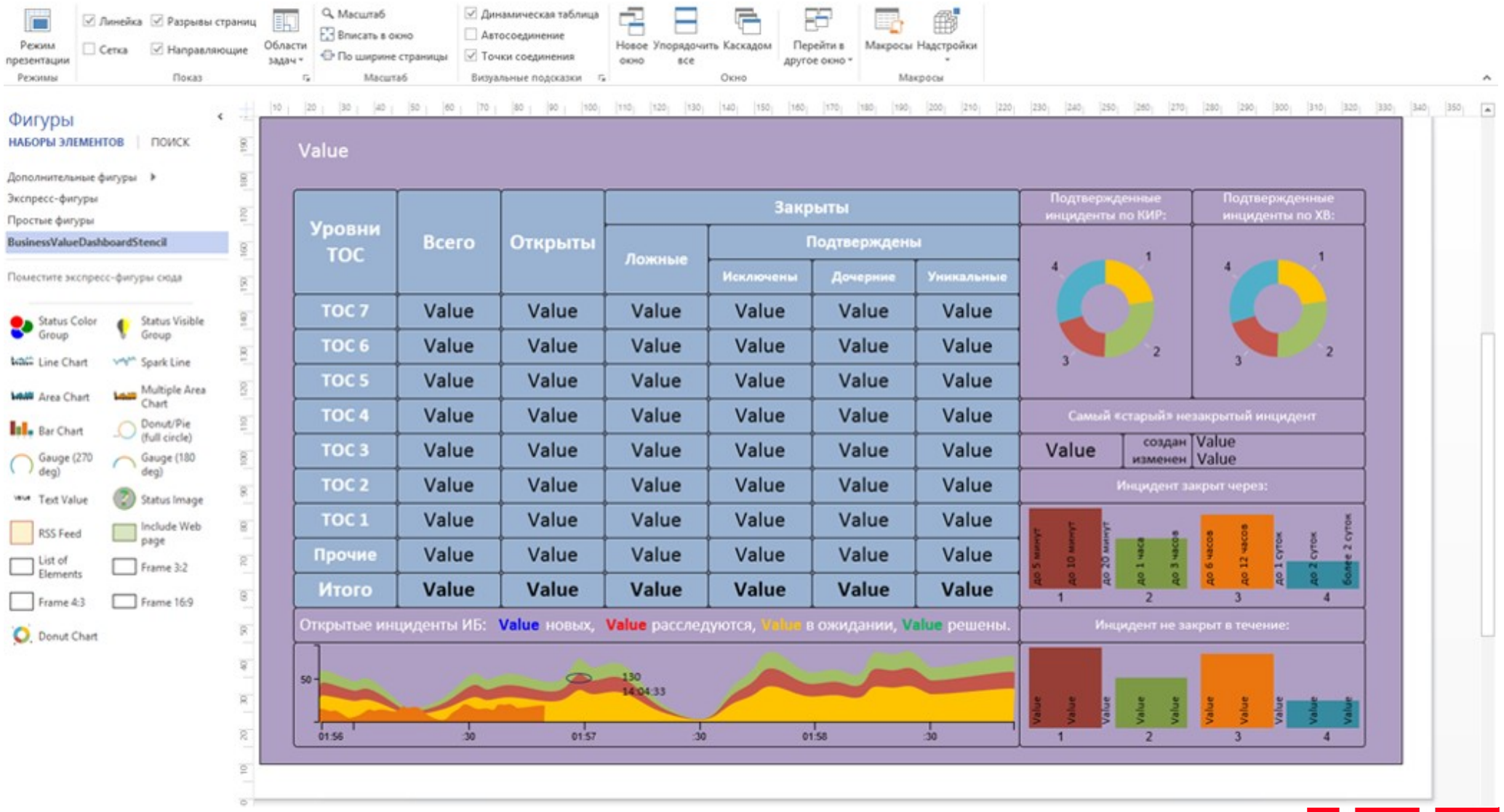
Реализация: сбор данных из АС

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

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