

БЕЗОПАСНОСТЬ

ВМЕСТЕ

Бизнес-прозрачность безопасности приложений
через метрики и автоматизацию



sultanovdr@msk.bcs.ru

01

Отчёты разрознены и закрыты

02

Непонятный вклад ИБ-команды в выручку

03

Сложно сопоставить с финансами и рисками

04

Потеря фокуса и время на рутину отчетности

05

Ручной сбор данных поздний и манипулируем

06

Отсутствие единого стандарта метрик



Открытые метрики

Выделение сервисов безопасности

KPI/SLA/ROI понятные для руководителей

Перевод технических результатов в бизнес-смысл

Визуализация в Power BI для разных уровней управления

Автоматизация

Автоматический сбор данных от всех источников

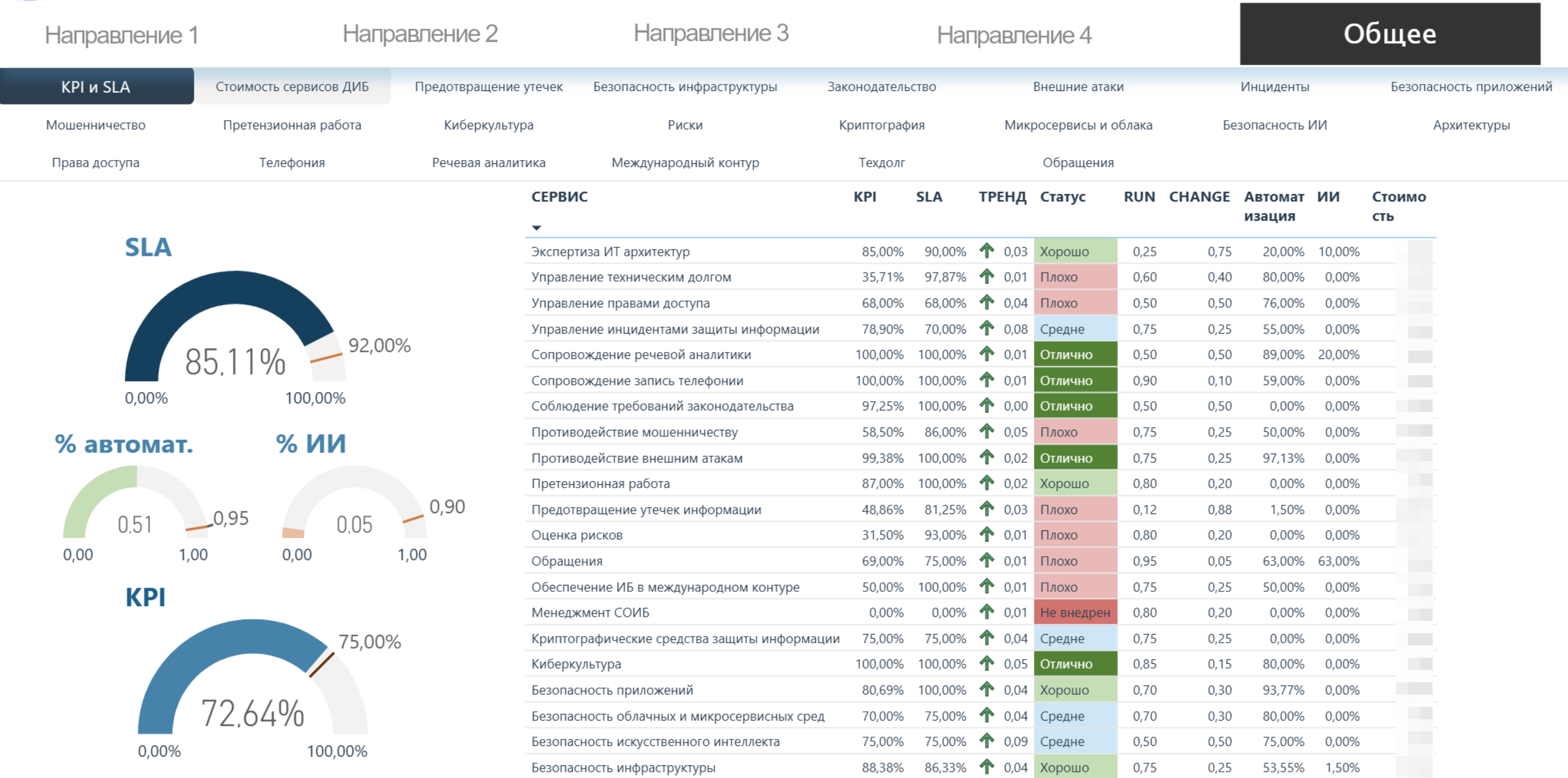
Нормализация и дедупликация с помощью Airflow

Устранение рутины и фокус на инженерных улучшениях

Результат

Превращение ИБ из «чёрного ящика» в понятный продукт с прозрачной ценностью для бизнеса

БКС Сервисы безопасности | Дирекция информационной безопасности



Покрытие проверками
90%

Время недоступности
сервиса
0 мин.

Число автопроверок
1238

- Бизнес-эффект:**
- ✓ Перевод времени атак в стоимость простоя
 - ✓ Оценка предотвращенных потерь








Эффективность
противодействия DDoS-атакам
100%

Время недоступности под DDoS
0 мин.

Количество отраженных атак
301

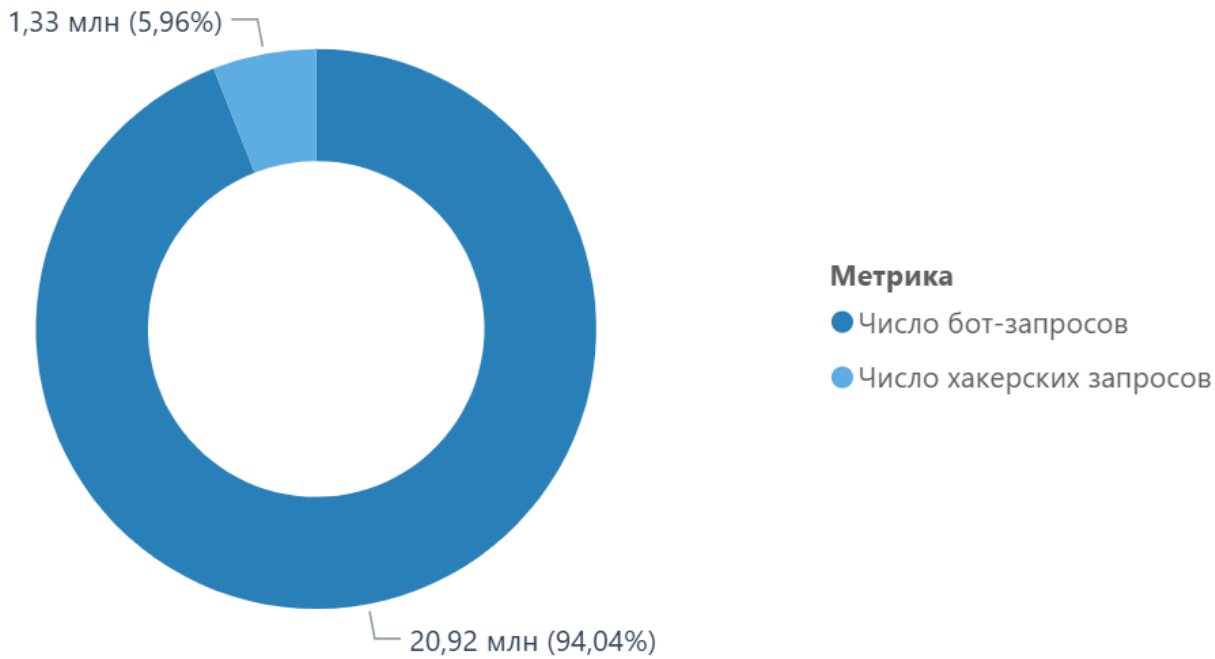
- Бизнес-эффект:**
- ✓ Перевод времени атак в стоимость простоя
 - ✓ Оценка предотвращенных потерь

БКС Противодействие внешним атакам

Направление 1		Направление 2		Направление 3		Направление 4		Общее	
KPI		SLA		Автоматизация		ИИ		 млн рублей	
	99,38%		100,00%		97,13%		0,00%		
Время DDoS-атак		Время недоступности под DDoS-атаками		Максимальное число RPS/RPM		Число целевых атак			
12 866,00		МИН. 0,00		МИН. 923 538,00		301,00			

KPI	Сумма	Значение
Процент доверенных портов		87,6%
Процент отклонение времени реагирования больше 15 минут		100,0%
Процент ошибок блокирования		100,0%
Эффективность противодействия DDoS-атакам		100,0%

SLA	Сумма	Значение
Процент атак без вмешательства		100,0%
Процент отклонение жизни фишингового ресурса от 10 дней		100,0%
Процент ошибок блокирования		100,0%

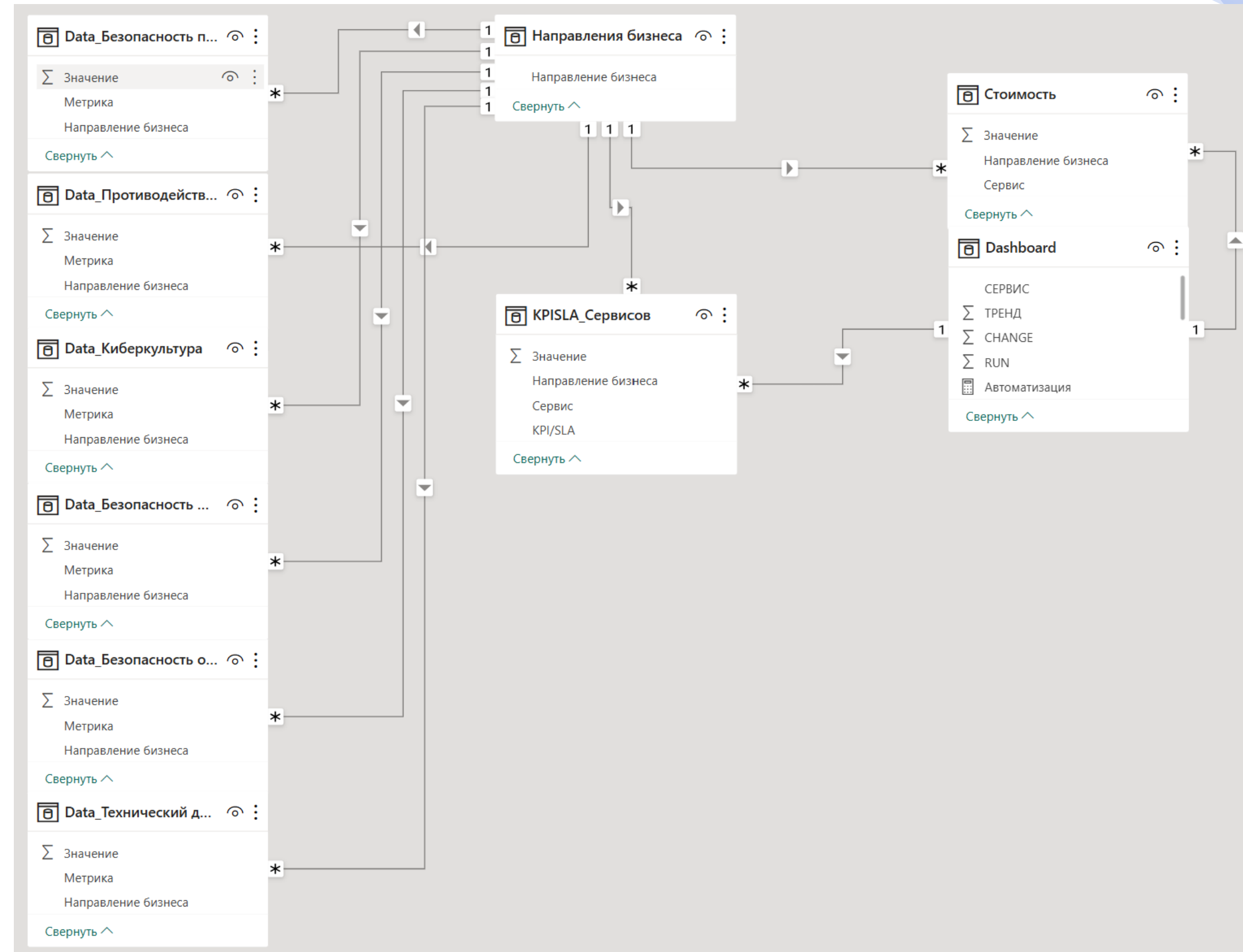


Структура данных и взаимосвязи



- ❑ Единая структура метрик по направлениям бизнеса
- ❑ Связь между KPI, SLA и сервисами
- ❑ Автоматическое обновление из источников
- ❑ Разграничение доступа в том числе по ролям

- 💡 Руководитель видит только бизнес-метрики
- 💡 Технические специалисты получают детализацию



Преимущества автоматизации

Устранение ручного сбора данных и манипуляций

Повышение экспертизы команды безопасности – старт разработки и применение ИИ

Повышение мотивации – меньше текучки, больше инженерных задач

Не обязательно (но можно) приобретать дорогостоящие решения




Наш пример развития

66 DAG (автоматизаций) сбора и обработки данных

- ✓ Мониторинг внешних атак и инцидентов
- ✓ Сбор метрик из систем защиты
- ✓ Обработка данных по уязвимостям
- ✓ Автоматическая классификация обращений
- ✓ И многое другое

Поставка новых версий DAG через интеграцию с GitLab с проверками SAST/DAST/SCA

Автоматизация на opensource? БКС МИР ИНВЕСТИЦИЙ

 Airflow

DAGs

Cluster Activity

Datasets

Security




Browse

Admin

Docs





<div><div></div></div> llm_classifaer_ping	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div>11558</div><div>1</div><div>260</div></div>	<div>***** <div>i</div></div>	<div>2025-09-23, 23:25:00</div> <div>i</div>	<div>2025-09-23, 23:17:00</div> <div>i</div>
<div><div></div></div> LLM_Helper	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div>3828</div><div></div><div>430</div></div>	<div>*/3 ***** <div>i</div></div>	<div>2025-09-23, 23:21:00</div> <div>i</div>	<div>2025-09-23, 23:15:00</div> <div>i</div>
<div><div></div></div> Management_GEO_Block	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div>12925</div><div>1</div><div></div></div>	<div>*/1 ***** <div>i</div></div>	<div>2025-09-23, 23:25:00</div> <div>i</div>	<div>2025-09-23, 23:17:00</div> <div>i</div>
<div><div></div></div> Management_GEO_Block_Auto	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div>112</div><div></div><div></div></div>	<div>None</div> <div>i</div>	<div>2025-09-15, 04:01:03</div> <div>i</div>	
<div><div></div></div> Management_instructions_report	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div>2570</div><div></div><div>15</div></div>	<div>*/5 ***** <div>i</div></div>	<div>2025-09-23, 23:20:00</div> <div>i</div>	<div>2025-09-23, 23:15:00</div> <div>i</div>
<div><div></div></div> Monitoring_internal	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div>12925</div><div>1</div><div></div></div>	<div>*/1 ***** <div>i</div></div>	<div>2025-09-23, 23:25:00</div> <div>i</div>	<div>2025-09-23, 23:17:00</div> <div>i</div>
<div><div></div></div> Phishing_search_and_delete	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><div>12812</div><div>1</div><div>16</div></div>	<div>*/1 ***** <div>i</div></div>	<div>2025-09-23, 23:25:00</div> <div>i</div>	<div>2025-09-23, 23:17:00</div> <div>i</div>

Очевидные плюсы

-  Прозрачность процессов ИБ для бизнеса
-  Автоматизация рутинных операций
-  Измеримый ROI сервисов безопасности
-  Повышение мотивации сотрудников



Неочевидные плюсы

-  Возможность масштабирования автоматизации
-  Дальнейшая интеграция с ИИ на базе airflow
-  Типовые задачи сотрудники захотят автоматизировать
-  Появляется

Пример дорожной карты

Неделя	Базовые задачи	Параллельные задачи автоматизации (Airflow)
1	Выделение сервисов ИБ	Запуск Airflow и конфигурирование, получение доступов
2	Определение источников данных и требований	
3	Определение минимальных SLA/KPI	Проработка основных сценариев где нужна автоматизация
4-5	Разработка модели данных, способа хранения, витрин (Power BI)	Перенос ранее существующей автоматизации, разработка DAG (как минимум 2 типа: framework, script) с помощью ИИ
6	Тестирование, отладка, демонстрация	Тестирование и запуск

СПАСИБО
ЗА ВНИМАНИЕ

ЕСТЬ ВОПРОСЫ?

Султанов Денис Радикович