# Модельный Риск

Подход к централизованному управлению и мониторингу моделей машинного обучения в X5

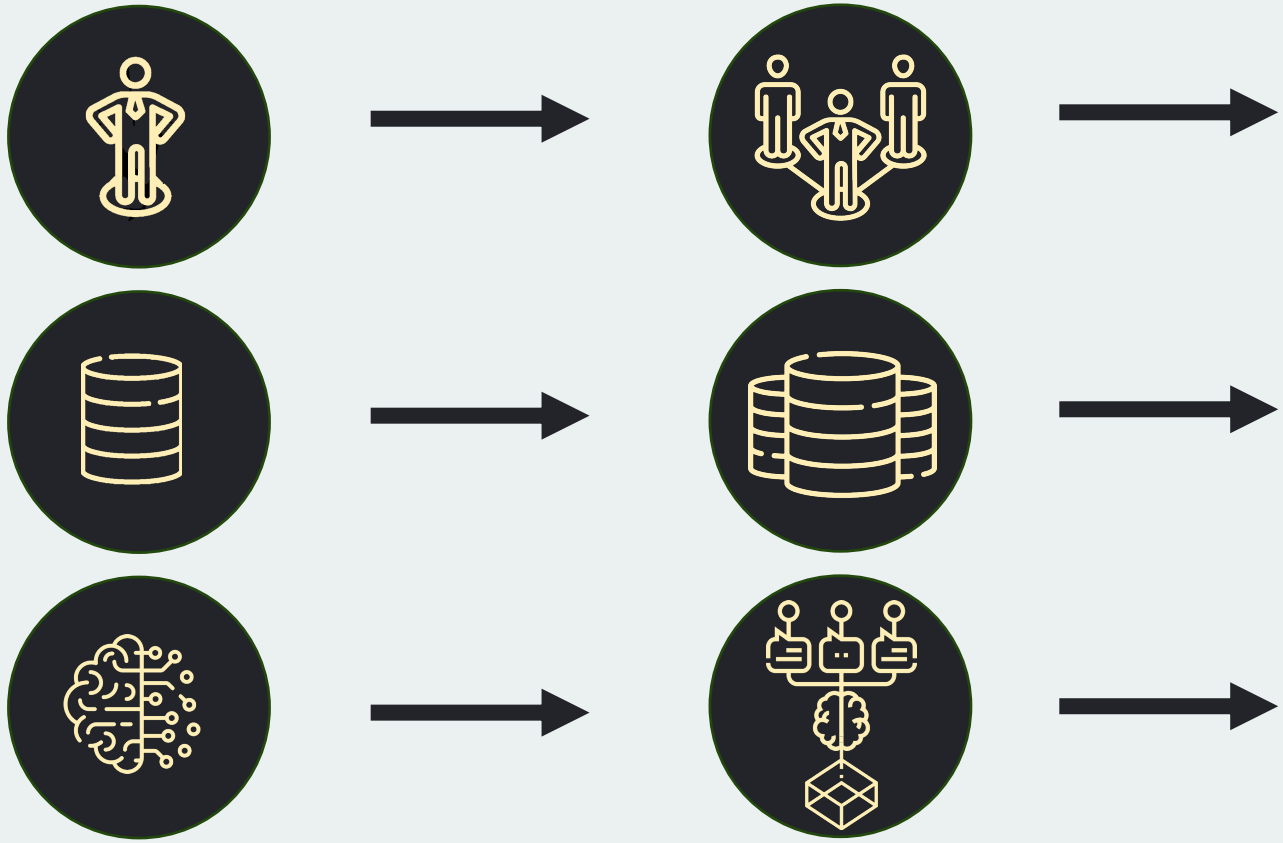
X5 Tech

**Сахнов Александр**

Head of DA/DS
Департамент анализа данных X5 Group

# Зачем нужен контроль модельного риска?

Модельный риск - риск возникновения убытков в результате использования недостаточно точных моделей для принятия решений



People management

Data-driven

???

# Как понять что нужен контроль за модельным риском?

**1;**

## Сложность моделей

Необходим контроль из-за сложности pipeline’ов и трудности интерпретации

**2;**

## Критичность решений

Высокая степень критичности решений, основанных на предсказаниях модели

**3;**

## Динамичность данных

Частые изменения и вариативность исходных данных

**4;**

## Регулятивные требования

Строгие стандарты для моделей машинного обучения

**5;**

## История ошибок

Уже возникшие проблемы с работой и валидацией моделей

**6.**

## Систематизация

Множество моделей, приводящее к дублированию и удлинению разработки

# Как понять что нужен контроль за модельным риском?

1;

## Сложность моделей

Необходим контроль из-за сложности pipeline’ов и трудности интерпретации

2;

## Критичность решений

Высокая степень критичности решений, основанных на предсказаниях модели

3;

## Динамичность данных

Частые изменения и вариативность исходных данных

4;

## Регулятивные требования

Строгие стандарты для моделей машинного обучения

5;

## История ошибок

Уже возникшие проблемы с работой и валидацией моделей

6.

## Систематизация

Множество моделей, приводящее к дублированию и удлинению разработки

# Как понять что нужен контроль за модельным риском?

1;

## Сложность моделей

Необходим контроль из-за сложности pipeline'ов и трудности интерпретации

2;

## Критичность решений

Высокая степень критичности решений, основанных на предсказаниях модели

3;

## Динамичность данных

Частые изменения и вариативность исходных данных

4;

## Регулятивные требования

Строгие стандарты для моделей машинного обучения

5;

## История ошибок

Уже возникшие проблемы с работой и валидацией моделей

6.

## Систематизация

Множество моделей, приводящее к дублированию и удлинению разработки

# Как понять что нужен контроль за модельным риском?

1;

## Сложность моделей

Необходим контроль из-за сложности pipeline'ов и трудности интерпретации

2;

## Критичность решений

Высокая степень критичности решений, основанных на предсказаниях модели

3;

## Динамичность данных

Частые изменения и вариативность исходных данных

4;

## Регулятивные требования

Строгие стандарты для моделей машинного обучения

5;

## История ошибок

Уже возникшие проблемы с работой и валидацией моделей

6.

## Систематизация

Множество моделей, приводящее к дублированию и удлинению разработки

# Как понять что нужен контроль за модельным риском?

1;

## Сложность моделей

Необходим контроль из-за сложности pipeline'ов и трудности интерпретации

2;

## Критичность решений

Высокая степень критичности решений, основанных на предсказаниях модели

3;

## Динамичность данных

Частые изменения и вариативность исходных данных

4;

## Регулятивные требования

Строгие стандарты для моделей машинного обучения

5;

## История ошибок

Уже возникшие проблемы с работой и валидацией моделей

6.

## Систематизация

Множество моделей, приводящее к дублированию и удлинению разработки

# Как понять что нужен контроль за модельным риском?

1;

## Сложность моделей

Необходим контроль из-за сложности pipeline'ов и трудности интерпретации

2;

## Критичность решений

Высокая степень критичности решений, основанных на предсказаниях модели

3;

## Динамичность данных

Частые изменения и вариативность исходных данных

4;

## Регулятивные требования

Строгие стандарты для моделей машинного обучения

5;

## История ошибок

Уже возникшие проблемы с работой и валидацией моделей

6.

## Систематизация

Множество моделей, приводящее к дублированию и удлинению разработки

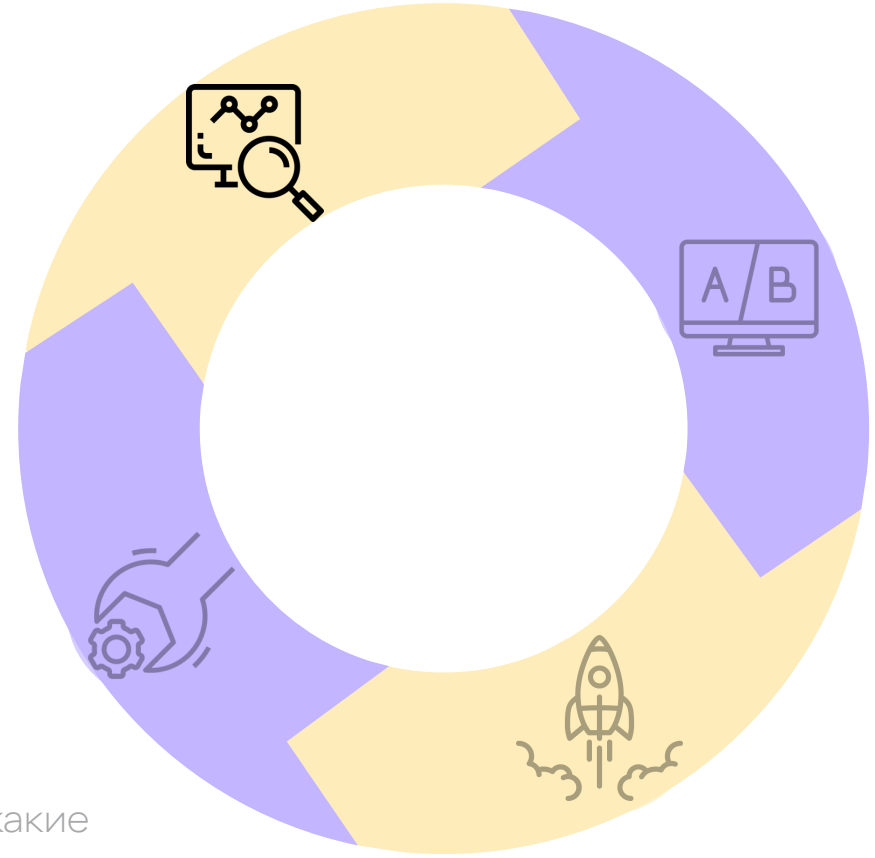
# Типичные проблемы при разработке и деплое ML-модели

## R&D процесс создания модели

- Нет понимания, какие модели уже есть в компании – есть вероятность продублировать уже имеющуюся модель
- Нет контактов владельцев и разработчиков уже имеющихся моделей

## Модификация модели, смена владельца

- Новый руководитель не знает какие модели есть в его подразделении
- При уходе ключевых разработчиков нет регламентов передачи модели




## Пилотирование модели, А/Б-тест

- Нет регламентов и требований к качеству моделей после защиты проекта

## Работа модели в production

- Фактическое качество модели ниже заявленного
- Модель работает на неактуальных данных
- Разработчики не оповещаются о изменении бизнес-процессов, которые связаны с моделью

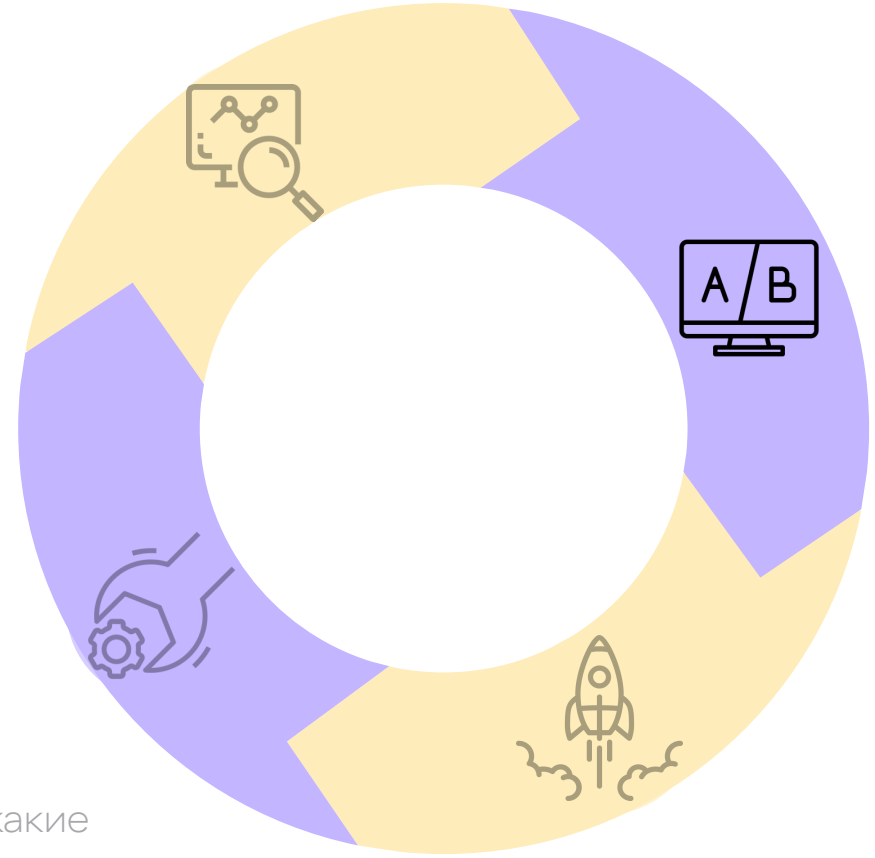
# Типичные проблемы при разработке и деплое ML-модели

## R&D процесс создания модели

- Нет понимания какие модели уже есть в компании – есть вероятность продублировать уже имеющуюся модель
- Нет контактов владельцев и разработчиков уже имеющихся моделей

## Модификация модели, смена владельца

- Новый руководитель не знает какие модели есть в его подразделении
- При уходе ключевых разработчиков нет регламентов передачи модели




## Пилотирование модели, А/Б-тест

- Нет регламентов и требований к качеству моделей после защиты проекта

## Работа модели в production

- Фактическое качество модели ниже заявленного
- Модель работает на неактуальных данных
- Разработчики не оповещаются о изменении бизнес-процессов, которые связаны с моделью

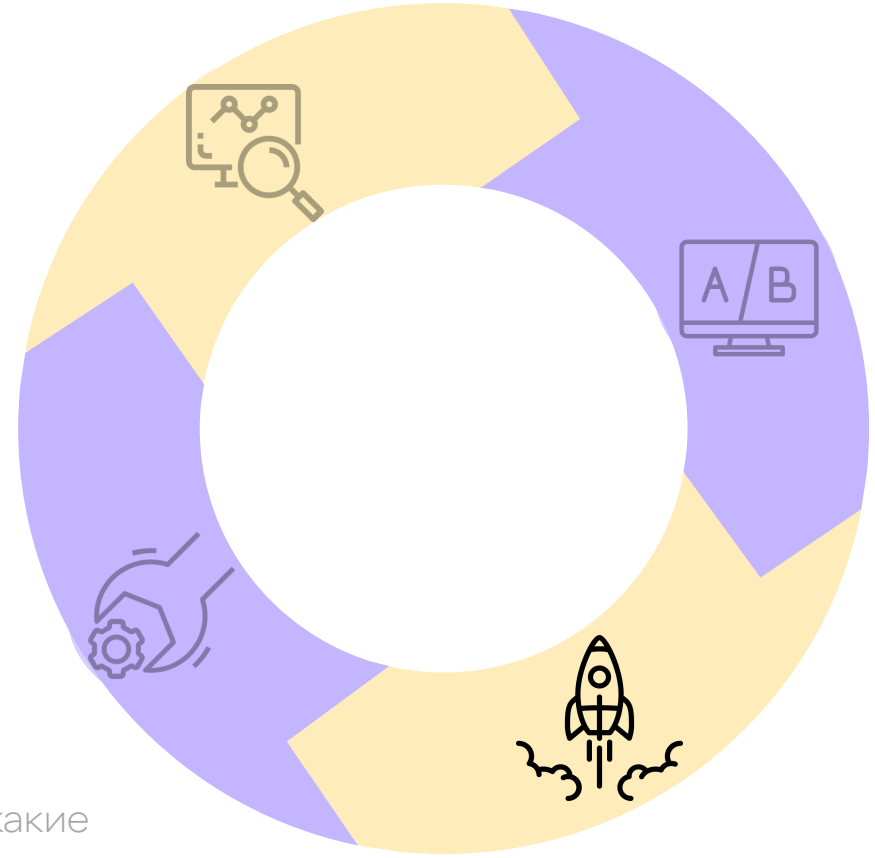
# Типичные проблемы при разработке и деплое ML-модели

## R&D процесс создания модели

- Нет понимания какие модели уже есть в компании – есть вероятность продублировать уже имеющуюся модель
- Нет контактов владельцев и разработчиков уже имеющихся моделей

## Модификация модели, смена владельца

- Новый руководитель не знает какие модели есть в его подразделении
- При уходе ключевых разработчиков нет регламентов передачи модели




## Пилотирование модели, А/Б-тест

- Нет регламентов и требований к качеству моделей после защиты проекта

## Работа модели в production

- Фактическое качество модели ниже заявленного
- Модель работает на неактуальных данных
- Разработчики не оповещаются о изменении бизнес-процессов, которые связаны с моделью

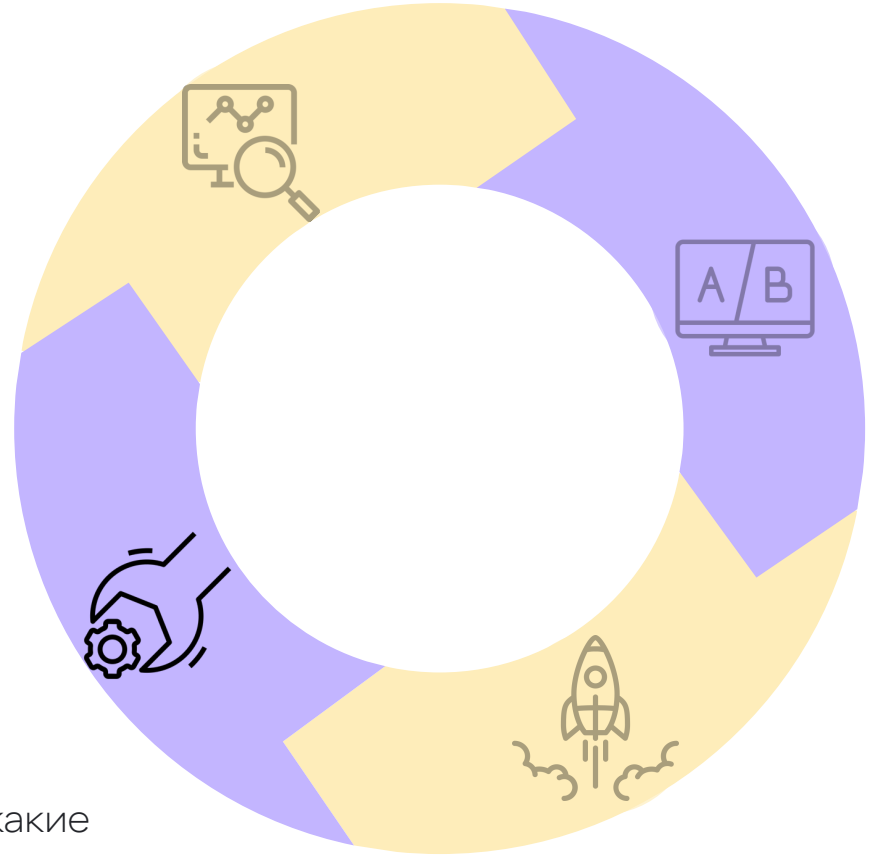
# Типичные проблемы при разработке и деплое ML-модели

## R&D процесс создания модели

- Нет понимания какие модели уже есть в компании – есть вероятность продублировать уже имеющуюся модель
- Нет контактов владельцев и разработчиков уже имеющихся моделей

## Модификация модели, смена владельца

- Новый руководитель не знает, какие модели есть в его подразделении
- При уходе ключевых разработчиков нет регламентов передачи модели




## Пилотирование модели, А/Б-тест

- Нет регламентов и требований к качеству моделей после защиты проекта

## Работа модели в production

- Фактическое качество модели ниже заявленного
- Модель работает на неактуальных данных
- Разработчики не оповещаются о изменении бизнес-процессов, которые связаны с моделью

# Типичные проблемы при разработке и деплое ML-модели

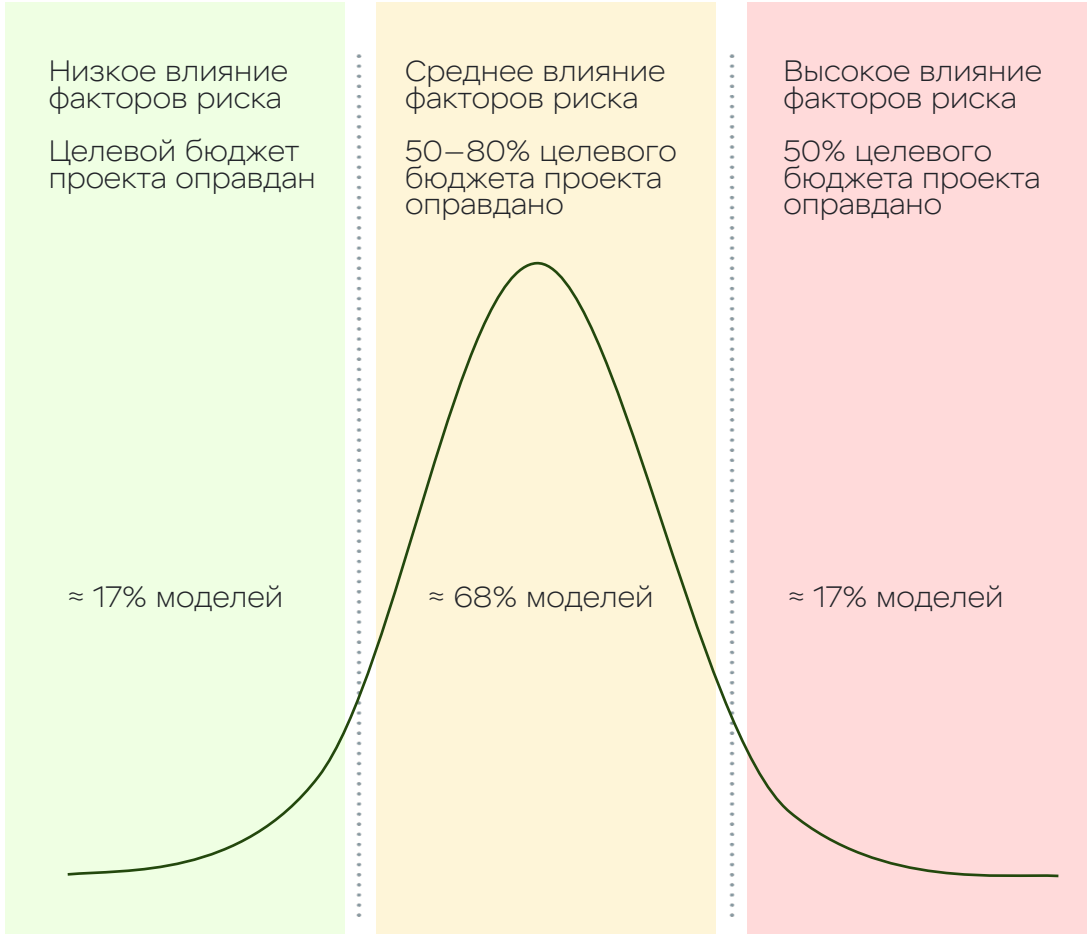
Как обычно решают эти проблемы:

- Ответственность за мониторинг ложится на продактов/разработчиков
- Команды отдельно ведут свой реестр моделей, никто не знает, что происходит вовне
- При уходе ключевых разработчиков модель попадает в legacy и “устаревает”
- Модель переобучается только при наличии ресурсов в команде
- После деплоя метрики модели “подгоняются”, зачастую игнорируется честная валидация

# Теоретическая оценка убытков от модельного риска

- Пусть есть модель X, стоимость разработки и поддержки которой стоит в среднем 1 усл. ед. руб. в год
- Оценим всевозможные модельные риски
- Усредним влияние рисков и оценим убытки с 1 модели:

Оптимистично: **0.2 усл. ед. руб. убытков**
Пессимистично: **0.5 усл. ед. руб. убытков**




## Теоретическая оценка:

Если в компании всего 50 моделей со средним бюджетом в 10 млн. в год на каждую, то получим:

Оптимистично: **100 млн убытков в год**
Пессимистично: **250 млн убытков в год**

Стоит учитывать, что одна модель может использоваться в разных продуктах, и модельный риск также кратно увеличивает вероятность убытков во всех связанных продуктах

# Какие бывают риски?

## Риски связанные с работой модели:

- ☑ Модель не обновляла метрики N дней
- ☑ Модель не делала предсказаний n часов

## Риски связанные с исходными данными:

- ☑ Структура исходных данных изменилась
- ☑ В исходных данных наблюдаются distribution shift'ы
- ☑ Исходные данные потеряли актуальность

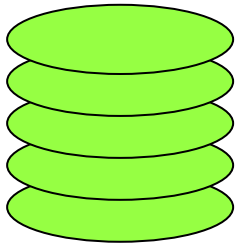
## Риски связанные с информацией о модели:

- ☑ Код pipeline'а по обучению модели не воспроизводим
- ☑ Не заполнена/актуализирована информация о модели, ее владельцах и решаемой задаче
- ☑ Не заполнены актуальные бизнес-метрики и прокси-метрики модели

## Другие риски:

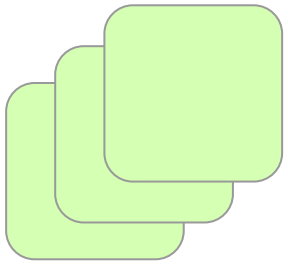
- ☑ Значение метрики/количества предсказаний в единицу времени значительно изменилось
- ☑ Alert/обратная связь от стейкхолдеров из бизнеса
- ☑ Baseline решение превышает последнее значение целевой метрики

# Как модельный риск решает эти проблемы?



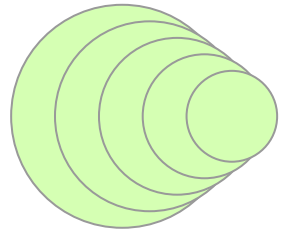
## Актуализация

Информирование product и project-менеджеров, ML/DS-разработчиков и стейкхолдеров о состоянии и изменениях в работе моделей



## Мониторинг

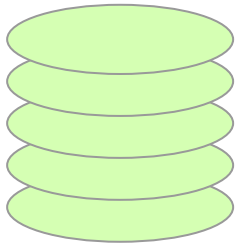
Единое место, где все участники процессов, связанных с моделью, смогут отслеживать все доступные модели и их метрики



## Централизация

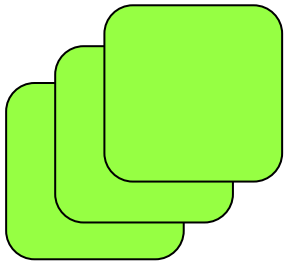
Проявляется централизованный верхнеуровневый мониторинг над моделями: все модели регистрируются в единой системе

# Как модельный риск решает эти проблемы?



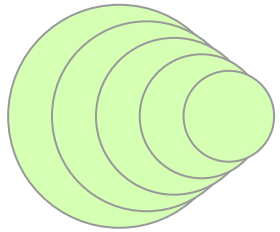
## Актуализация

Информирование product и project менеджеров, ML/DS разработчиков и стейкхолдеров о состоянии и изменениях в работе моделей



## Мониторинг

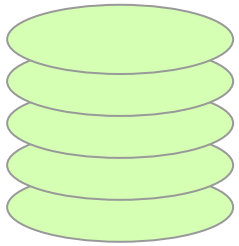
Единое место, где все участники процессов, связанные с моделью, смогут отслеживать все доступные модели и их метрики



## Централизация

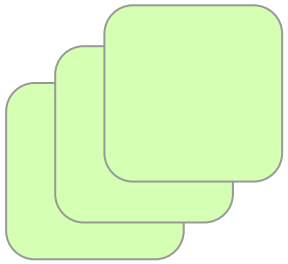
Проявляется централизованный верхнеуровневый мониторинг над моделями: все модели регистрируются в единой системе

# Как модельный риск решает эти проблемы?



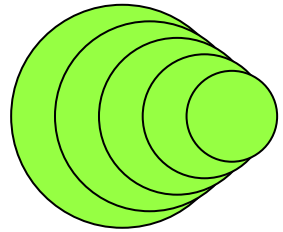
## Актуализация

Информирование product и project менеджеров, ML/DS разработчиков и стейкхолдеров о состоянии и изменениях в работе моделей



## Мониторинг

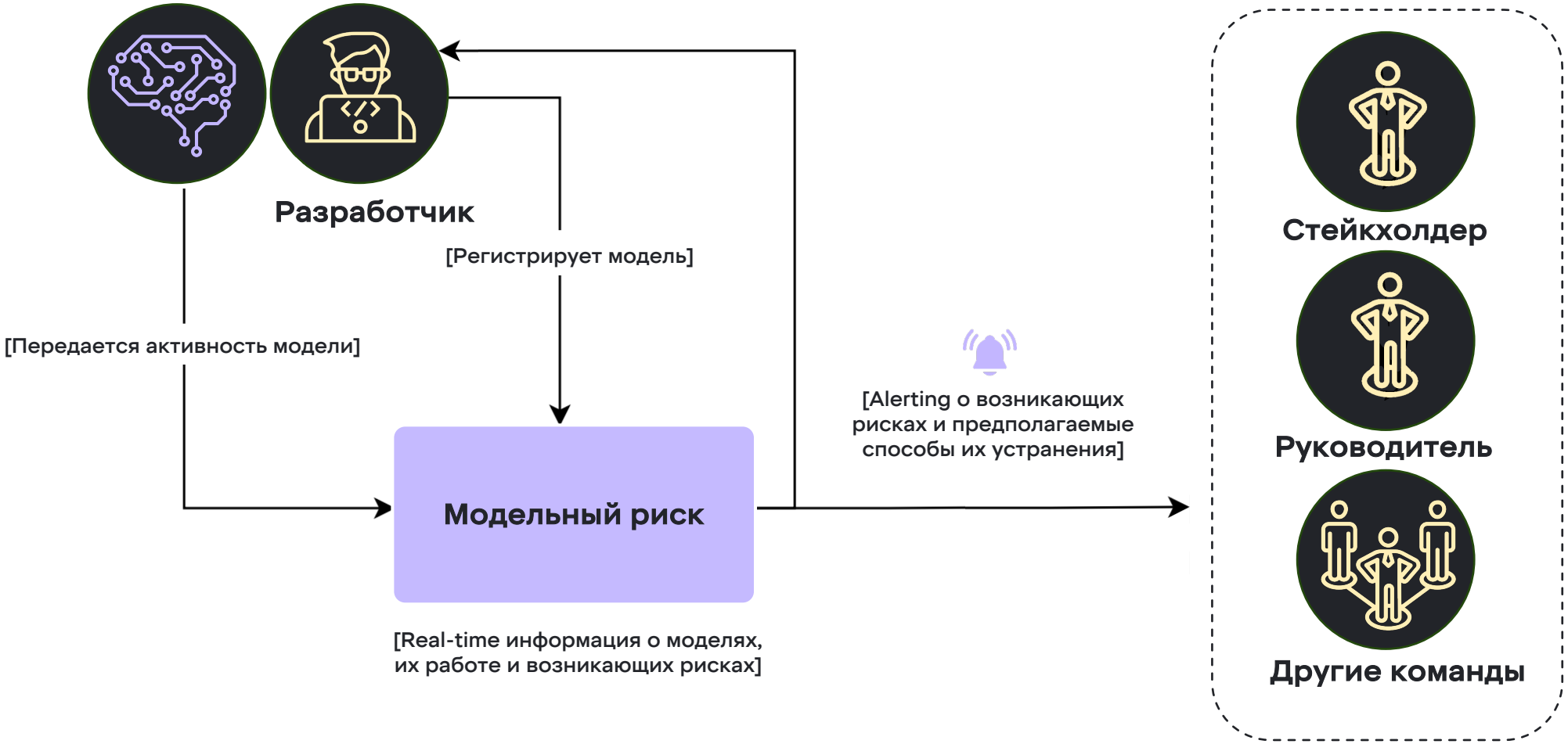
Единое место, где все участники процессов, связанных с моделью, смогут отслеживать все доступные модели и их метрики



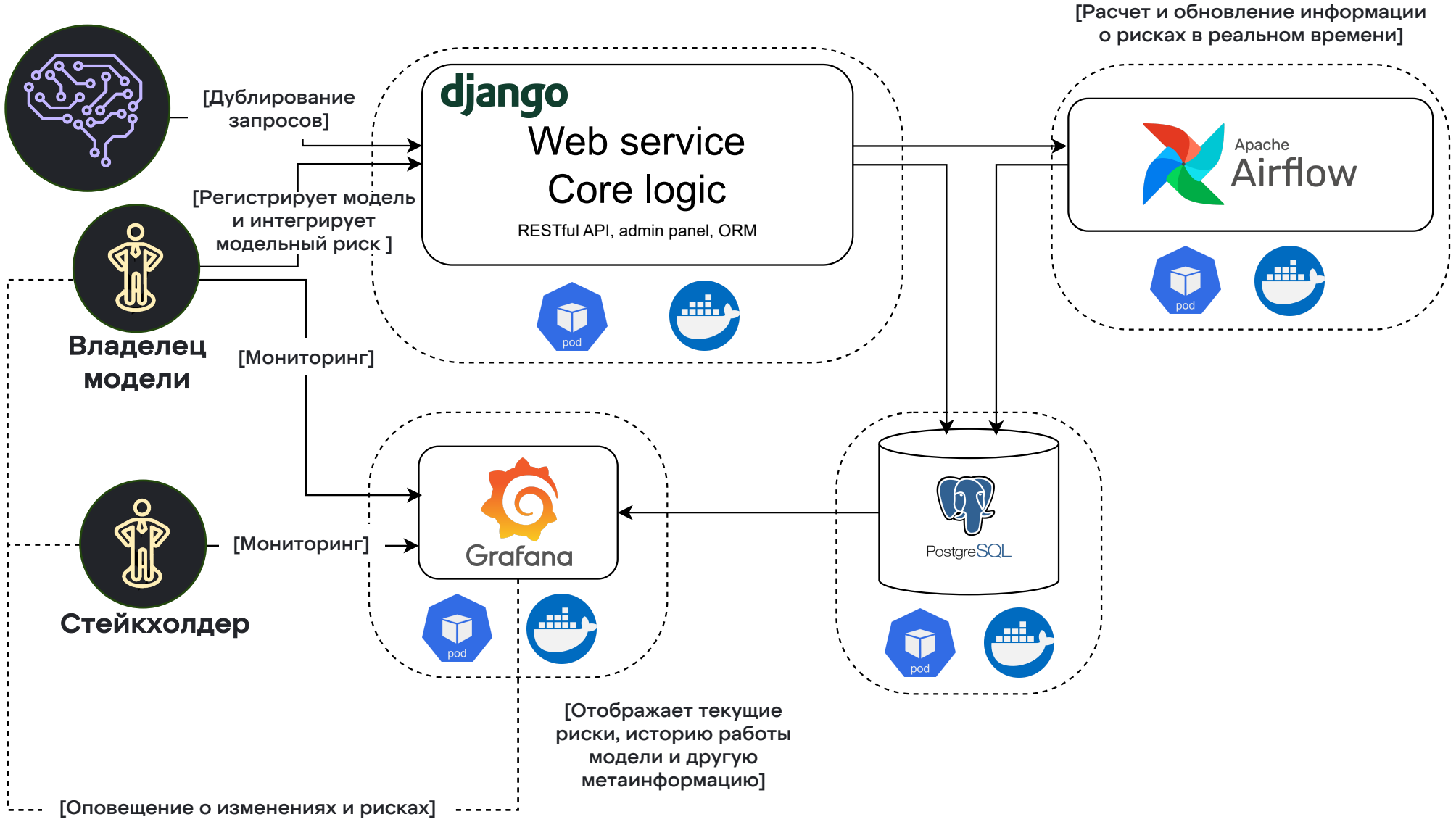
## Централизация

Проявляется централизованный верхнеуровневый мониторинг над моделями: все модели регистрируются в единой системе

# Схема работы

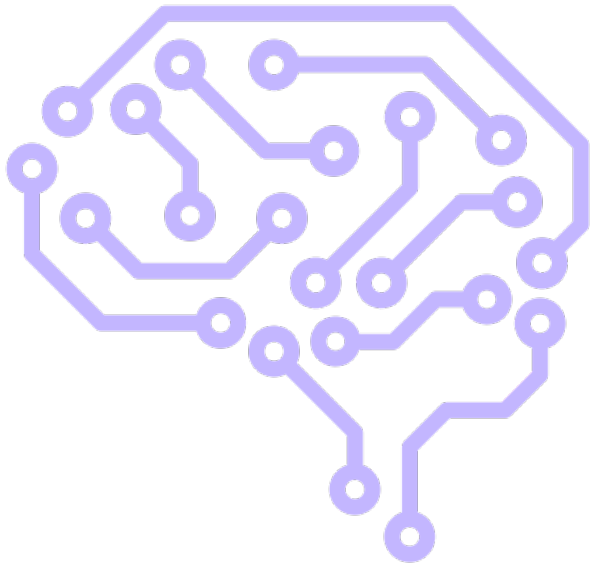


# Архитектура



# Что такое «модель»

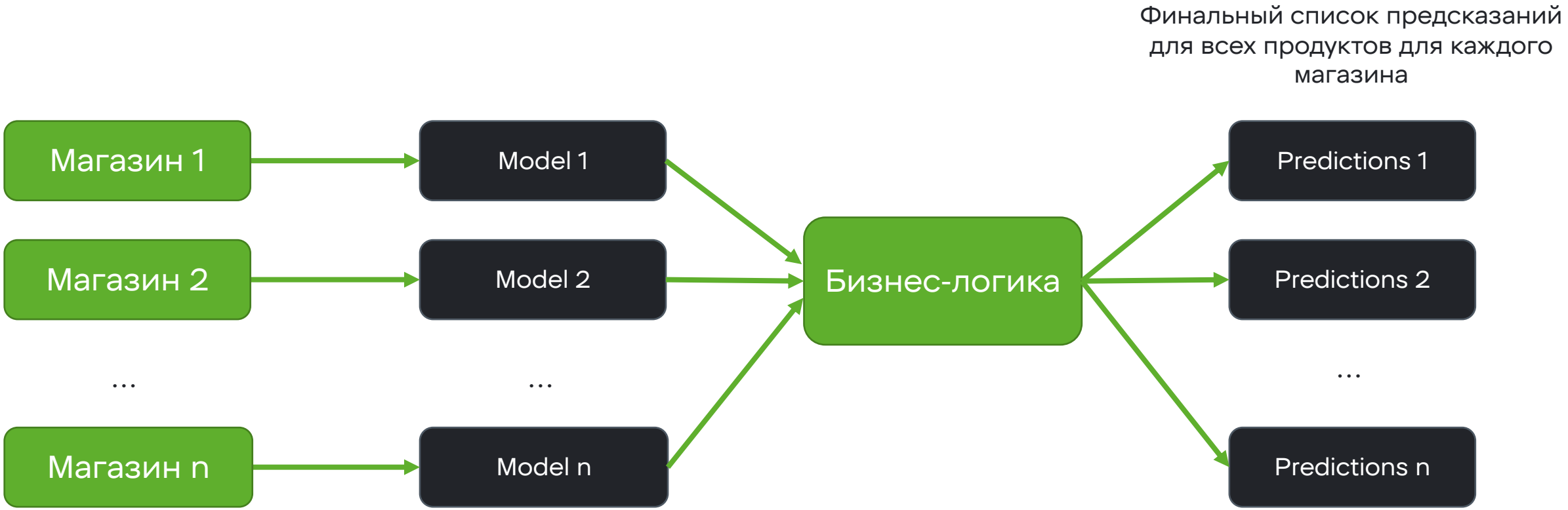
- Модель выполняет определенную **бизнес-логику**
- За моделью закрепляется ее **владелец**
- Работает в **Production** среде
- Имеет 1 и более **прокси-метрик**



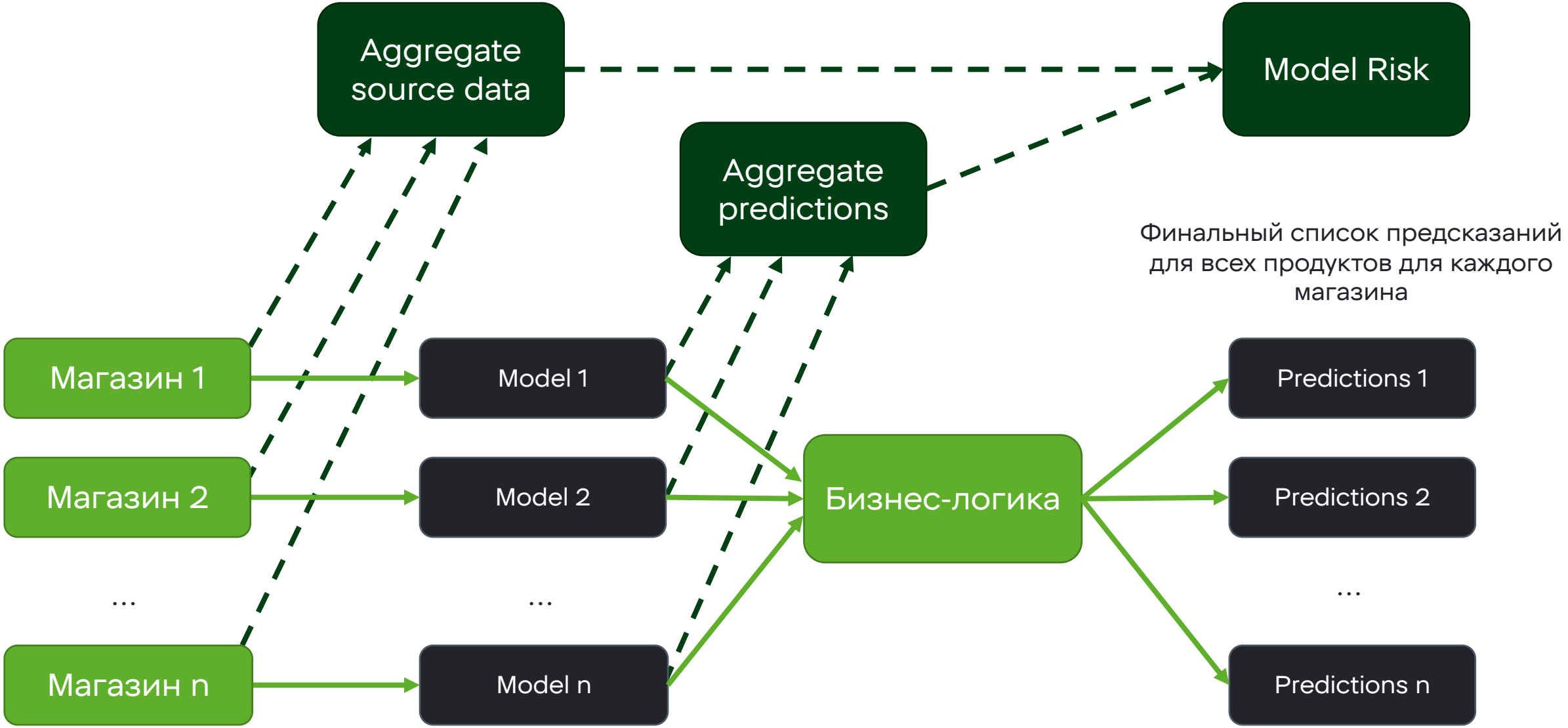
| | |
|---|---|
| XGBoost, в котором после переобучения изменился max_depth | → **Одна и та же модель** |
| XGBoost, для которого изменился feature engineering | → **Одна и та же модель** |
| XGBoost с той же архитектурой, но с другим таргетом | → **Другая модель** |

# Пример «сложной модели»

Набор моделей, каждая из которых предсказывает X для каждого товара в каждом отдельном магазине, имеющий единую бизнес-логику:

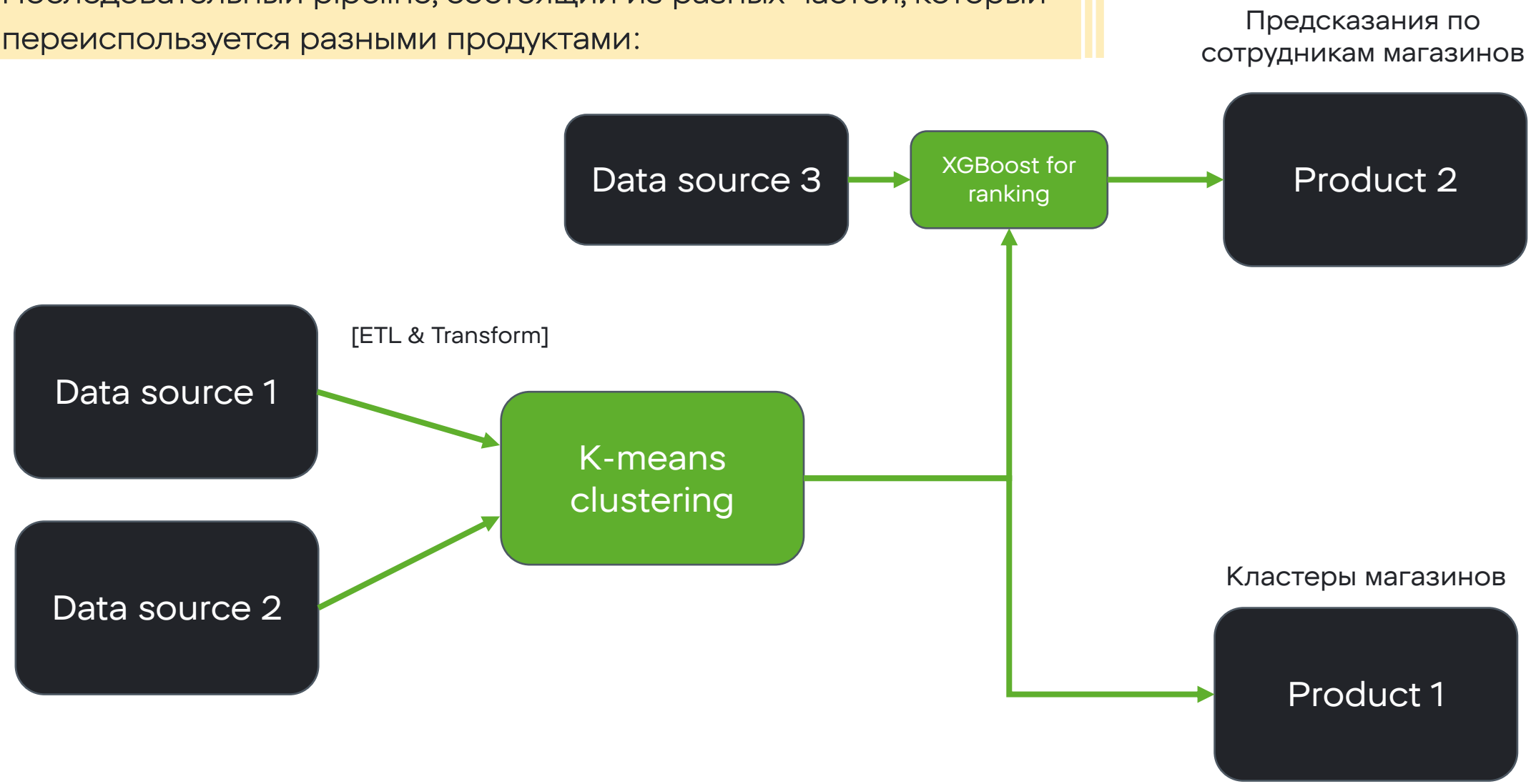


# Пример «сложной модели»

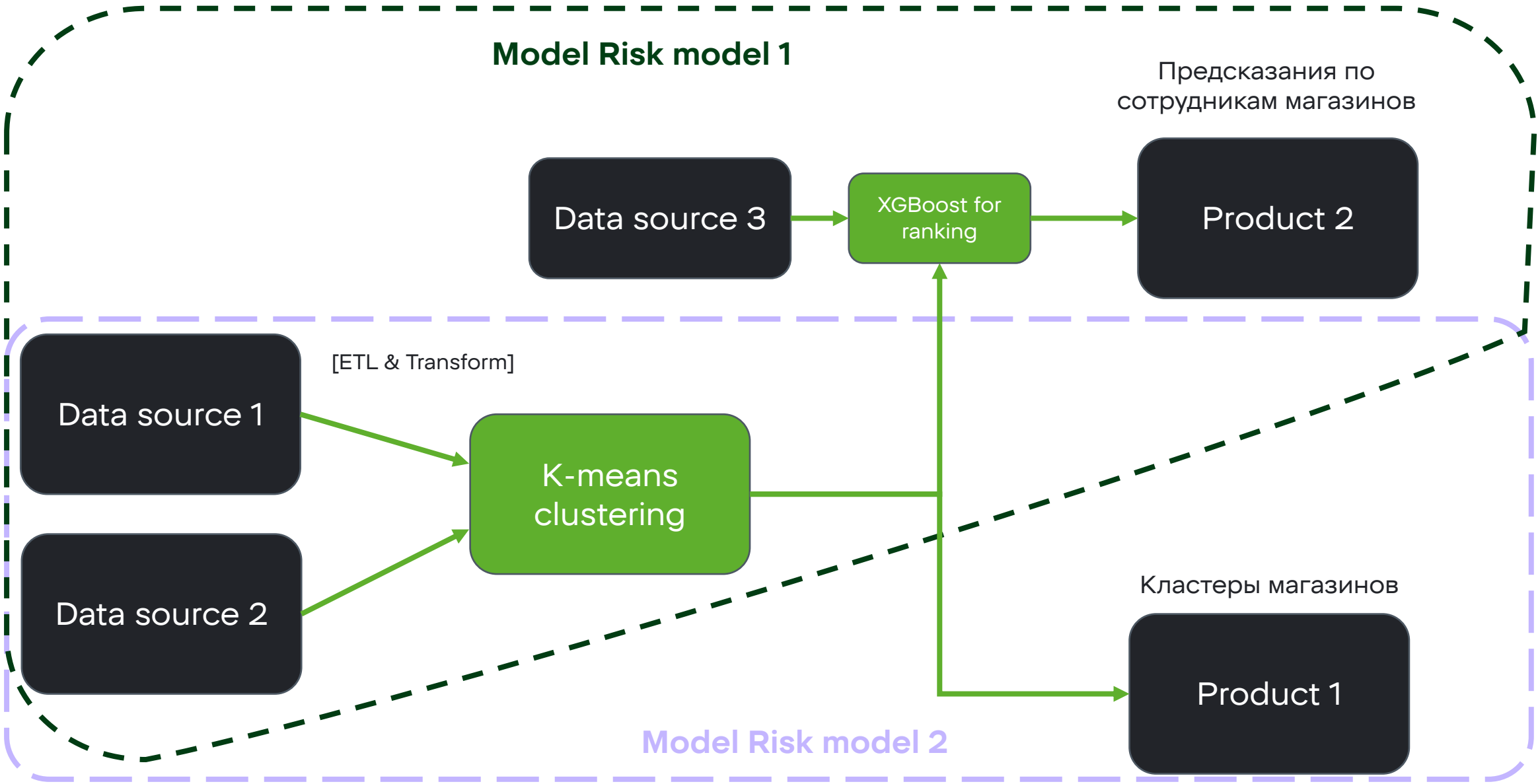


# Пример «сложной модели»

Последовательный pipeline, состоящий из разных частей, который переиспользуется разными продуктами:

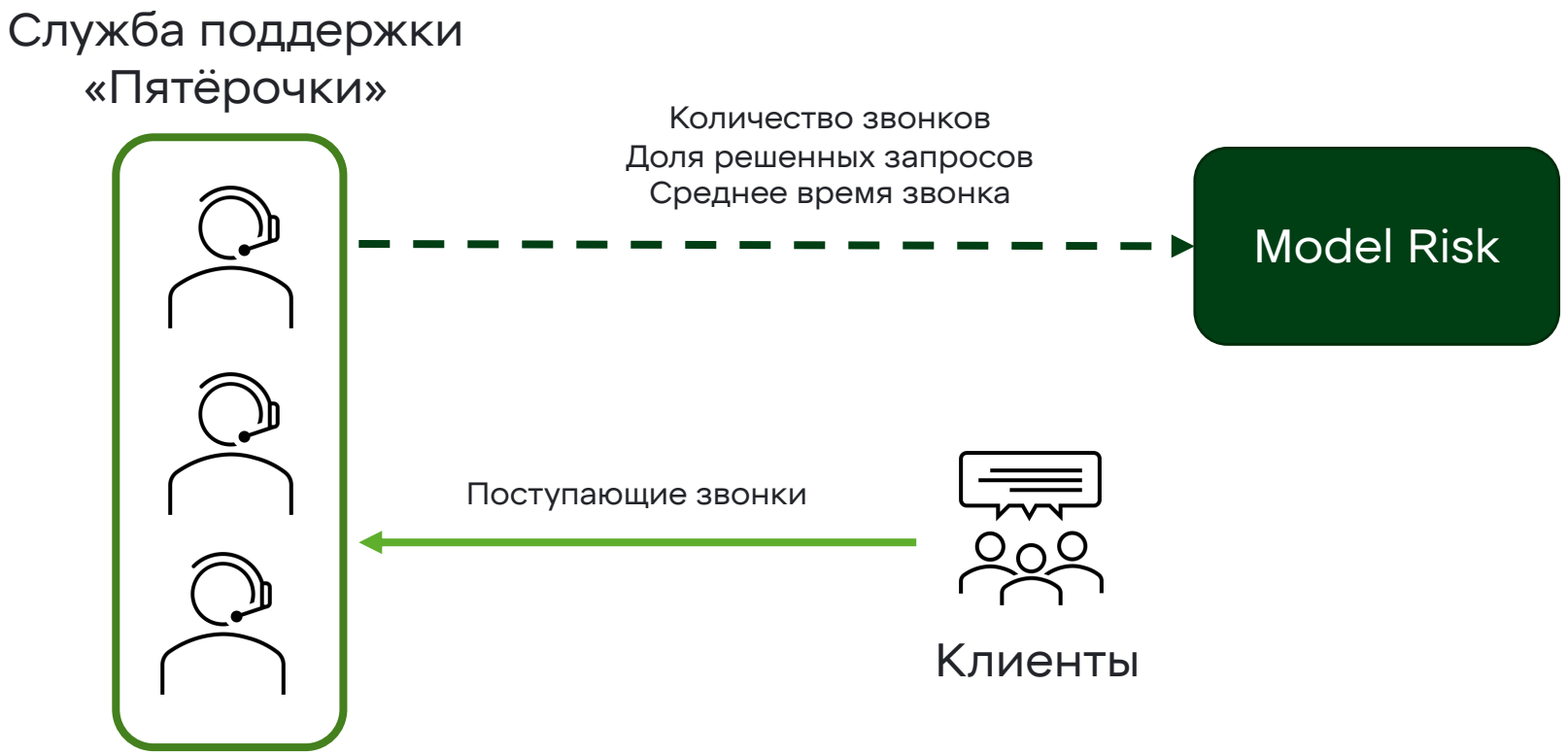


# Пример «сложной модели»

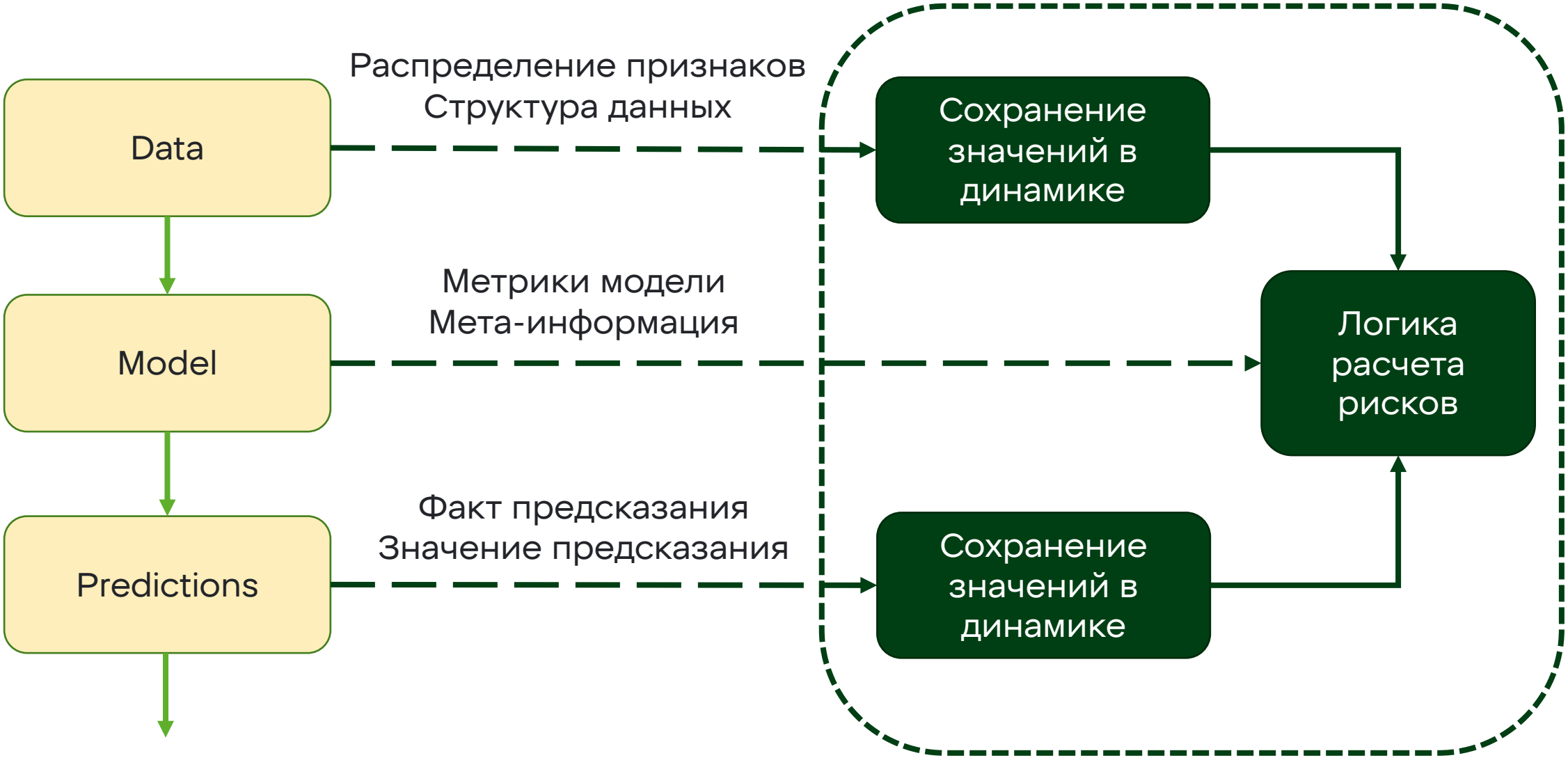


# Модель службы поддержки

Модель в модельном риске не всегда может быть только ML моделью
Как пример нетривиальной модели – служба поддержки магазинов



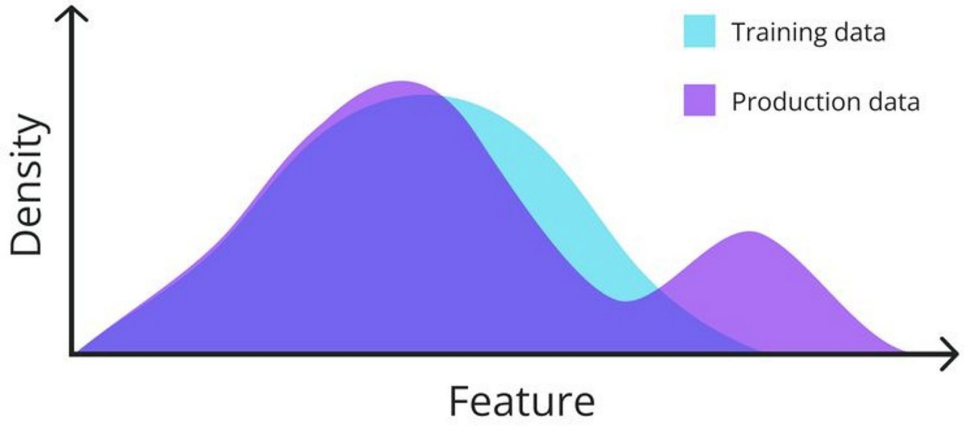
# Что мы знаем про модель?



# Критерий Колмогорова-Смирнова для мониторинга

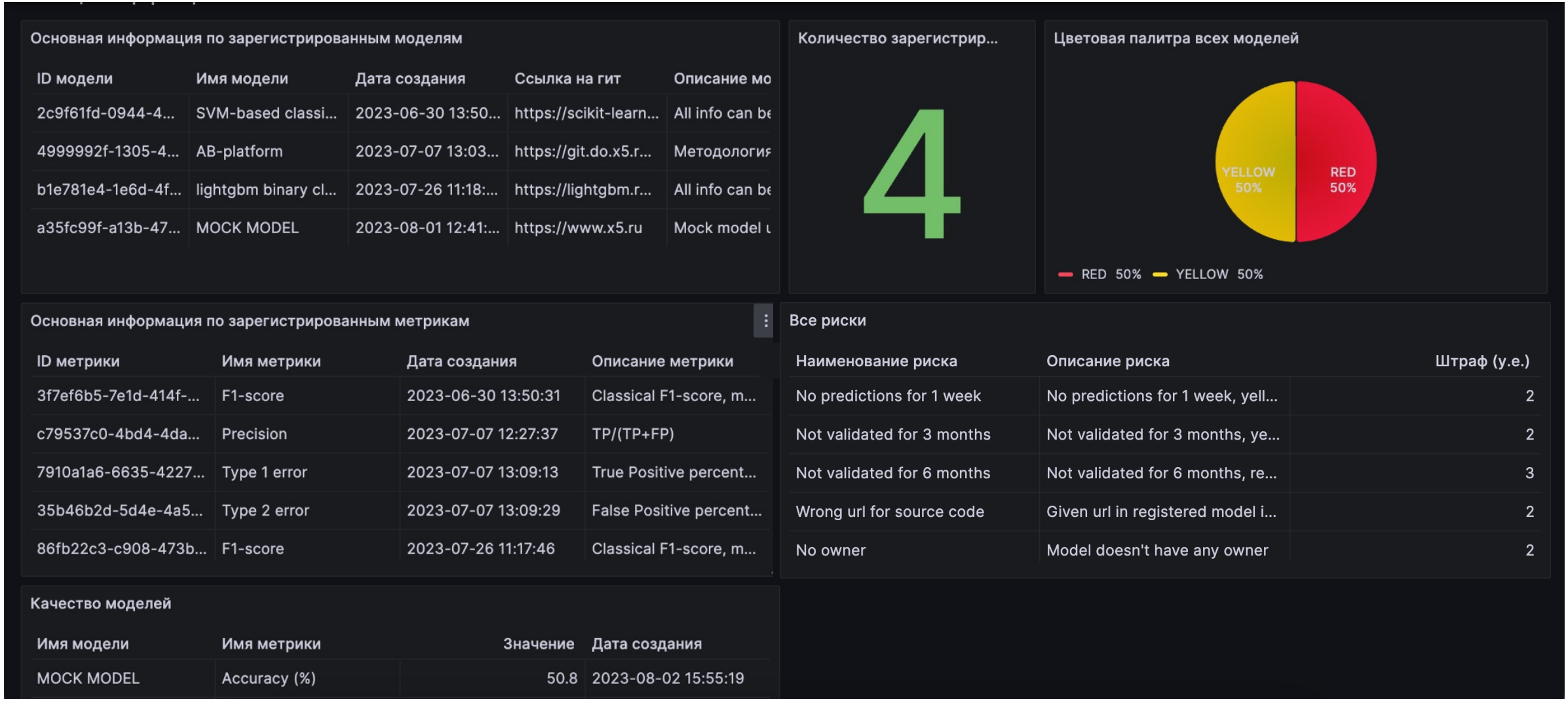
Отслеживаем изменение распределений

- Признаков исходных данных по сравнению с данными с прошлой валидации модели (с поправкой на множественную проверку гипотез)
- Значений предсказаний модели по сравнению с данными с прошлой валидации модели
- Частоты предсказаний модели по времени




$$\lambda' = \sqrt{\frac{n_1 n_2}{n_1 + n_2}} \cdot \max \left| F_{n_1}(x) - F_{n_2}(x) \right|$$

# Пример реестра моделей



Основная информация по зарегистрированным моделям

| ID модели | Имя модели | Дата создания | Ссылка на гит | Описание мо |
|---|---|---|---|---|
| 2c9f61fd-0944-4... | SVM-based classi... | 2023-06-30 13:50... | https://scikit-learn... | All info can be |
| 4999992f-1305-4... | AB-platform | 2023-07-07 13:03... | https://git.do.x5.r... | Методология |
| b1e781e4-1e6d-4f... | lightgbm binary cl... | 2023-07-26 11:18:... | https://lightgbm.r... | All info can be |
| a35fc99f-a13b-47... | MOCK MODEL | 2023-08-01 12:41:... | https://www.x5.ru | Mock model u |





Основная информация по зарегистрированным метрикам

| ID метрики | Имя метрики | Дата создания | Описание метрики |
|---|---|---|---|
| 3f7ef6b5-7e1d-414f-... | F1-score | 2023-06-30 13:50:31 | Classical F1-score, m... |
| c79537c0-4bd4-4da... | Precision | 2023-07-07 12:27:37 | TP/(TP+FP) |
| 7910a1a6-6635-4227... | Type 1 error | 2023-07-07 13:09:13 | True Positive percent... |
| 35b46b2d-5d4e-4a5... | Type 2 error | 2023-07-07 13:09:29 | False Positive percent... |
| 86fb22c3-c908-473b... | F1-score | 2023-07-26 11:17:46 | Classical F1-score, m... |

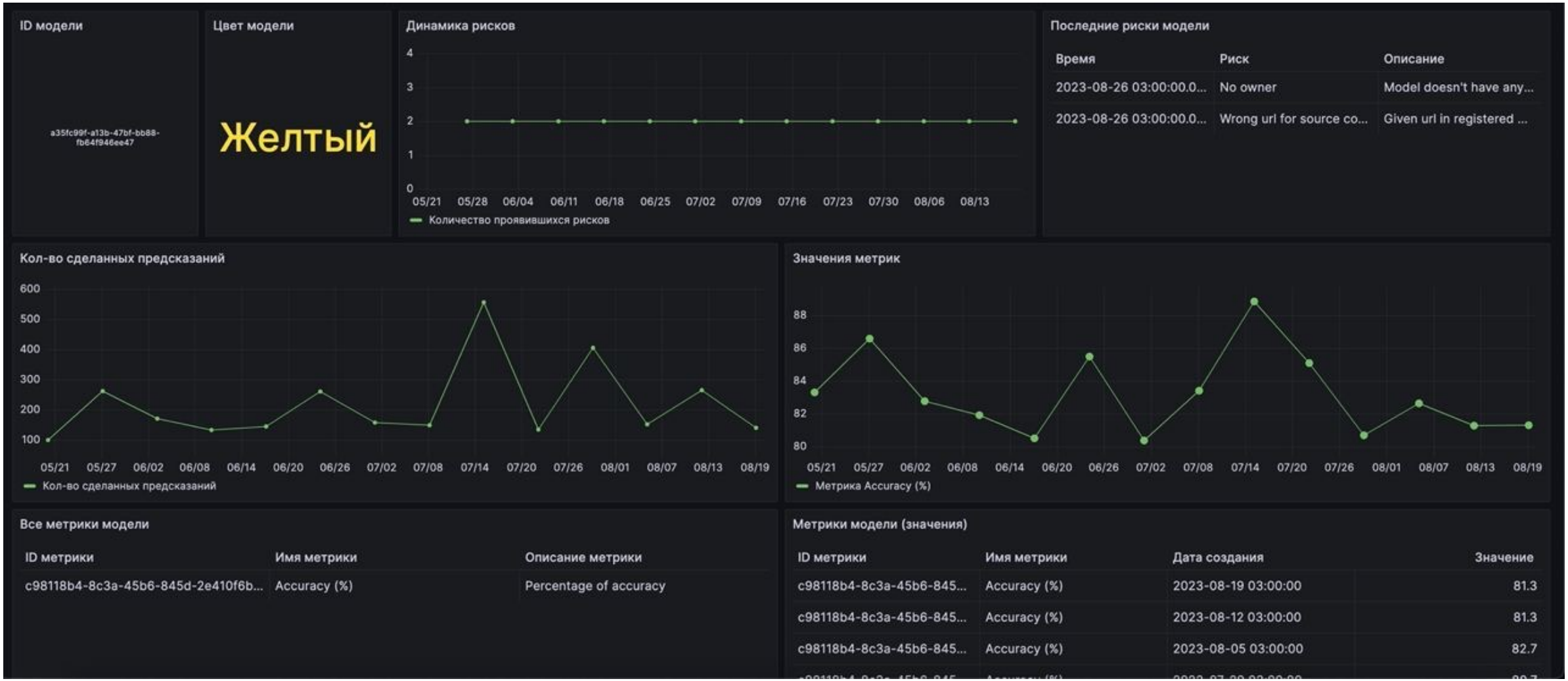
Все риски

| Наименование риска | Описание риска | Штраф (у.е.) |
|---|---|---|
| No predictions for 1 week | No predictions for 1 week, yell... | 2 |
| Not validated for 3 months | Not validated for 3 months, ye... | 2 |
| Not validated for 6 months | Not validated for 6 months, re... | 3 |
| Wrong url for source code | Given url in registered model i... | 2 |
| No owner | Model doesn't have any owner | 2 |

Качество моделей

| Имя модели | Имя метрики | Значение | Дата создания |
|---|---|---|---|
| MOCK MODEL | Accuracy (%) | 50.8 | 2023-08-02 15:55:19 |

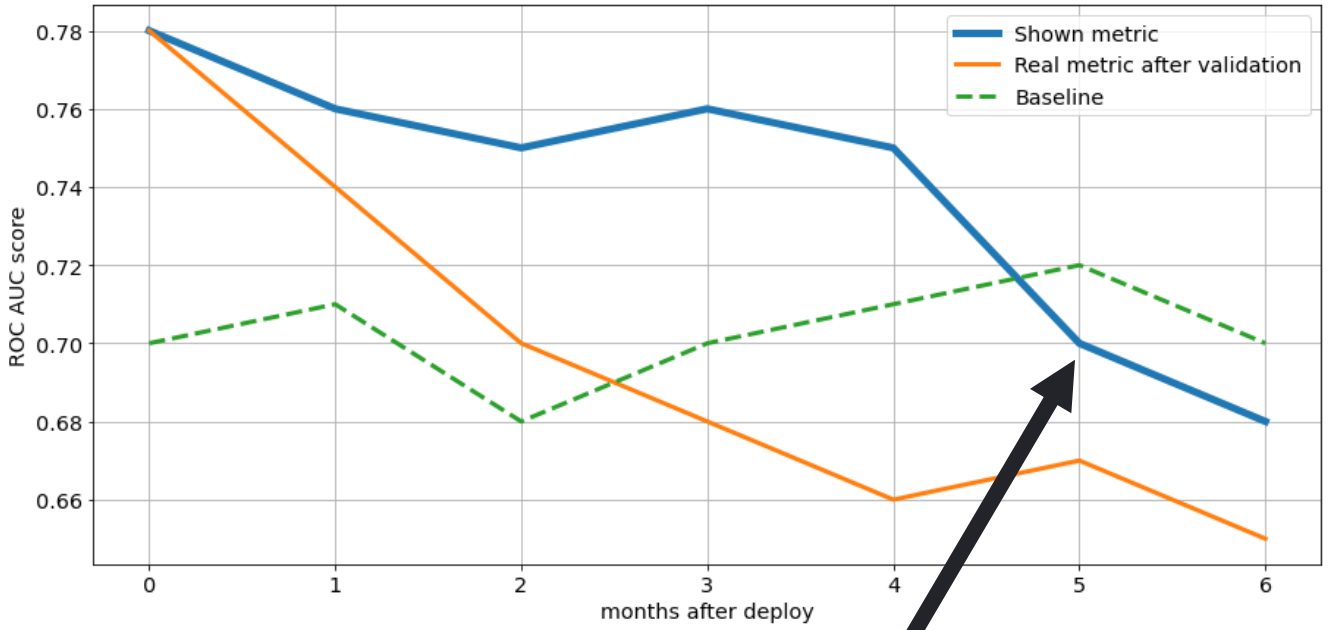
# Пример информации про модель



# Кейс предотвращения убытков

Модель предсказывает вероятность события X в магазине, на основе предсказаний модели строится бизнес-логика нескольких продуктов и работа персонала

- Модель успешно защитилась, и переобучалась раз в 3 мес.
- Модельный риск зафиксировал аномальные изменения в метриках модели спустя 6 мес.
- При проверке оказалось, что бейзлайн-решение превышает метрики модели, были найдены ошибки при валидации модели

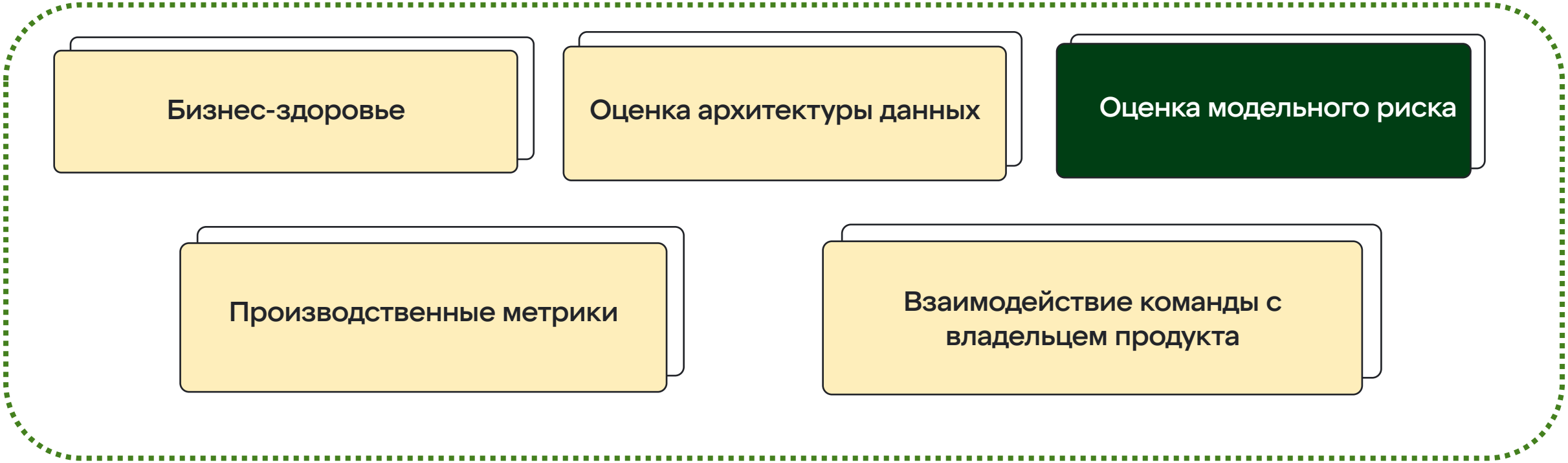



Alert от модельного риска

Ориентировочные предотвращенные убытки: десятки млн рублей в год

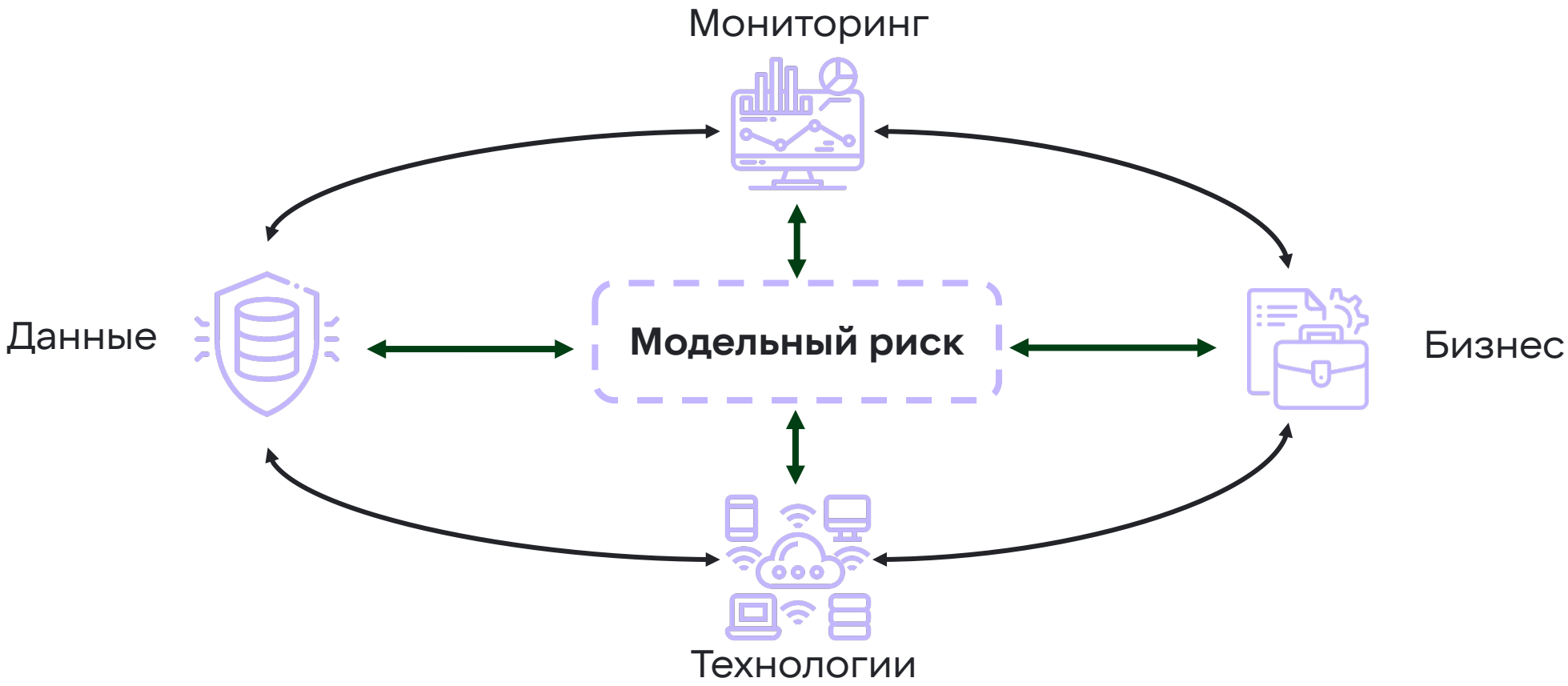
# Модельный риск – часть оценки эффективности продуктов

## Продуктовый градусник




Оценка **количественных показателей** (выполнение плана по метрикам) производится раз в квартал, **качественных** (соответствие критериям) – раз в полгода

# Модельный риск как решение задачи разладки в общем случае



# Что дальше?

- Сравнение моделей с baseline
- Поиск зависимости бизнес-метрик от прокси-метрик модели
- Составление плана по отдельным рискам в зависимости от контекста
- Составление реестра всех ML-моделей в компании

# Что дальше?

- Сравнение моделей с baseline
- Поиск зависимости бизнес-метрик от прокси-метрик модели
- Составление плана по отдельным рискам в зависимости от контекста
- Составление реестра всех ML-моделей в компании

# Что дальше?

Сравнение моделей с baseline

Поиск зависимости бизнес-метрик
от прокси-метрик модели

Составление плана по отдельным рискам
в зависимости от контекста

Составление реестра всех ML-моделей
в компании

# Что дальше?

Сравнение моделей с baseline

Поиск зависимости бизнес-метрик
от прокси-метрик модели

Составление плана по отдельным рискам
в зависимости от контекста

Составление реестра всех ML-моделей
в компании

X5 Tech

# Вопросы?

Александр Сахнов
Head of DA/DS, X5 Tech