

Похожие задачи – разные протоколы

Кяжин Сергей Николаевич, к.ф. – м.н.
Никифорова Лидия Олеговна
ООО «КРИПТО-ПРО»

Мечта

Задача 1

Задача 2

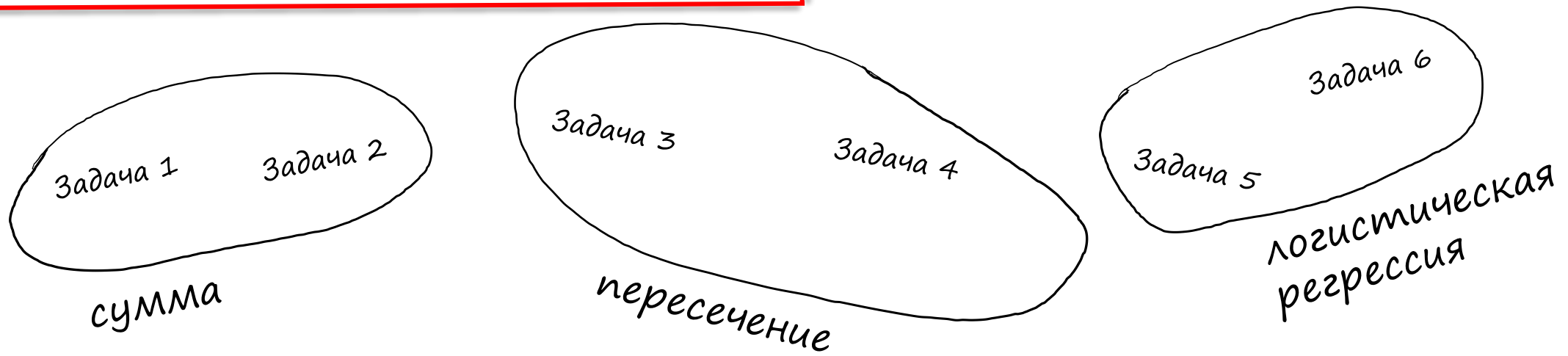
Задача 3

Задача 4

Задача 5

Задача 6

Мечта

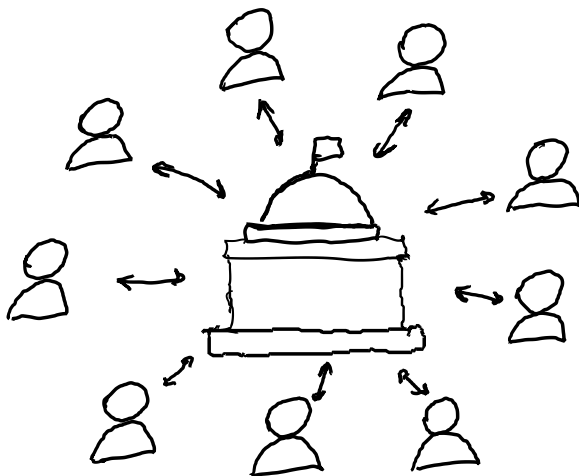


Мечта



Реальность. Задачи

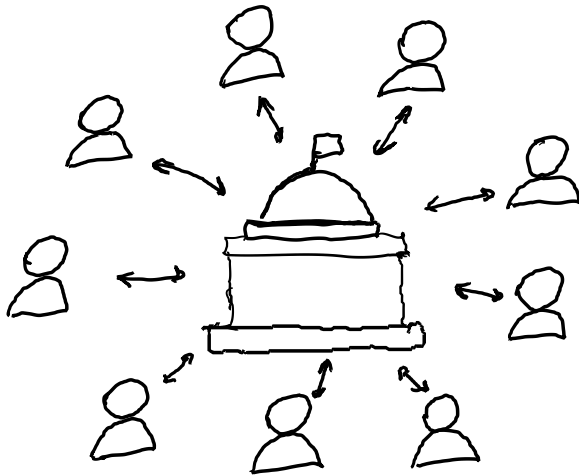
ДЭГ



Задача: посчитать сумму голосов,
сохранив тайну голосования

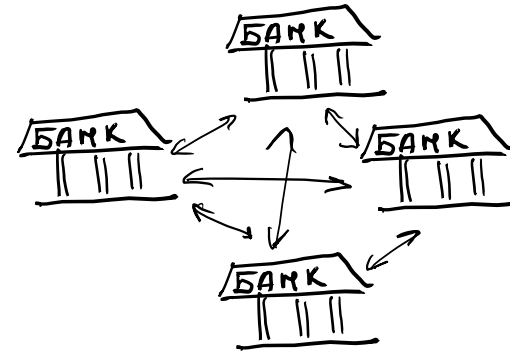
Реальность. Задачи

ДЭГ



Задача: посчитать сумму голосов, сохранив тайну голосования

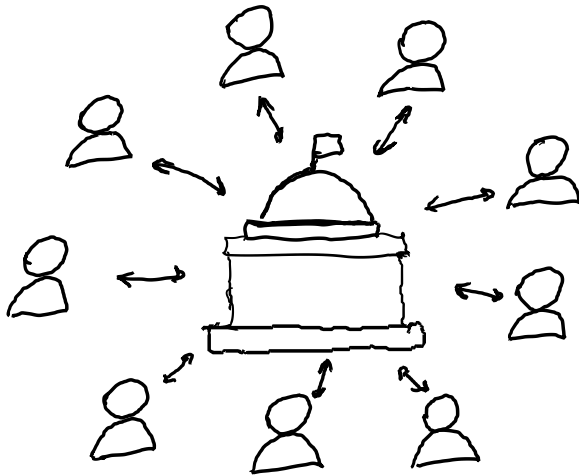
Скоринг



Задача: посчитать сумму средств на счетах клиента в разных банках, сохранив банковскую тайну

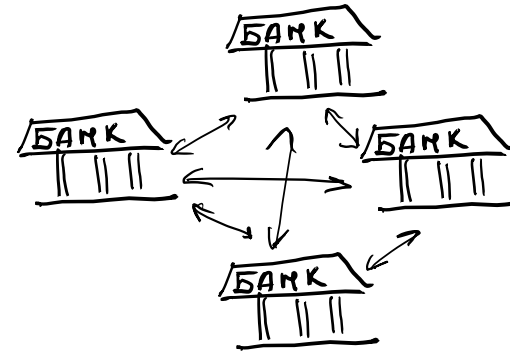
Реальность. Задачи

ДЭГ



Задача: посчитать сумму голосов, сохранив тайну голосования

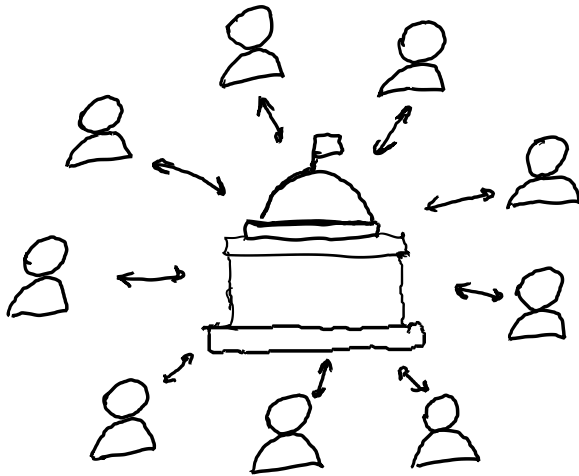
Скоринг



Задача: посчитать сумму средств на счетах клиента в разных банках, сохранив банковскую тайну

Реальность. Задачи

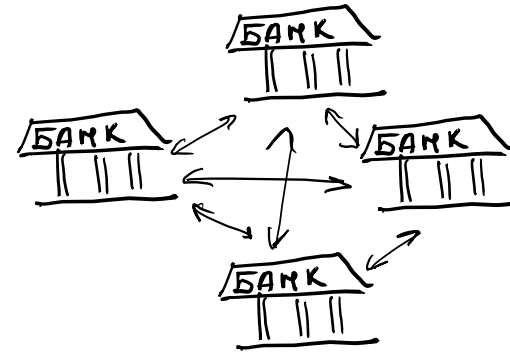
ДЭГ



посчитать сумму,
не раскрывая слагаемые

Задача: посчитать сумму голосов,
сохранив тайну голосования

Скоринг



Задача: посчитать сумму средств на
счетах клиента в разных банках,
сохранив банковскую тайну

Сравнение задач

ДЭГ

посчитать сумму,
не раскрывая слагаемые

Скоринг

Сравнение задач

ДЭГ

Скоринг

посчитать сумму,
не раскрывая слагаемые

ММ

можно участвовать не всем

Сравнение задач

ДЭГ

Скоринг

посчитать сумму,
не раскрывая слагаемые

ММ

можно участвовать не всем

результат может получить
любой участник

ММ

Сравнение задач

ДЭГ

Скоринг

посчитать сумму,
не раскрывая слагаемые

ММ

можно участвовать не всем

результат может получить
любой участник

МММ

может применяться
много раз

ММММ

Сравнение задач

ДЭГ

Скоринг

посчитать сумму,
не раскрывая слагаемые

можно участвовать не всем

результат может получить
любой участник

может применяться
много раз

сильные ограничения
на данные

Сравнение задач

функциональные
требования

другие свойства
безопасности

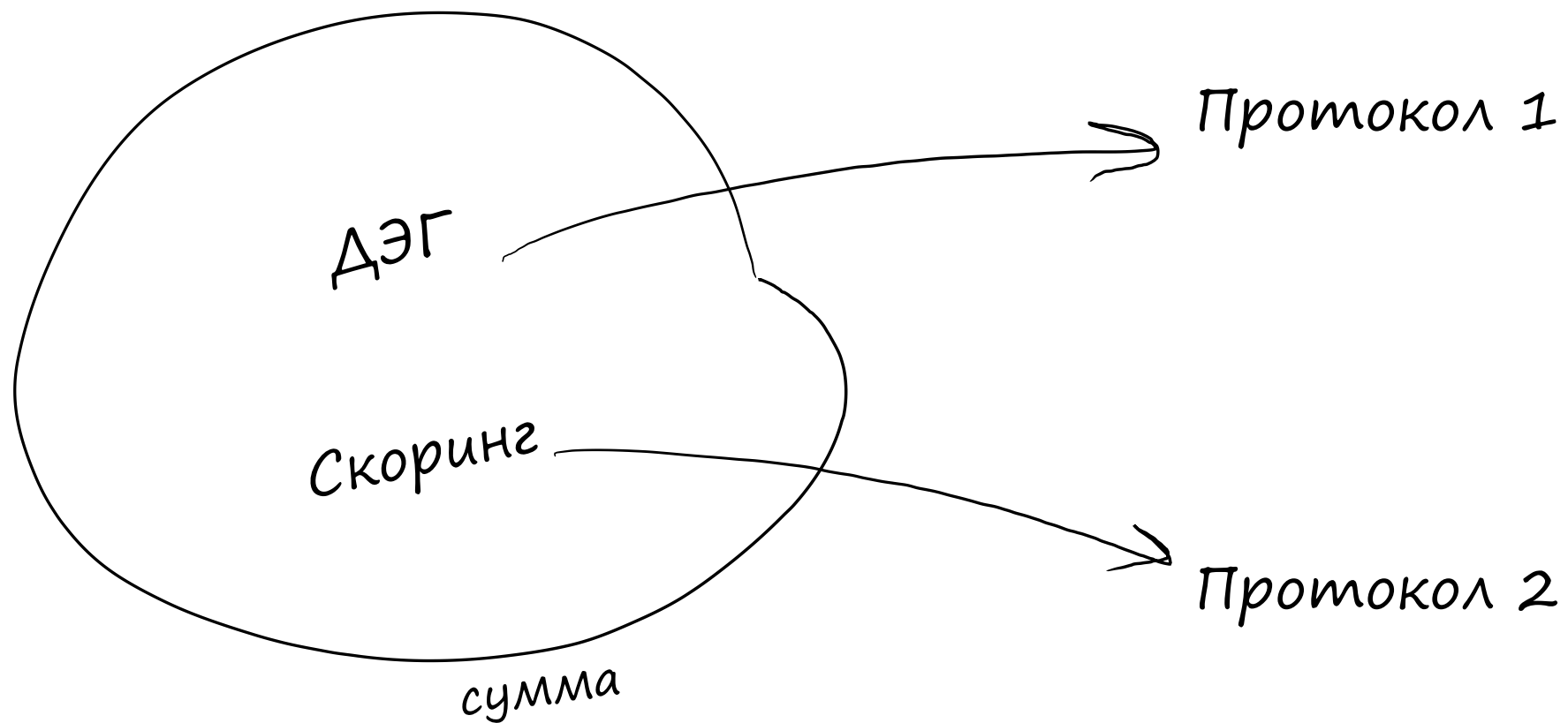
можно участвовать не всем

результат может получить
любой участник

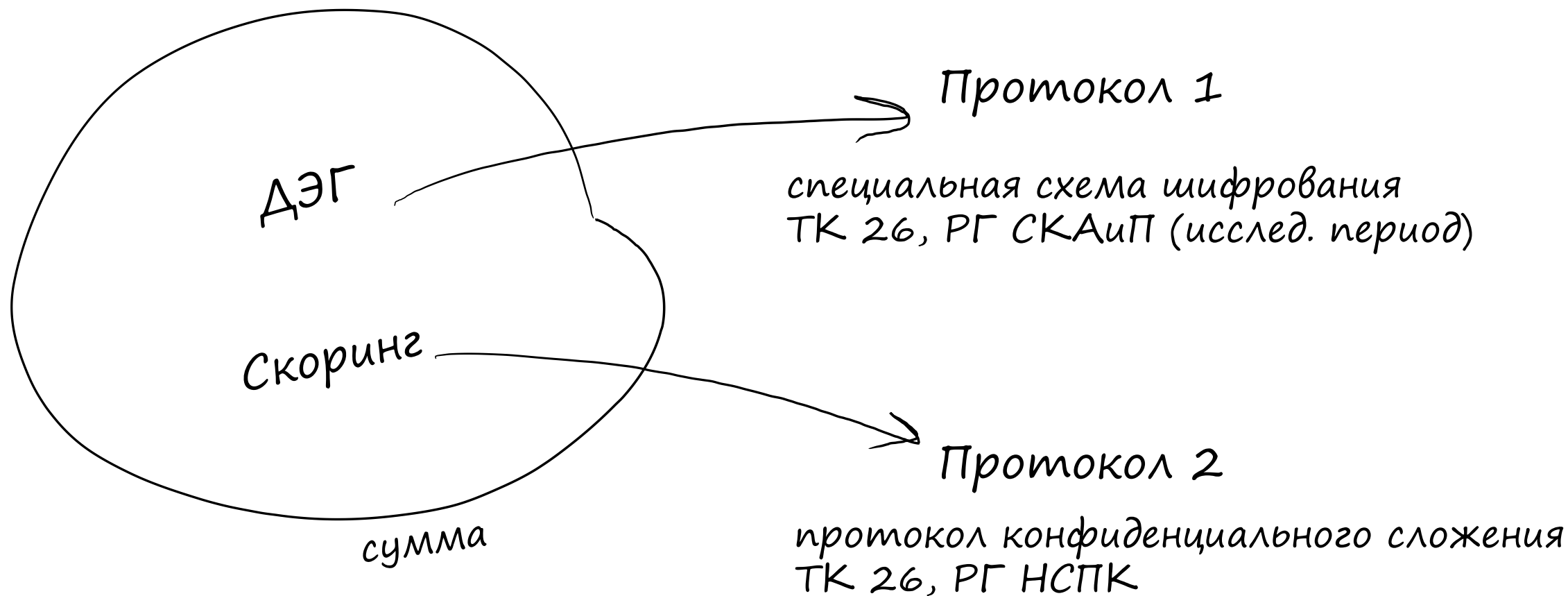
может применяться много
раз

сильные ограничения на
данные

Реальность. Решения

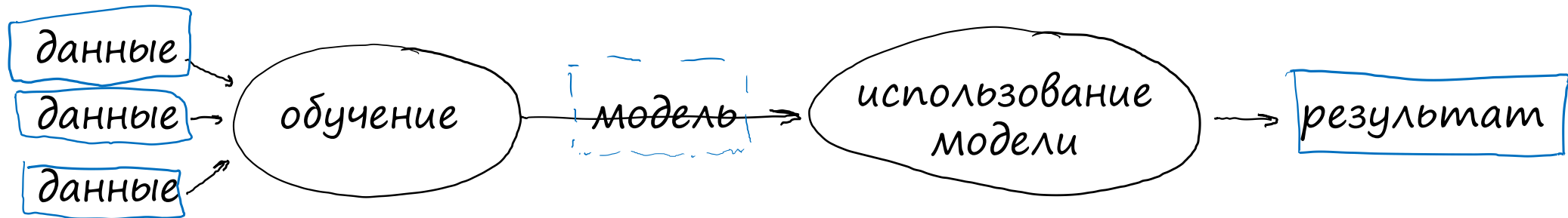


Реальность. Решения



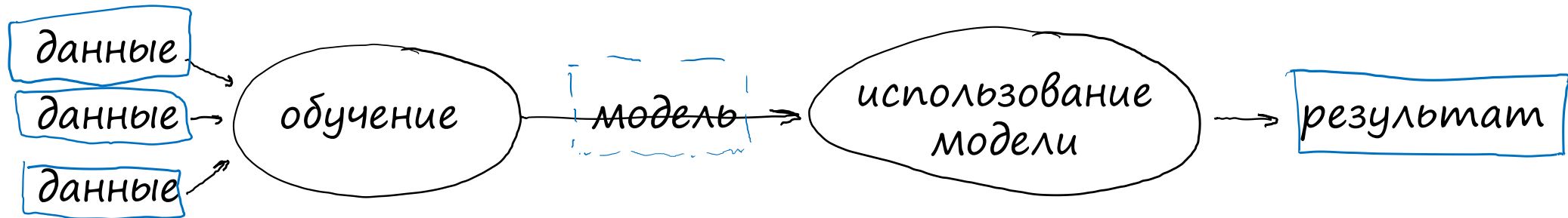
Реальность. Ещё пример

Конфиденциальное машинное обучение



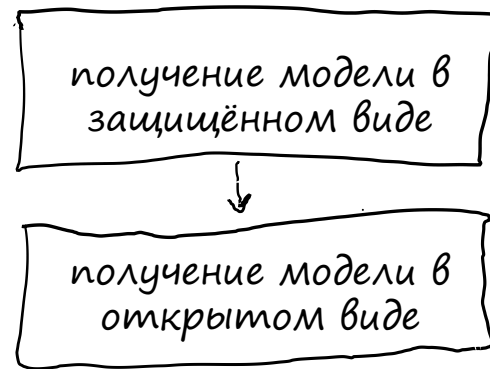
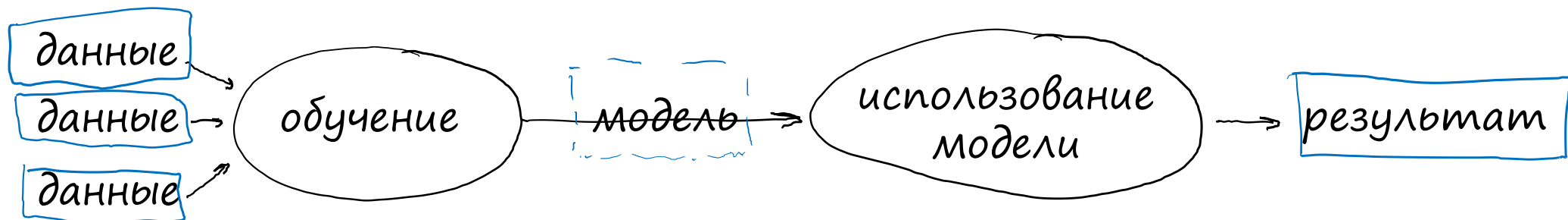
Реальность. Ещё пример

Конфиденциальное машинное обучение



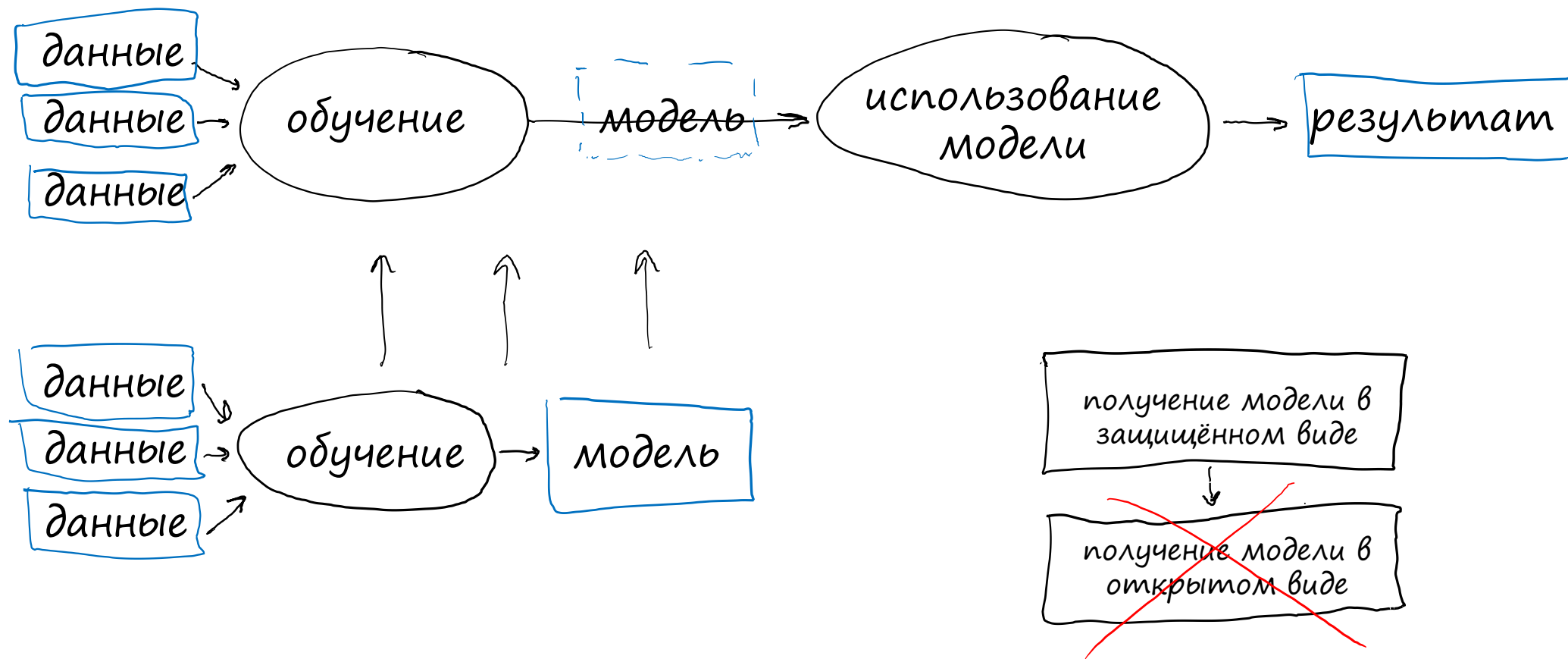
Реальность. Ещё пример

Конфиденциальное машинное обучение



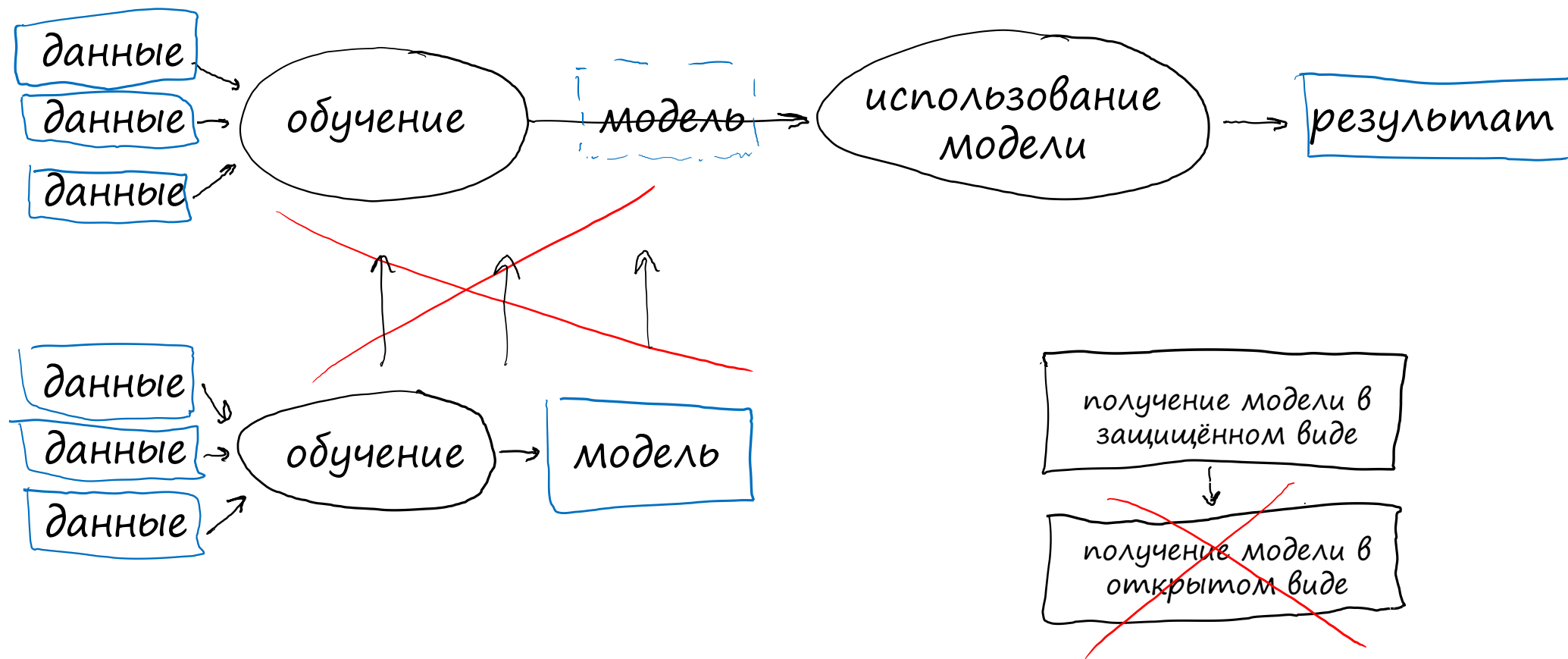
Реальность. Ещё пример

Конфиденциальное машинное обучение



Реальность. Ещё пример

Конфиденциальное машинное обучение





Имеются противопоказания.
Перед применением
проконсультируйтесь с криптографом

