МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

Дипломный проект

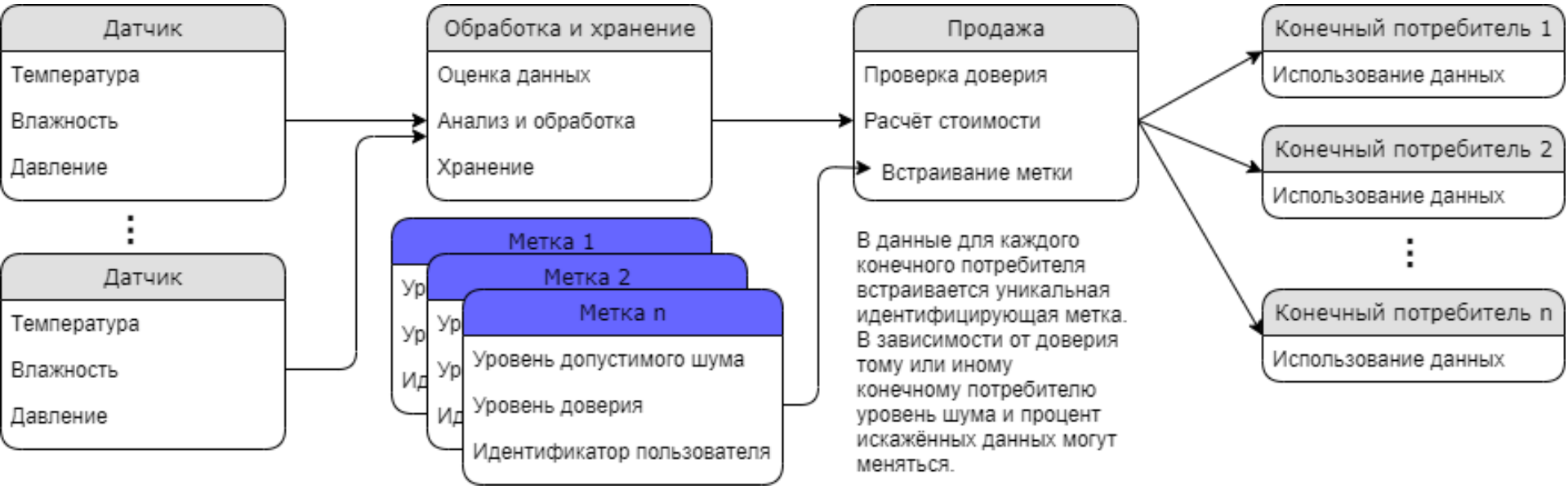
Комплексная система защиты для распределённого сбора данных в системах интернета вещей

Выполнил: Федоров М. В.
гр. 5611

Руководитель:
Пастушок И. А.

Санкт-Петербург
2020

Принципиальная схема



План выступления

- Цели и задачи
- Жизненный цикл
  - Сбор и передача
  - Обработка и хранение
  - Продажа и дальнейшее использование
- Угроза системе
  - Методы атаки
  - Способы противодействия
- Оценка разработанных контрмер

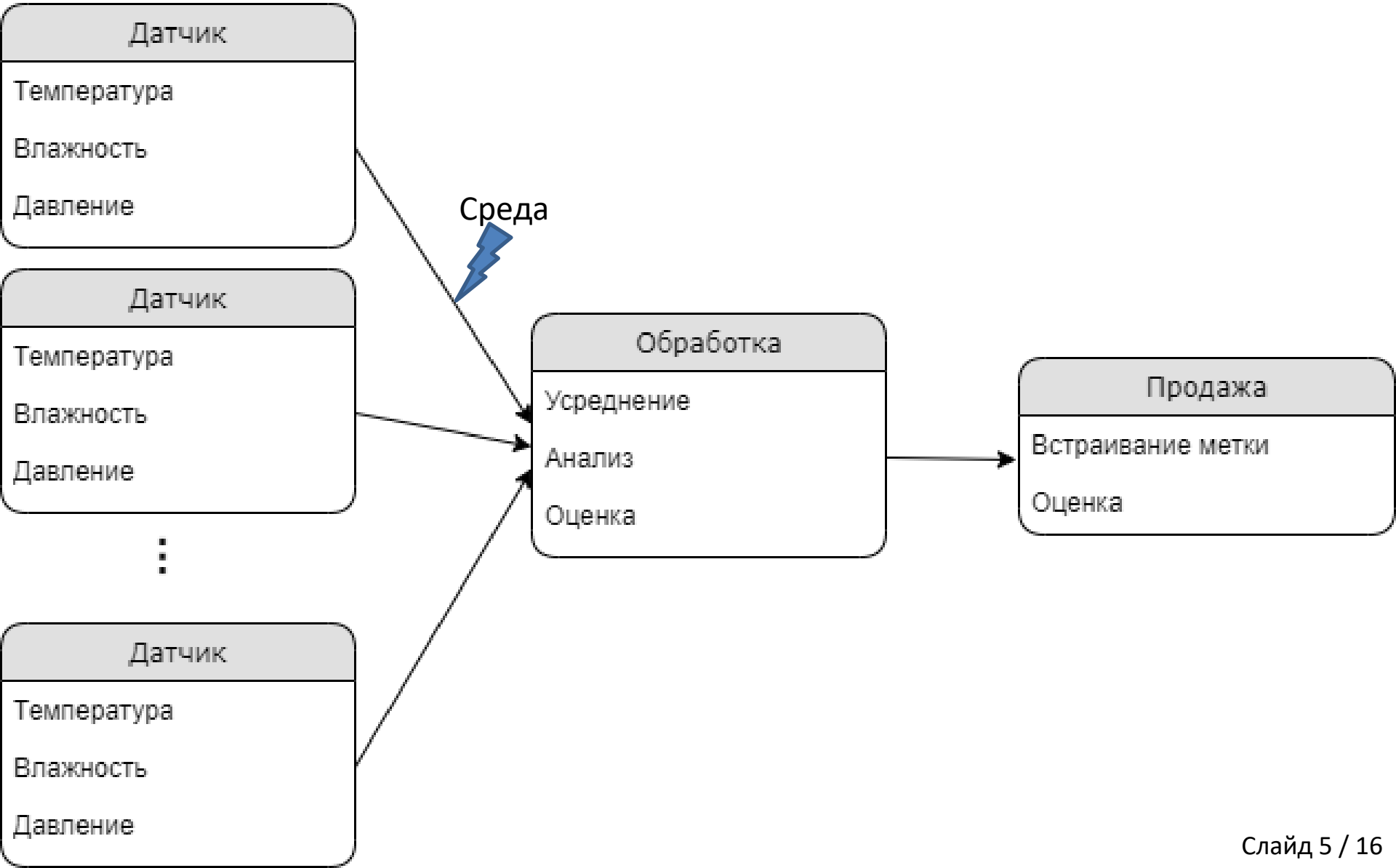
Цель дипломного проекта

Защитить систему сбора и обработки данных от повторной перепродажи данных одним злоумышленником или группой

Решаемые задачи

Обзор литературы по тематике исследования;
Разработка архитектуры программного комплекса;
Имплементация программного обеспечения;
Оценка эффективности разработанного ПО.

Цикл передачи информации



Защита на этапе сбора и передачи

- Помехоустойчивое кодирование
- Защита информации от умышленного искажения
- Алгоритмы, устойчивые к атакам по побочным каналам

Алгоритмы, решающие данные задачи, существуют и широко используются

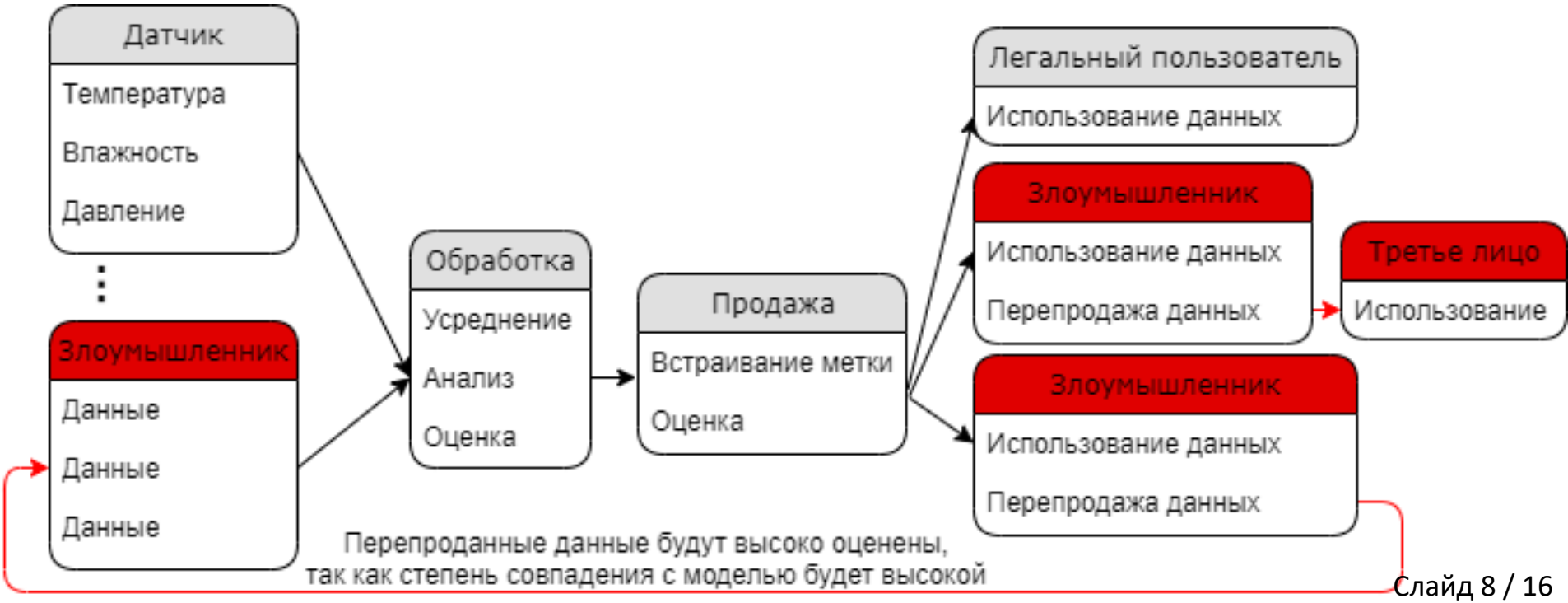
Защита на этапе обработки и хранения

- Распределённые вычисления
- Гомоморфное шифрование

Ввиду текущей неопределённости способов анализа и обработки информации, защита на данном этапе производится организационными мерами

Угрозы после продажи

- Незаконная перепродажа информации третьим лицам
- Перепродажа тех же данных агрегатору



Защита перед продажей

Встраивание меток покупателя в данные

- Метки не искажают данные слишком сильно
- Устойчивы к небольшим изменениям или искажениям, вносимым в данные
- Устойчивы к коалиционным атакам с небольшим числом участников
- Для хранения метки нужен небольшой контейнер
- Алгоритм, уничтожающий метку, слишком сильно искажает данные

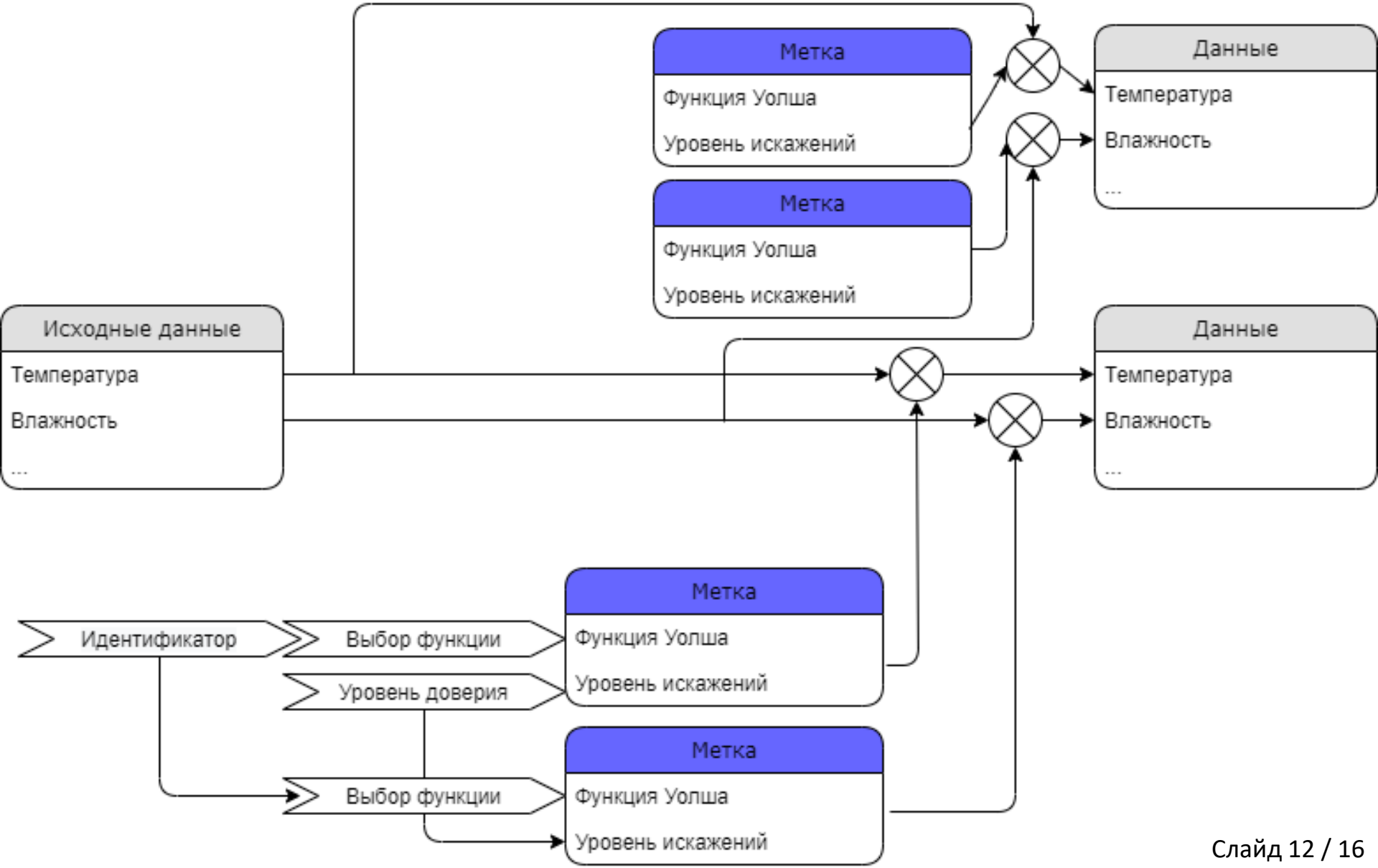
Модель атаки на метку

- Чем больше данные отличаются от исходных, тем ниже будет вознаграждение за продажу этих данных
- Если данные значительным образом систематически отличаются в большую или меньшую сторону, они считаются недостоверными (датчик стоит в тени или на свету; рядом с водоёмом или пыльной дорогой)
- Оптимальное искажение данных – добавление нормально распределённой псевдослучайной величины

Идея защищённой метки

- Требуется встраивание шумоподобного сигнала
  - Не слишком сильно искажает данные
  - Метка не стирается с добавлением шума
- Уничтожение метки происходит только в том случае, если шум, добавленный в данные, настолько сильный, что уничтожает сами данные
- Уровень сигнала метки должен легко регулироваться в зависимости от уровня доверия источнику

Архитектура метки

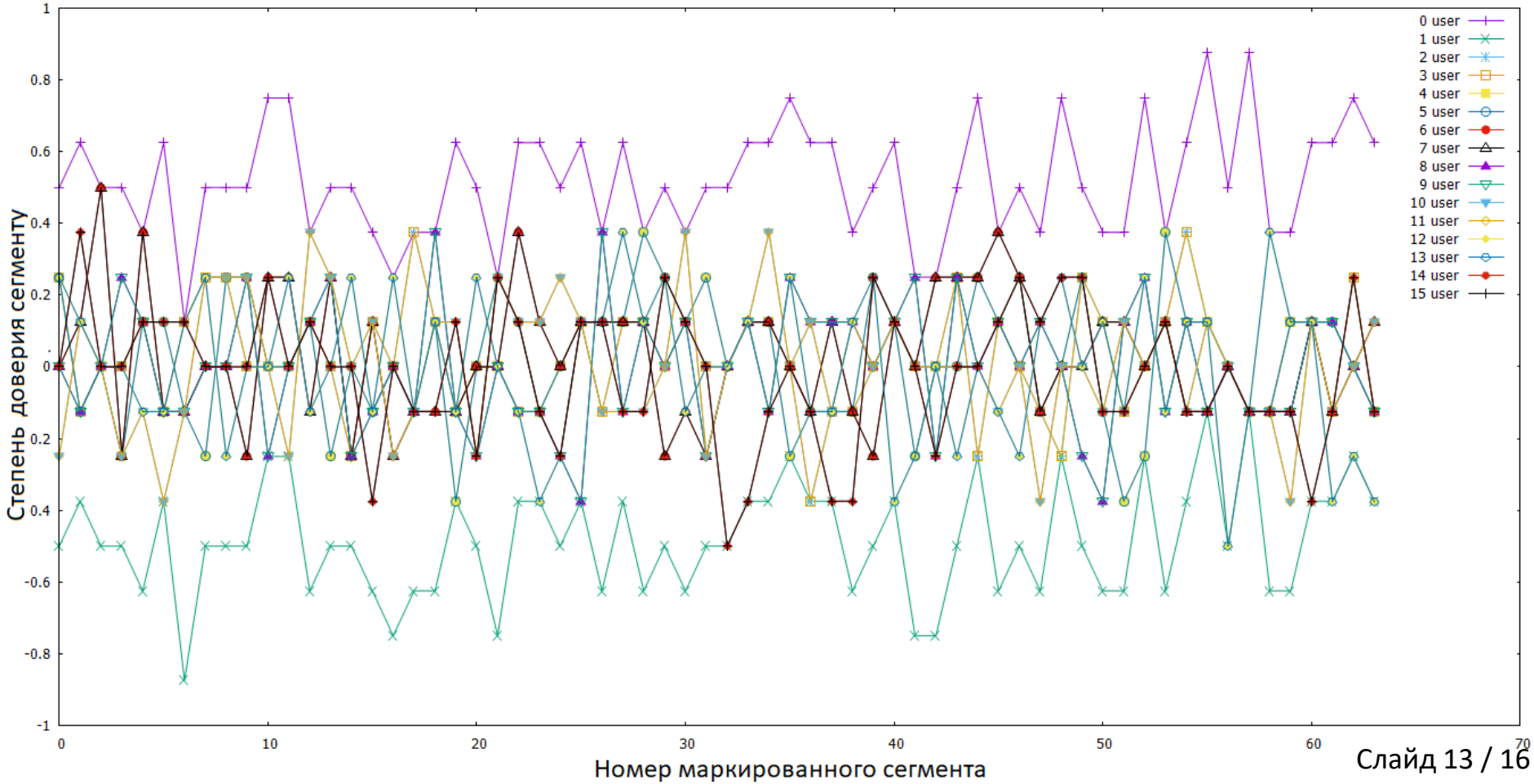


Атака зашумлением данных

Уровень шума превышает сигнал метки в 20 раз.

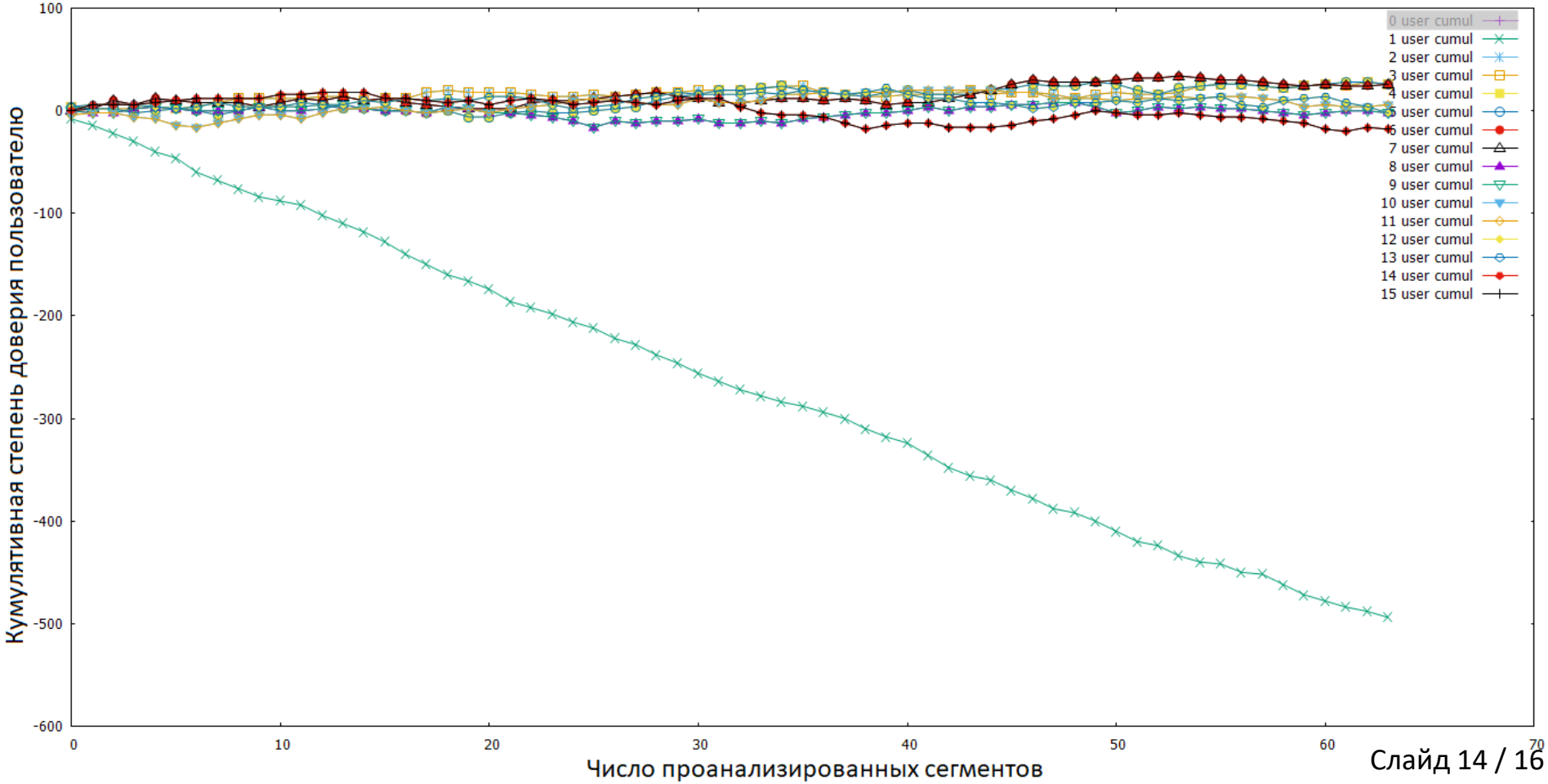
Атакующий определён корректно.

Низкая степень доверия данным атакующего.



Кумулятивная степень доверия

В целях повышения робастности оценивается кумулятивное доверие – это позволяет сохранять метку даже при больших искажениях

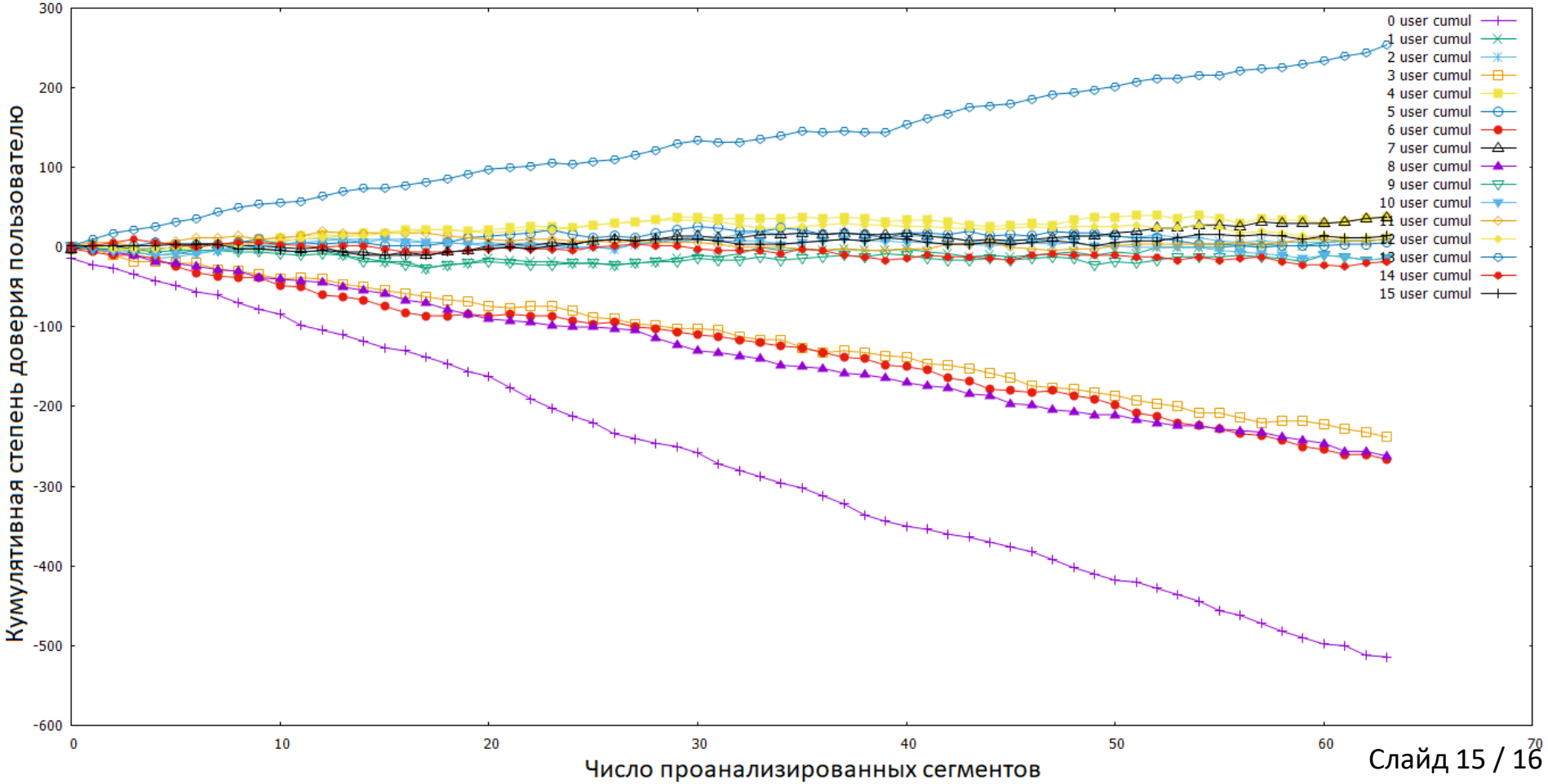


Коалиционные атаки

Пример коалиционной атаки.

Корректно определены все три атакующих.

С течением времени доверие к атакующим снижается.



Результаты

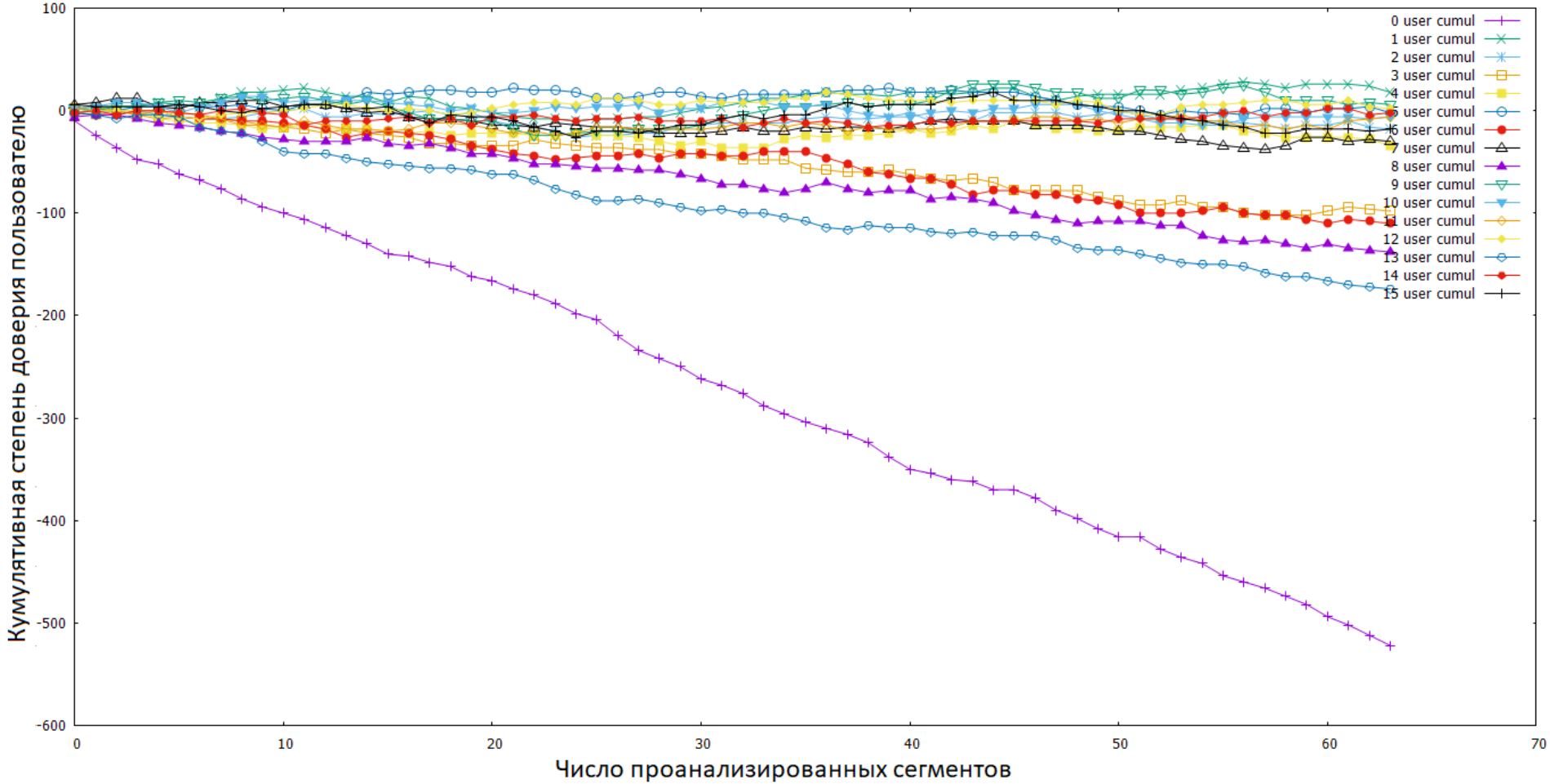
Разработана система защиты от повторной перепродажи со следующими свойствами:

- Некоалиционные атаки без шума определяются за n пакетов, где n – число пользователей.
- Атака зашумлением определяется в среднем за n * NSR помеченных пакетов, где NSR – отношение шума к силе сигнала метки.
- Для коалиционных атак справедливо следующее: PoM = t / (2 ^ ([log2(m)] + 1),

  где t – число помеченных пакетов, PoM – очки недоверия, m – число атакующих, [] – округление вниз.

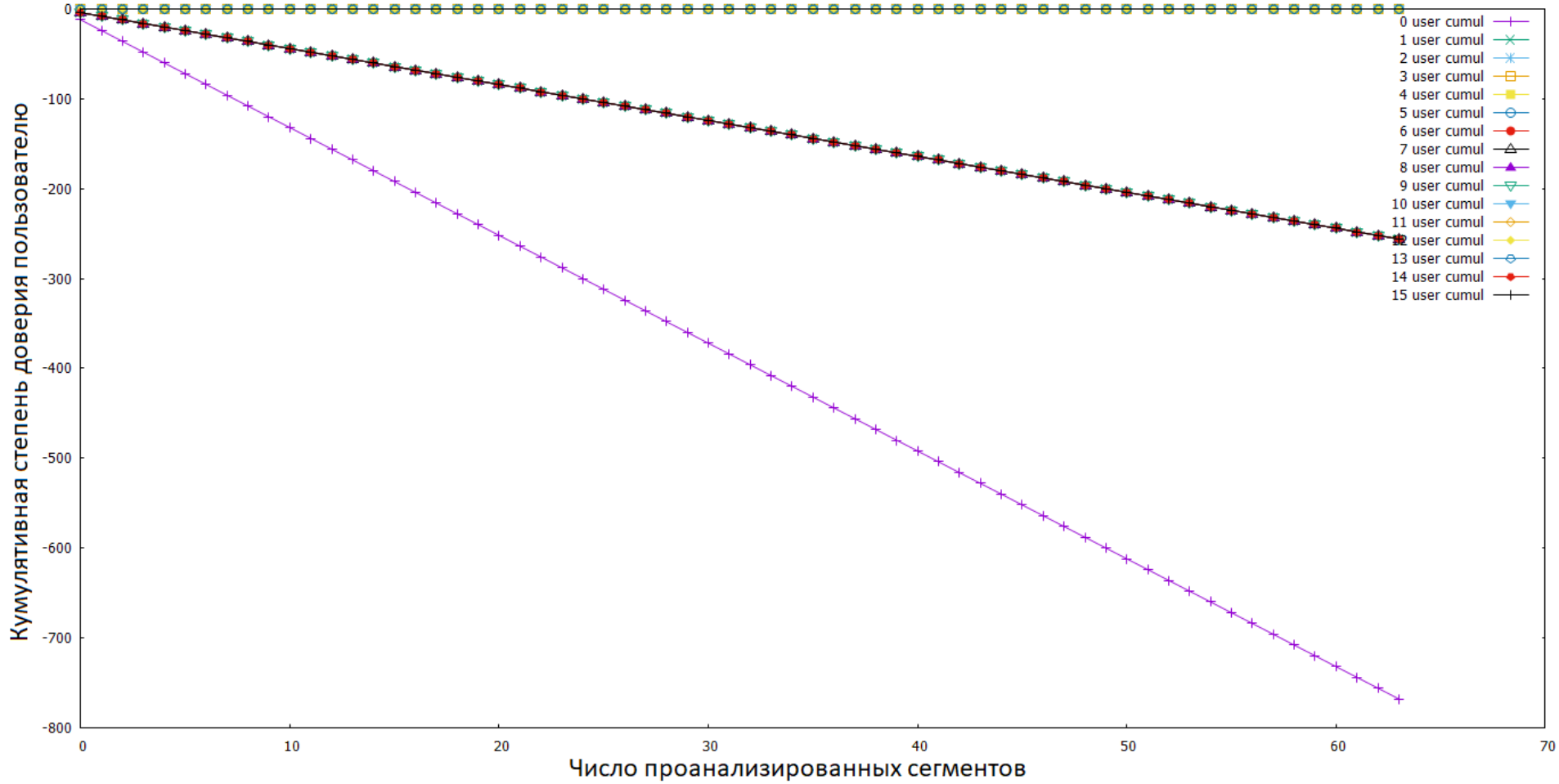
Атака выбором злоумышленников

- При добавлении в коалицию пользователя с высоким рейтингом доверия требуется гораздо больше пакетов для определения участников коалиции



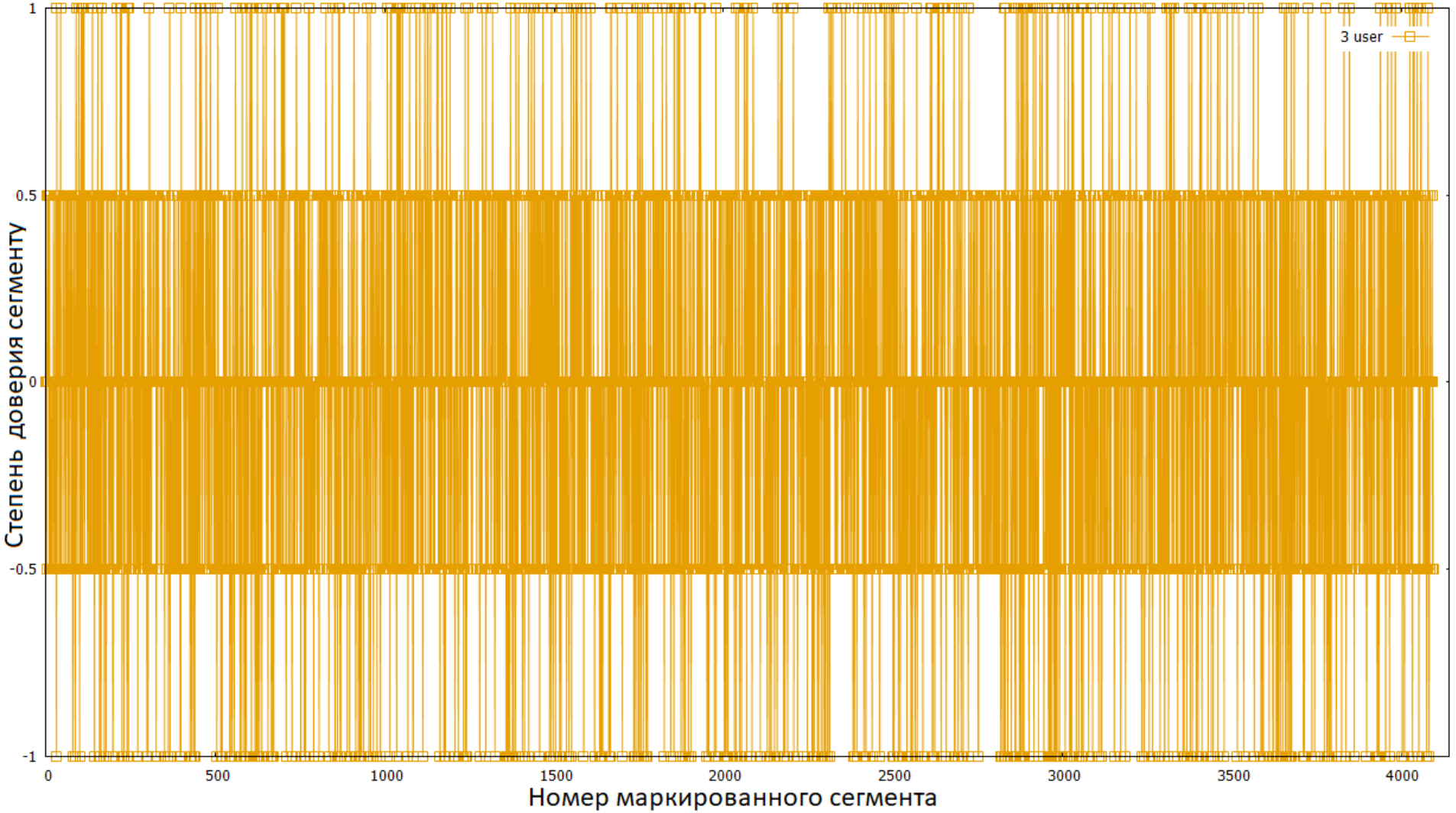
Атака выбором злоумышленников

- С использованием специальных данных можно добиться ложного обвинения, но не ложного принятия данных



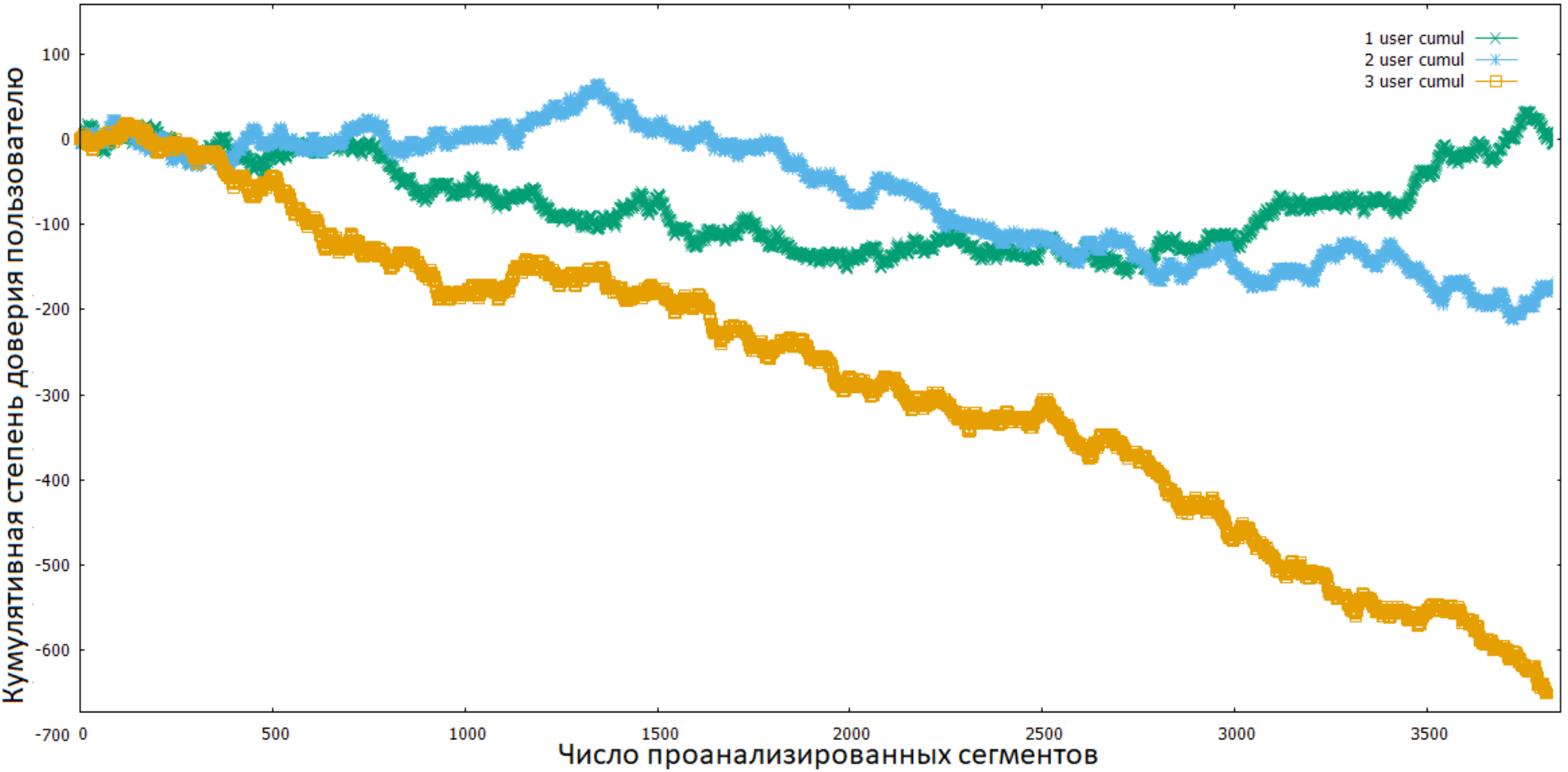
Сверхвысокий уровень шума

- Шум, уничтожающий данные, не уничтожает метку.



Сверхвысокий уровень шума

- При анализе достаточно большого числа сегментов единичный злоумышленник всё равно будет обнаружен



Формулы

Разработанные системы оценки:

Моментальное доверие (доверие пакету):

$$МДКП_u[i] = sig(u[i] - o[i]) * sig(wal_u[i])$$

Нормальное доверие (доверие сегменту):

$$НДКП_u[j] = \left(\sum_{i=j*L}^{(j+1)*L-1} МДКП_u[i] \right) / L$$

Кумулятивное доверие (доверие пользователю):

$$КДКП_u[q] = \sum_{j=0}^{q} НДКП_u[j]$$