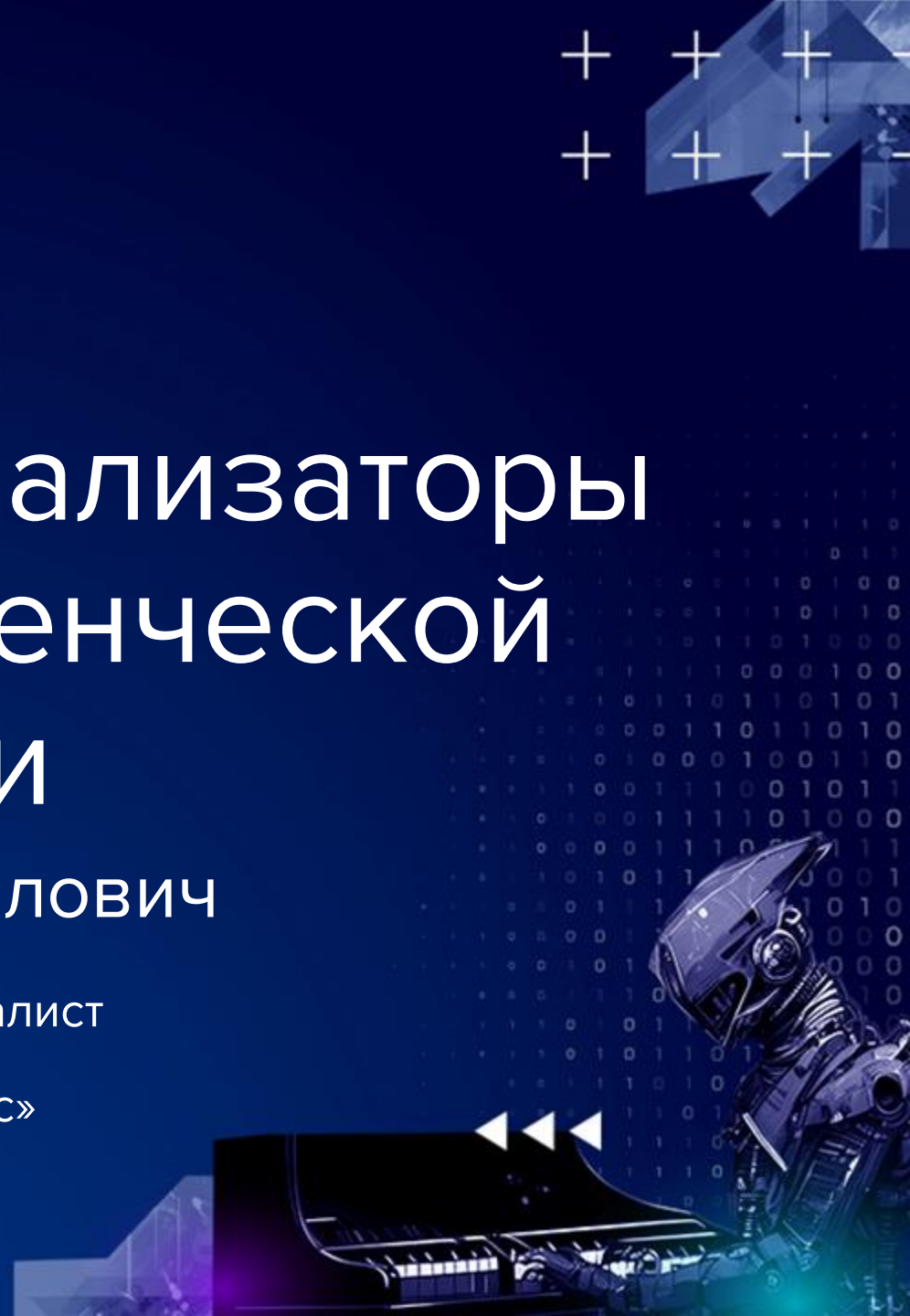
GIS DAYS

Топологические анализаторы в системах поведенческой аналитики

Чатоян Сергей Камалович

к.т.н., с.н.с., главный специалист

ООО «Газинформсервис»

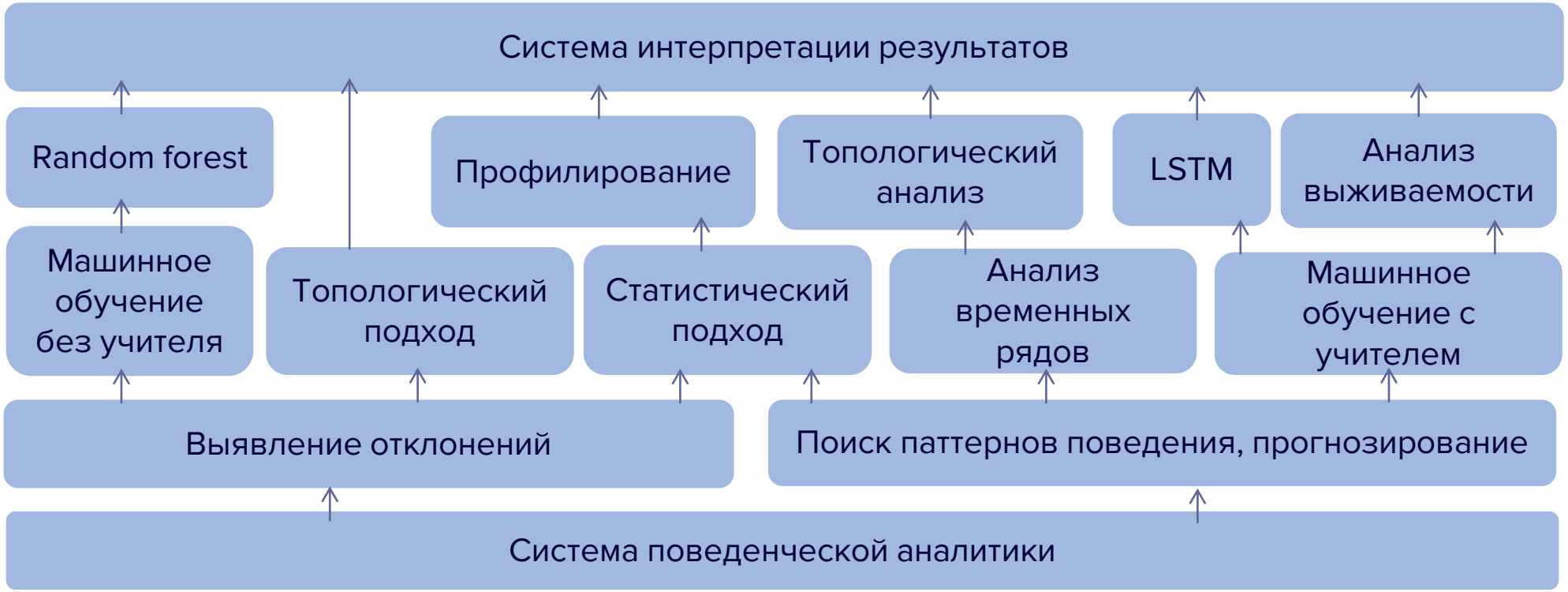


GIS DAYS

GIS ГАЗИНФОРМ СЕРВИС

Системы поведенческой аналитики

Системы анализа поведения пользователей и сущностей — решения, направленные на выявление и классификацию паттернов в поведении пользователей и различных систем.



Направления использования систем поведенческой аналитики

1. Кибербезопасность: детектирование боковых атак и атак на учетные записи
2. Эксплуатация программно-технических систем: прогнозирование и диагностика отказов/ошибок
3. Организационное управление: анализ производительности и информационных коммуникаций людей и команд
4. Антифрод

Системы поведенческой аналитики предоставляют полезную информацию во все большем разнообразии вариантов использования. Развитие AI/ML быстро расширяет их способность извлекать смысл из данных, разбросанных по времени, географии и системам.

Роль топологических анализаторов в данных системах

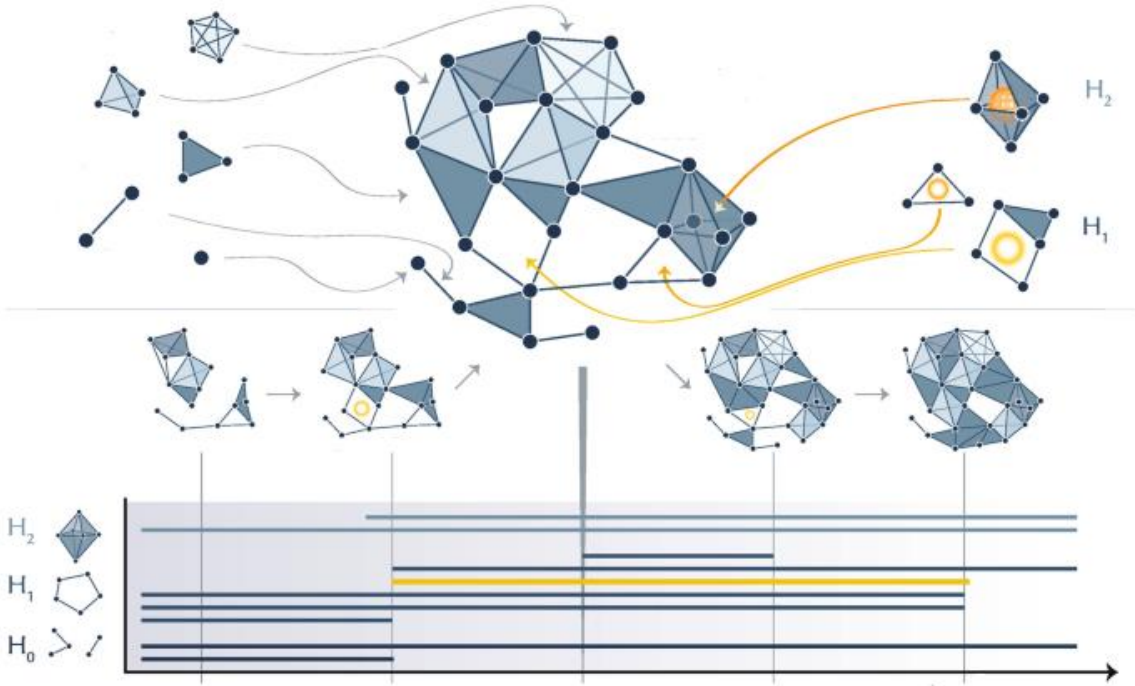
Обнаружение необычных паттернов в поведении пользователей и сущностей

Анализ сложных, зашумленных, многомерных данных с пропусками

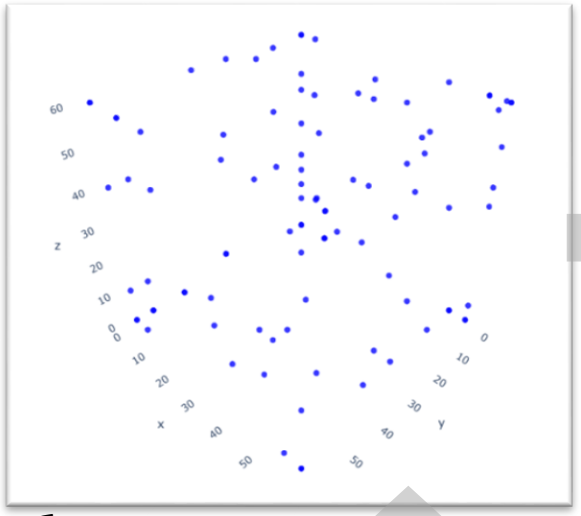
Глубокое понимание взаимодействий между пользователями и сущностями

Топологический анализ данных

Топологический анализ данных - новое направление в науке о данных, целью которого является раскрытие, понимание и использование топологической и геометрической структуры, содержащейся в данных.

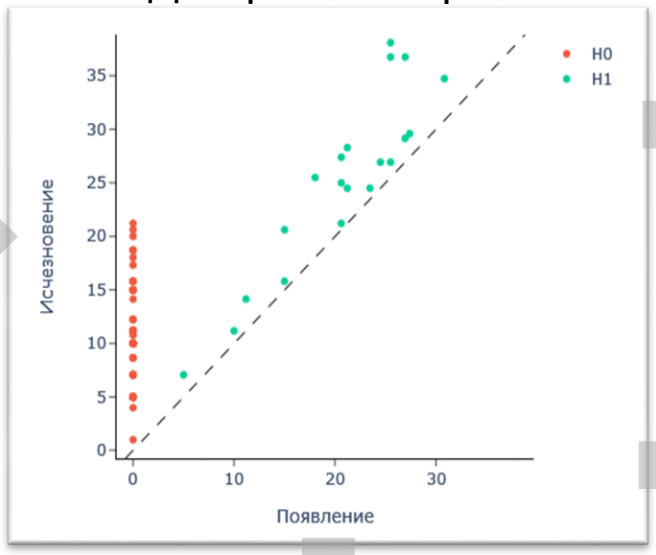


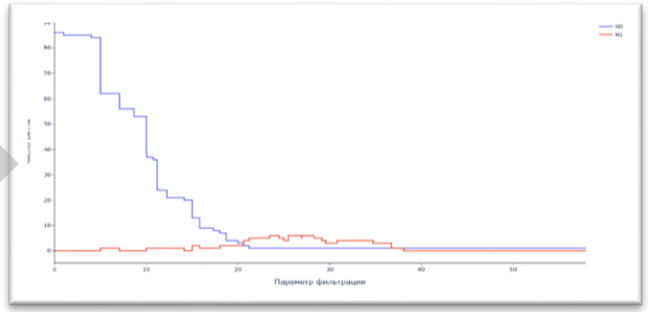
Основные понятия и принципы работы топологического анализа данных



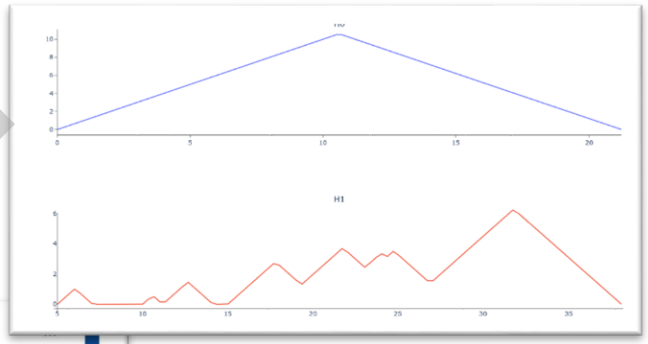
Облако точек

Диаграмма персистентности

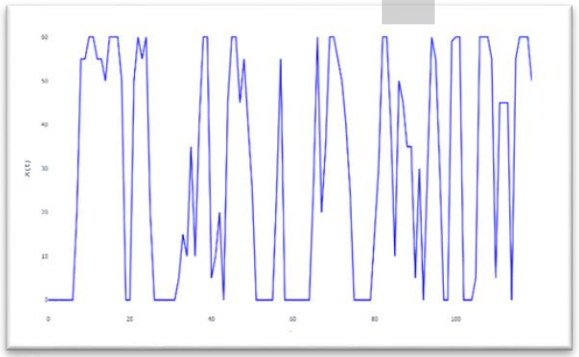




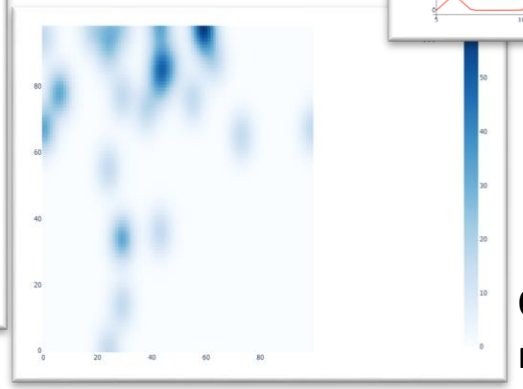
Кривые Бетти



Ландшафты персистентности



Временной ряд



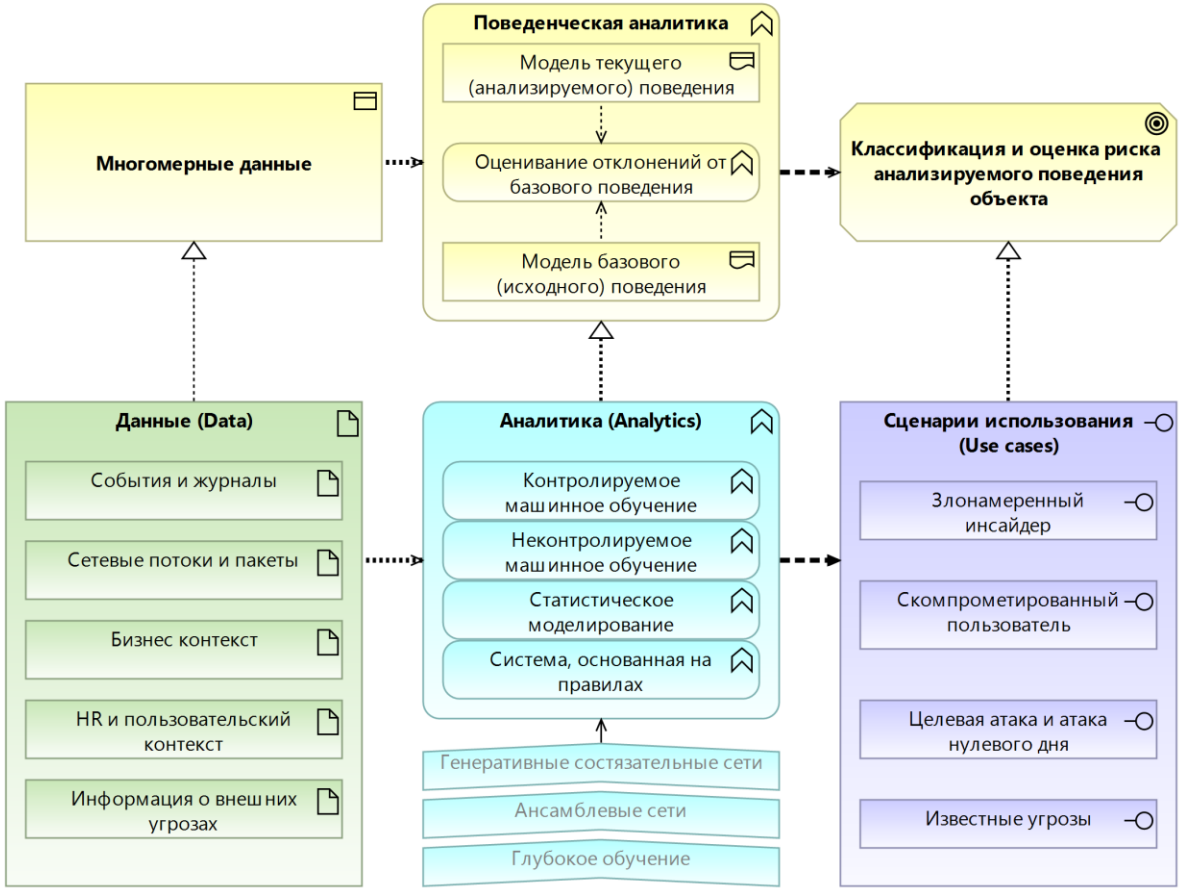
Образы персистентности

Применение топологических анализаторов в системах поведенческой аналитики

Анализ пользовательского поведения
Обнаружение аномалий и необычных паттернов
Анализ больших объемов данных из разных источников

Визуализация
Сводная информация
Дашборды, KPI, граф
Лента событий
сущностей

Применение топологических анализаторов в системах поведенческой аналитики



Применение топологических анализаторов в системах поведенческой аналитики

Результаты анализа | Детализация по датам

ФИО	Неделя	Параметр	Оценка риска	Обобщенная оценка риска	Подразделение	Режим	Тип профиля	Отклонение среднее	Отклонение суммарное
[redacted]	2023-04-03-2023-04-07	Активное время	Низкая	Средняя	ГИС-СТД-ДСИ-ОСУДиИД-Г4ПиВвД	Работает	Работа	Вверх	Вверх
[redacted]	2023-04-03-2023-04-07	Возможный вред	Низкая	Средняя	ГИС-СТД-ДСИ-ОСУДиИД-Г4ПиВвД	Работает	Работа	Нет	Нет
[redacted]	2023-04-03-2023-04-07	Время в интернете	Высокая	Средняя	ГИС-СТД-ДСИ-ОСУДиИД-Г4ПиВвД	Работает	Работа	Вверх	Вверх
[redacted]	2023-04-03-2023-04-07	Время в программах	Высокая	Средняя	ГИС-СТД-ДСИ-ОСУДиИД-Г4ПиВвД	Работает	Работа	Вверх	Вверх
[redacted]	2023-04-03-2023-04-07	Время на работе	Низкая	Средняя	ГИС-СТД-ДСИ-ОСУДиИД-Г4ПиВвД	Работает	Работа	Вверх	Вверх
[redacted]	2023-04-03-2023-04-07	Высокоприор... события	Низкая	Средняя	ГИС-СТД-ДСИ-ОСУДиИД-Г4ПиВвД	Работает	Работа	Нет	Нет
[redacted]	2023-04-03-2023-04-07	Набрано текста	Средняя	Средняя	ГИС-СТД-ДСИ-ОСУДиИД-Г4ПиВвД	Работает	Работа	Вниз	Вниз
[redacted]	2023-04-03-2023-04-07	Напечатано страниц	Низкая	Средняя	ГИС-СТД-ДСИ-ОСУДиИД-Г4ПиВвД	Работает	Работа	Нет	Нет
[redacted]	2023-04-03-2023-04-07	Низкоприорит... события	Средняя	Средняя	ГИС-СТД-ДСИ-ОСУДиИД-Г4ПиВвД	Работает	Работа	Вверх	Вверх

Параметр	Оценка активности	Оценка риска
Время на работе	0.870343	Низкая
Активное время	0.017111	Высокая
Время в программах	0.024848	Высокая
Время в интернете	0.024848	Высокая
Прочее	0.434587	Средняя
Социальные сети	0.291040	Высокая
СМИ и развлечения	0.291543	Высокая
Поиск работы	0.997108	Низкая
Возможный вред	0.998851	Низкая
Рабочие	0.007238	Высокая
Набрано текста	0.007143	Высокая
Письма e-mail	0.012412	Высокая
Чаты/звонки	0.184377	Высокая
Напечатано страниц	0.529228	Средняя
Отправлено + выведено файлов	0.288885	Высокая
Высокоприоритетные события	0.767963	Низкая
Низкоприоритетные события	0.291605	Высокая
Объем вх. писем, Кб	0.007242	Высокая
Писем вх., шт	0.898925	Низкая
Объем исх. писем, Кб	0.007242	Высокая

Преимущества использования топологических анализаторов

Одним из главных преимуществ использующихся методов топологического анализа является их способность выявлять скрытые и сложные структуры в данных, которые могут быть упущены другими методами.

Топологический анализ позволяет работать с данными различной природы, включая числовые, категориальные и графовые данные.

Ограничения и возможные проблемы при применении топологического анализа

Требуется хорошее понимание предметной области и особенностей данных

Подбор правильной метрики и установка параметров

Вычислительная сложность

GIS DAYS

СПАСИБО ЗА ВНИМАНИЕ

Контакты
www.gaz-is.ru
sale@gaz-is.ru

GIS
ГАЗИНФОРМ
СЕРВИС