Методы и модели визуализации для мониторинга безопасности компьютерных сетей

IM&CTCPA 2016

САНКТ-ПЕТЕРБУРГ, 2016

Коломеец Максим Вадимович
СПИИРАН

Визуализация безопасности

И что для этого нужно знать

Что такое визуализация?

Подходы к визуализации и кейсы ее использования

Архитектура систем

Visualization pipeline и ее место в системе безопасности

Графические модели

Виды, концепции построения и способы применения

Инструментарий

Библиотеки, платформы и данные

Будущее

Когнитивные технологии, способы взаимодействия, дополненная + виртуальная реальность

Визуализация безопасности

И что для этого нужно знать

Что такое визуализация?

Подходы к визуализации и кейсы ее использования

ПОДХОДЫ

к визуализации с разных сторон

Дизайн

Со стороны когнитивного восприятия

Концептуализация моделей визуализации; разработка решений, влияющих на эффективность восприятия информации пользователем

Наука

Со стороны Data Science

Визуализация как часть науки о данных; разработка моделей визуализации позволяющих эффективно извлекать информацию из данных; работа с большими данными гетерогенной структуры

Бизнес

Со стороны принятия решений

Визуализация как посредник и универсальный язык между отделом безопасности и бизнесом, принимающим большую часть решений; использование интуитивно понятных моделей визуализации

Безопасность

Со стороны анализа

Визуализация как инструмент обеспечения безопасности; способность визуализации обеспечивать анализ ситуации и находить события, а также инциденты безопасности

КЕЙСЫ

основные сценарии использования

ПРЕДСТАВЛЕНИЕ

Восприятие информации

Как представить набор данных наиболее эффективным образом? Как создать впечатление для принятия решений или выделить определенные компоненты?

Какие модели подходят лучше для текущей ситуации?

АНАЛИЗ

Со стороны принятия решений

Как наиболее эффективно анализировать данные в графической форме? Какие модели обеспечивают большую скорость анализа.

Какие модели подходят лучше для текущей ситуации?

Визуализация безопасности

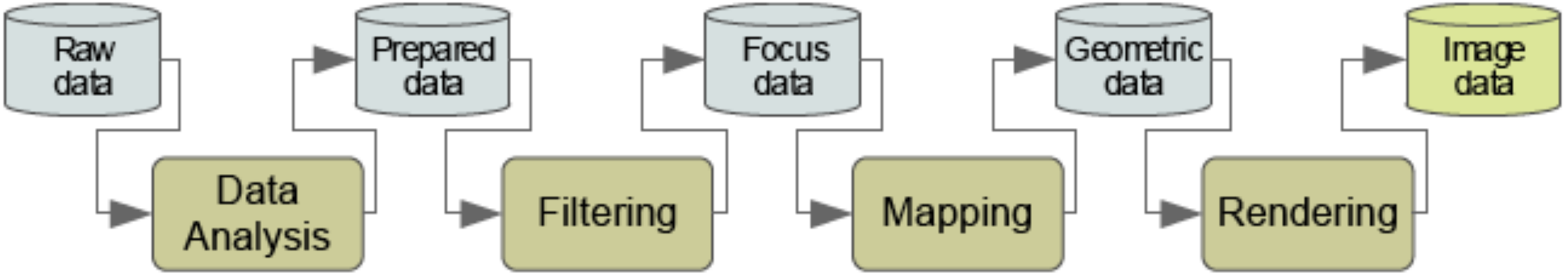
И что для этого нужно знать

Что такое визуализация?

Подходы к визуализации и кейсы ее использования

Архитектура систем

Visualization pipeline и ее место в системе безопасности



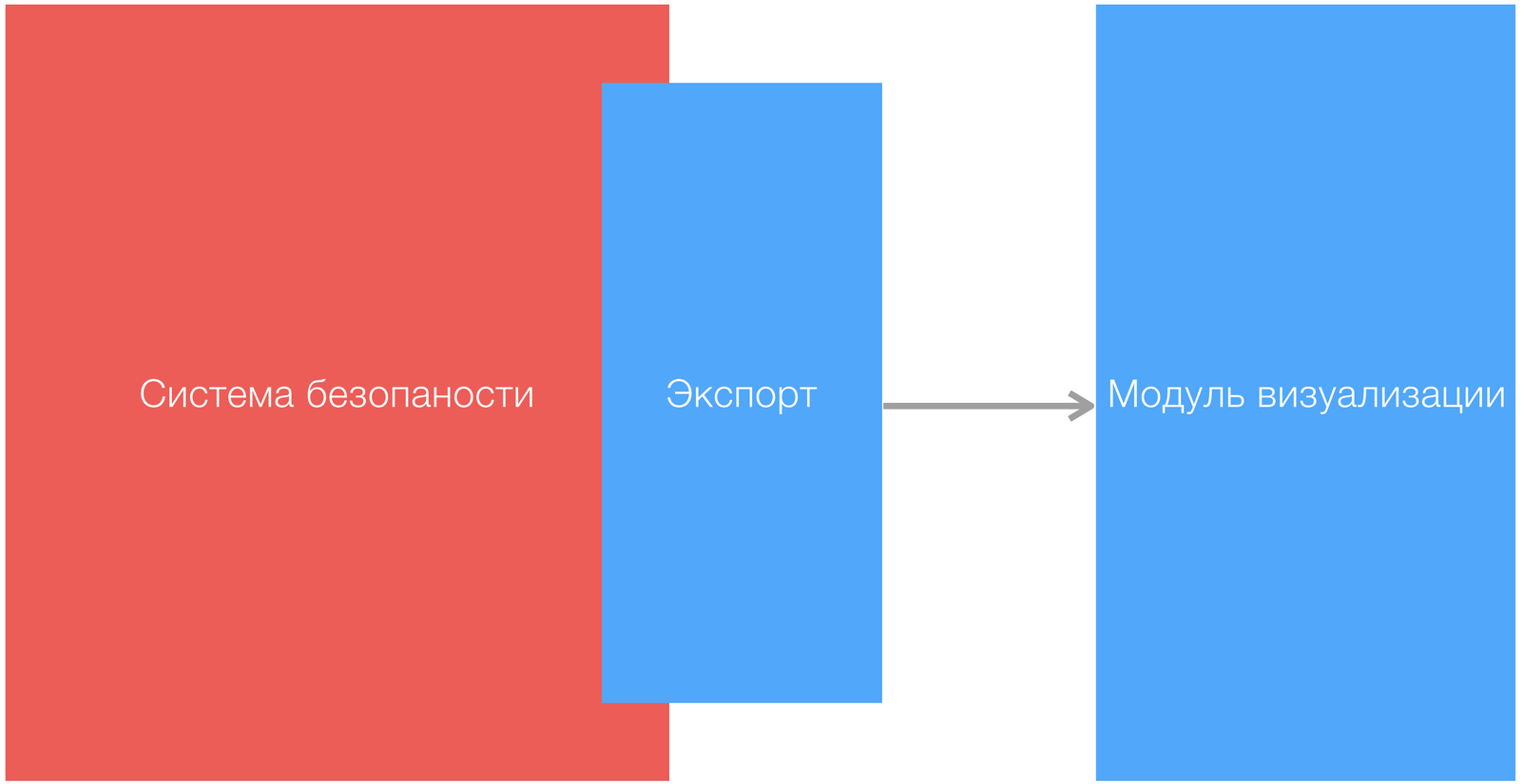
VISUALIZATION PIPELINE

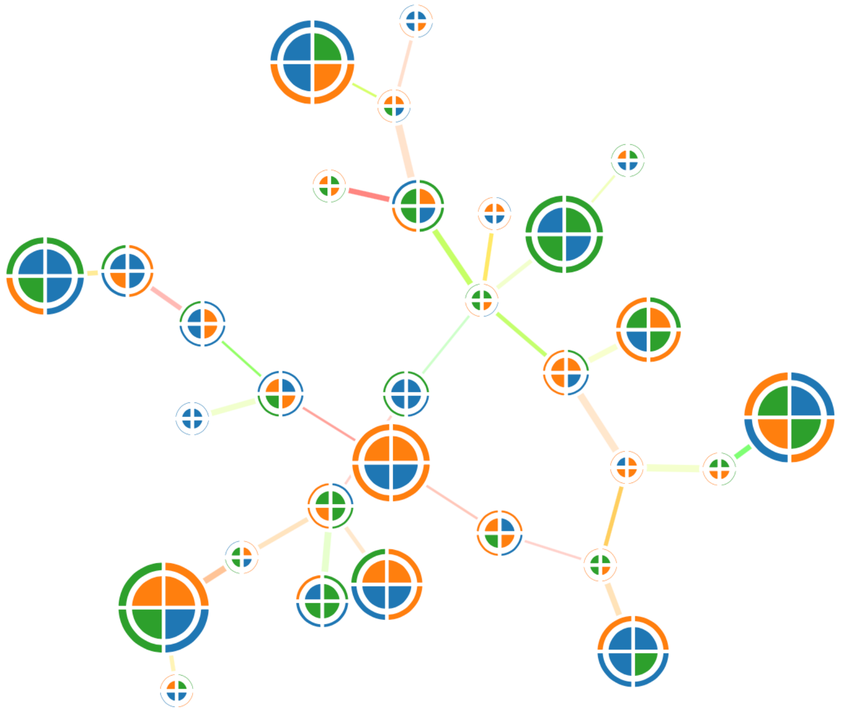
Data Analysis - отбор и обработка данных от системы безопасности

Filtering - обработка данных в соответствии с требованиями пользователя

Mapping - перевод данных в геометрические примитивы

Rendering - отрисовка





МОДУЛИ ВИЗУАЛИЗАЦИИ

Система безопасности - предоставляет данные для визуализации

Экспорт - преобразует данные в единый формат

Модуль визуализации - реализация Visualization Pipeline

Графические модели

Виды, концепции построения и способы применения

Модели визуализации

NUMERICAL

Можно представить в одной таблице

Pie Charts
Bar Charts
Line Charts
Area Charts
Stacked Charts
Bubble Charts
HeatMaps
Hexagonal Maps
Scatter Plots
Triangle Plots
Box Plots
Streamgraph

etc.

NOT NUMERICAL

Невозможно представить в одной таблице

Graphs
Trees
Matrices
TreeMaps
Voronoi Diagrams
Parallel Coordinates
Hive Plots
Circle Packing (Graphs of coins)
Interval Graphs
Attack Trees, Matrices, etc.
Geo
Education models

etc.

Модели визуализации

NUMERICAL

Можно представить в одной таблице

Pie Charts
Bar Charts
Line Charts
Area Charts
Stacked Charts
Bubble Charts
HeatMaps
Hexagonal Maps
Scatter Plots
Triangle Plots
Box Plots
Streamgraph

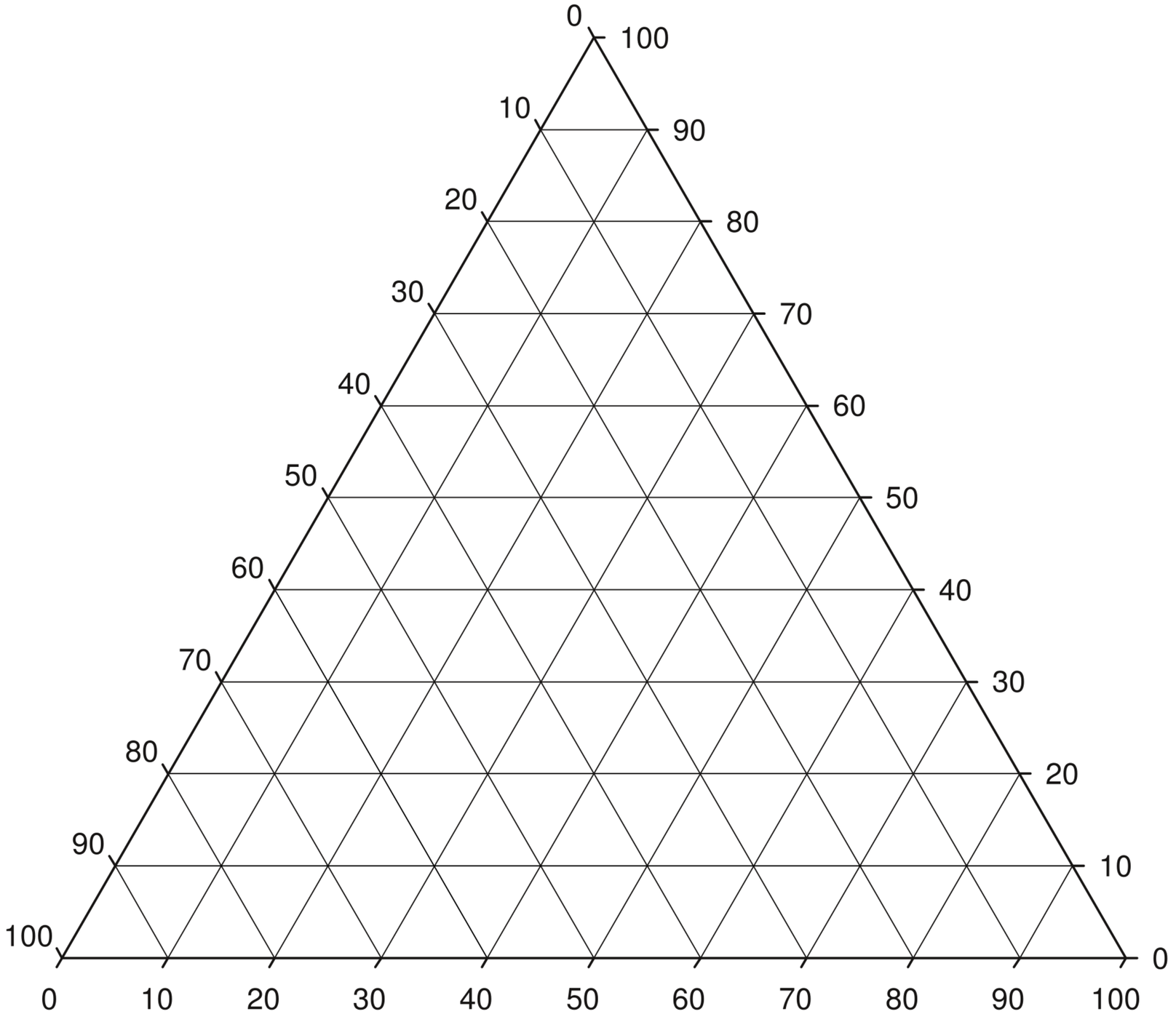
etc.

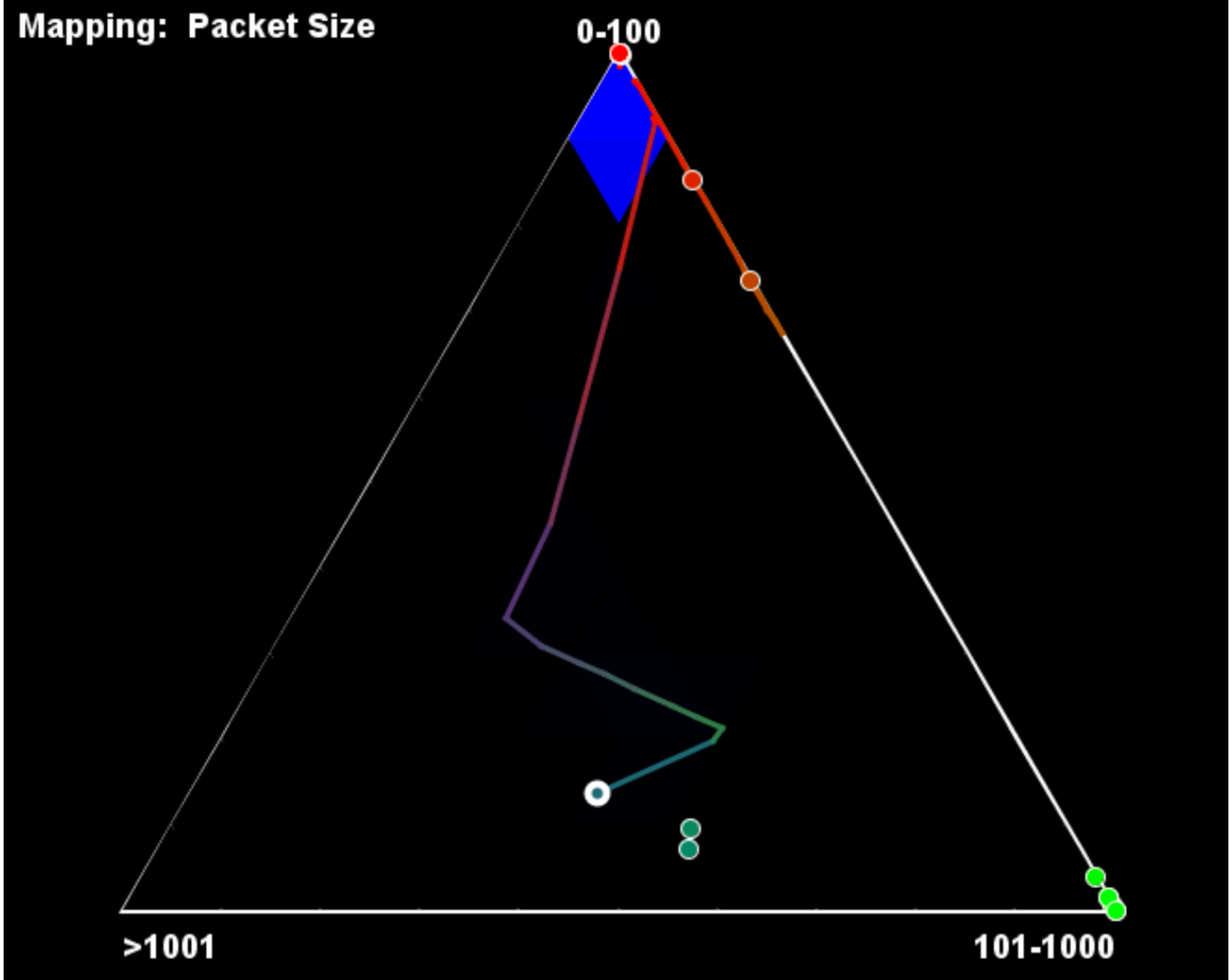
NOT NUMERICAL

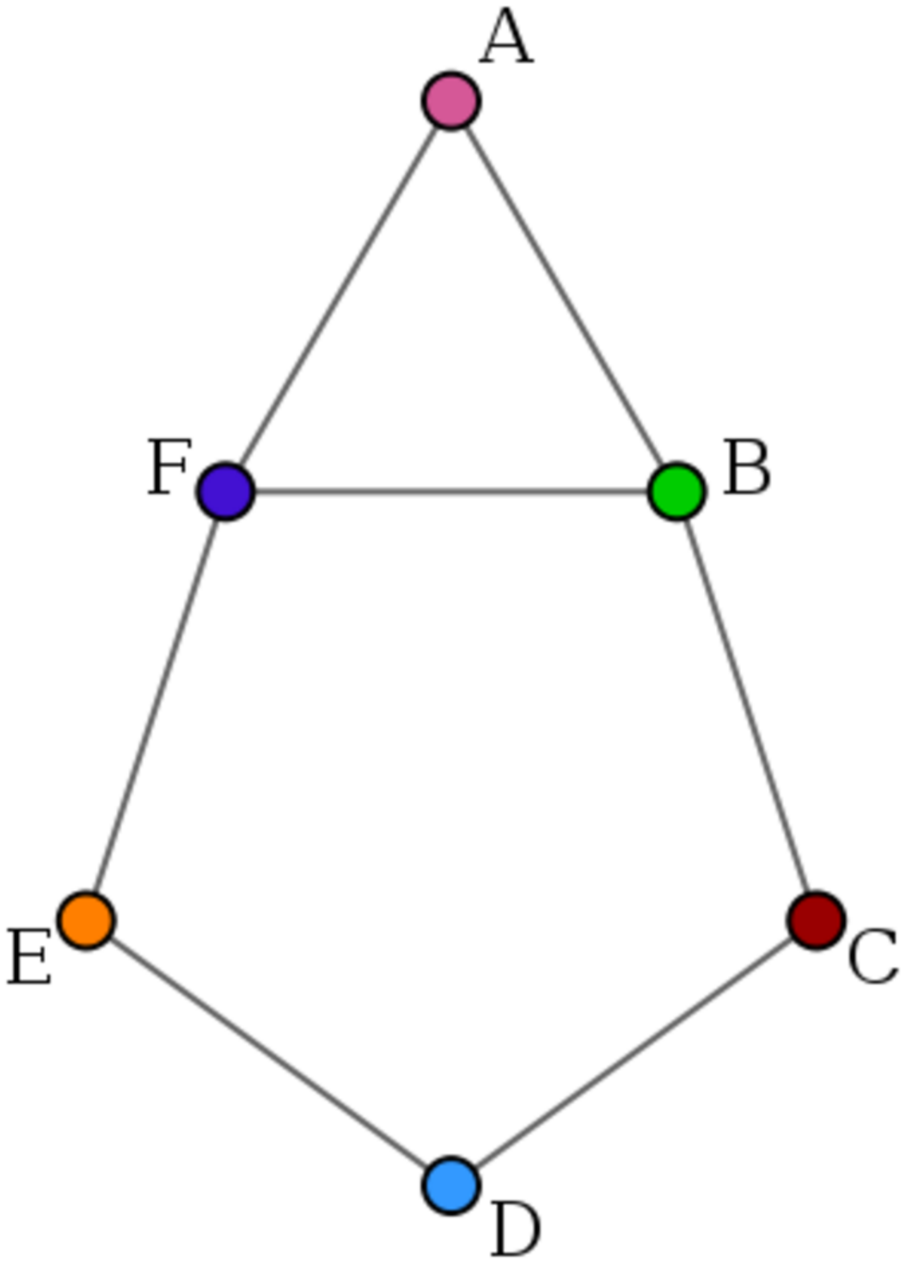
Невозможно представить в одной таблице

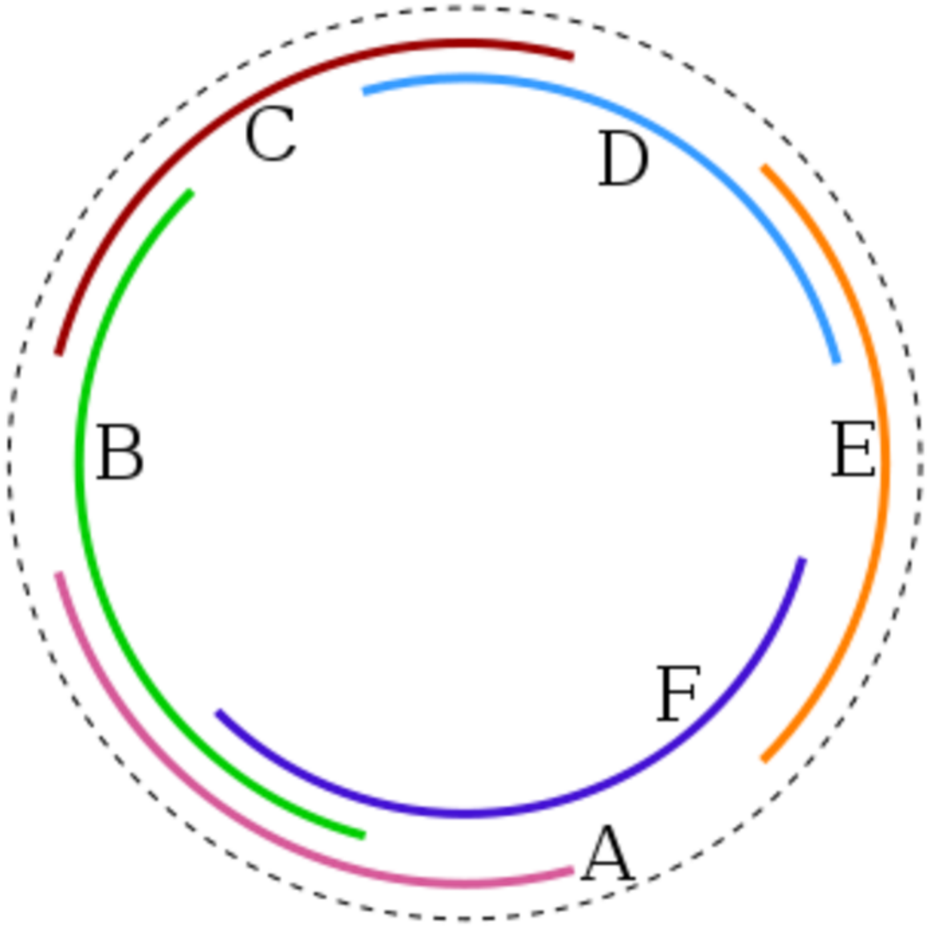
Graphs
Trees
Matrices
TreeMaps
Voronoi Diagrams
Parallel Coordinates
Hive Plots
Circle Packing (Graphs of coins)
Interval Graphs
Attack Trees, Matrices, etc.
Geo
Education models

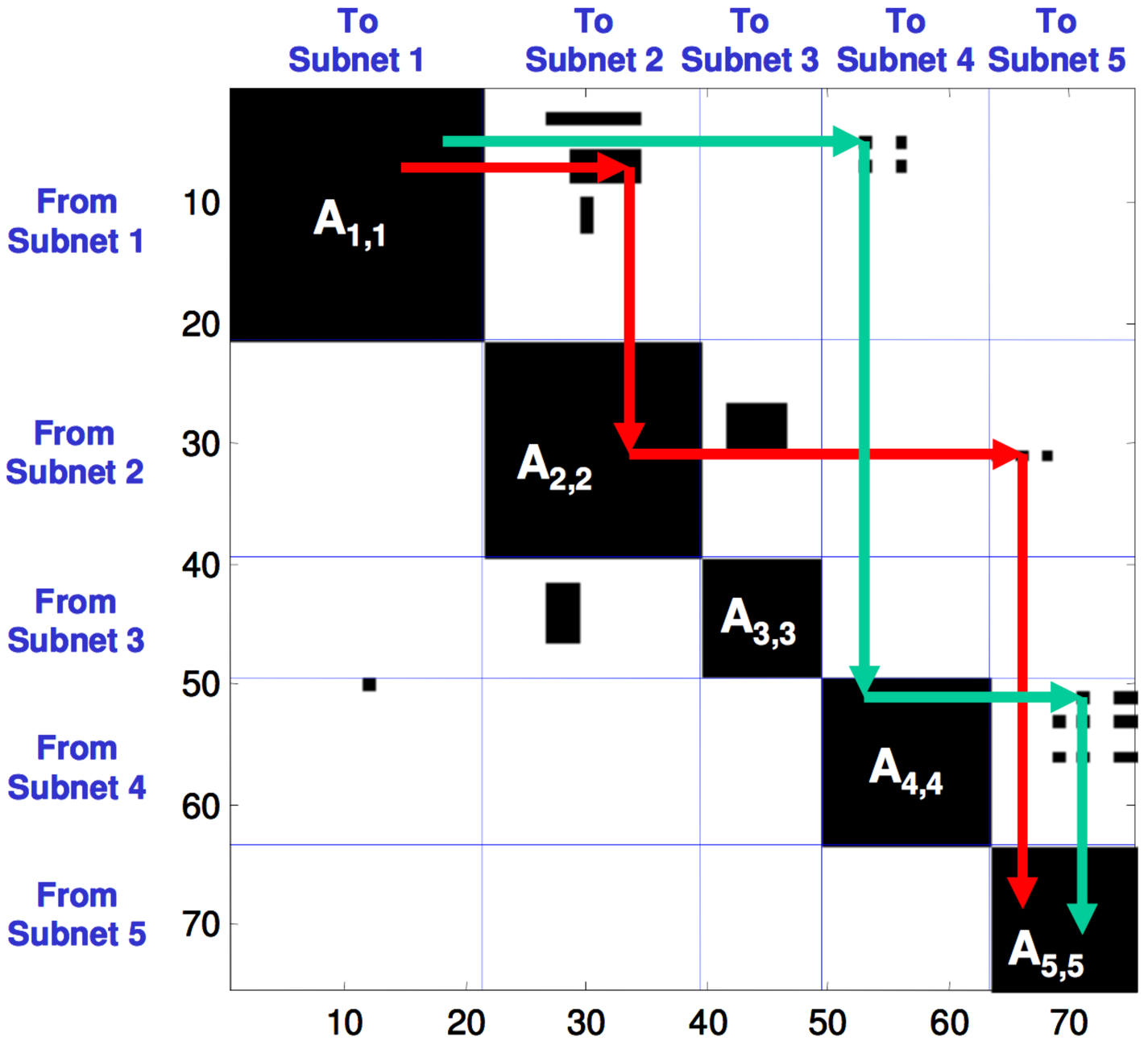
etc.


0
100
10
90
20
80
30
70
40
60
50
50
60
40
70
30
80
20
90
10
100
0
0
10
20
30
40
50
60
70
80
90
100


Mapping: Packet Size
0-100
>1001
101-1000


A
F
B
E
C
D


C
D
B
E
F
A


To Subnet 1
To Subnet 2
To Subnet 3
To Subnet 4
To Subnet 5
From Subnet 1
From Subnet 2
From Subnet 3
From Subnet 4
From Subnet 5
A1,1
A2,2
A3,3
A4,4
A5,5
10
20
30
40
50
60
70

Графические модели

Виды, концепции построения и способы применения

Инструментарий

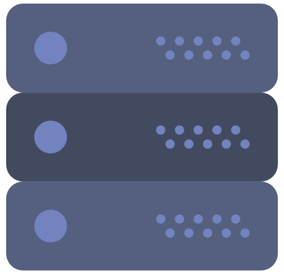
Библиотеки, платформы и данные

ИНСТРУМЕНТЫ

или с чего начать

БИБЛИОТЕКИ

D3.js - 2D визуализация
THREE.js - 3D визуализация
Библиотеки на R, Python
Игровые движки - ex. Unity



ПЛАТФОРМЫ

Онлайн API на основе разработанных графических моделей и своих данных

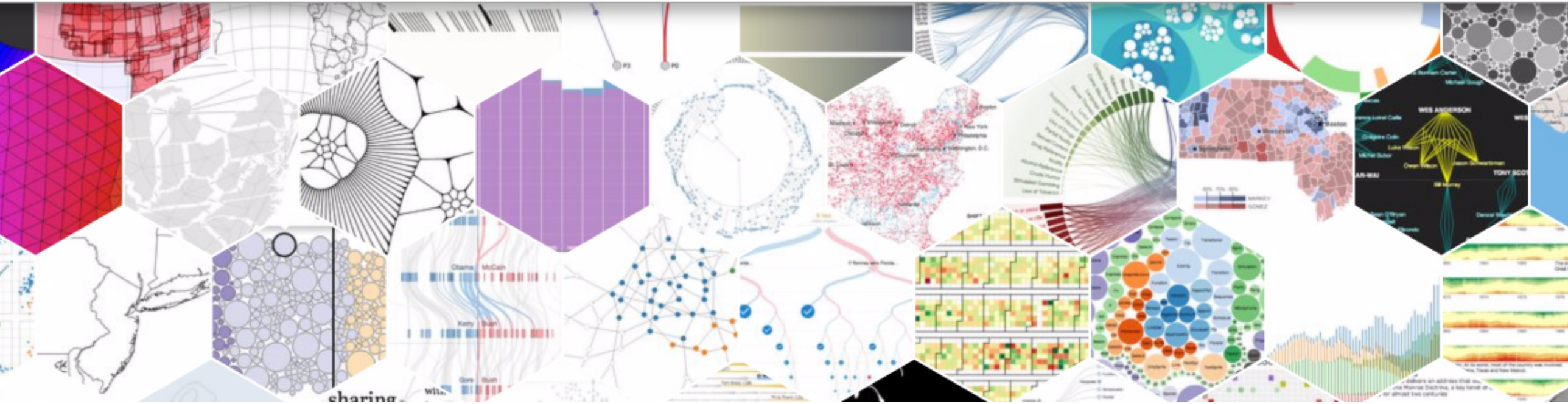
ДАННЫЕ

Где брать интересные данные когда их нет?

Overview Examples Documentation Source

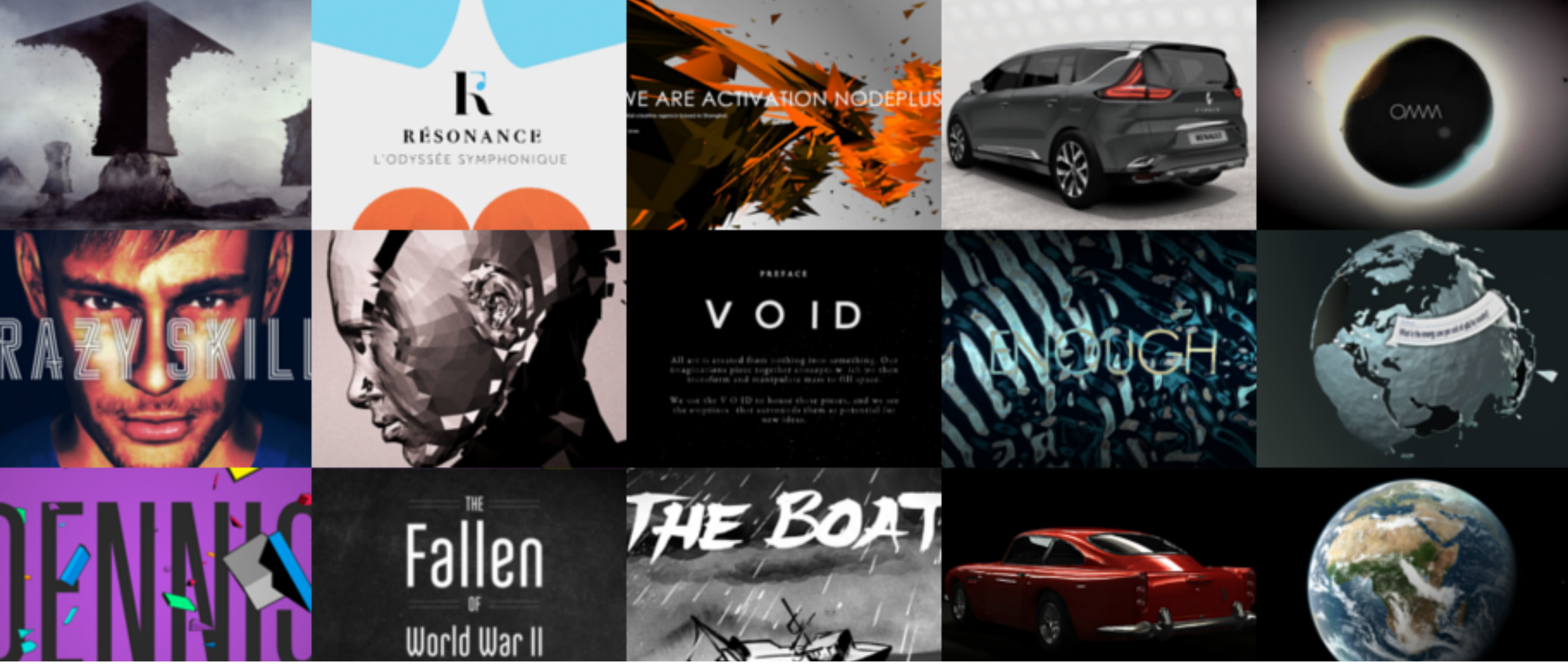
Fork me

Data-Driven Documents



Data Driven Document - D3.js

наиболее популярная библиотека для визуализации в 2D



THREE.js

наиболее простая библиотека для визуализации в 3D

```
30 barplot(sl)
31
32 pairs(iris[,1:5])
33
34 qqnorm(sl)
35 qqline(sl)
36
37 par(mfrow=c(2,2))
38
39 hist(sl,freq=F)
40 lines(sl.d)
41 boxplot(sl)
42 qqnorm(sl)
43 qqline(sl)
44 barplot(sl)
45
46 par(mfrow=c(1,1))
47
48
```

48:1 (Top Level) R Script

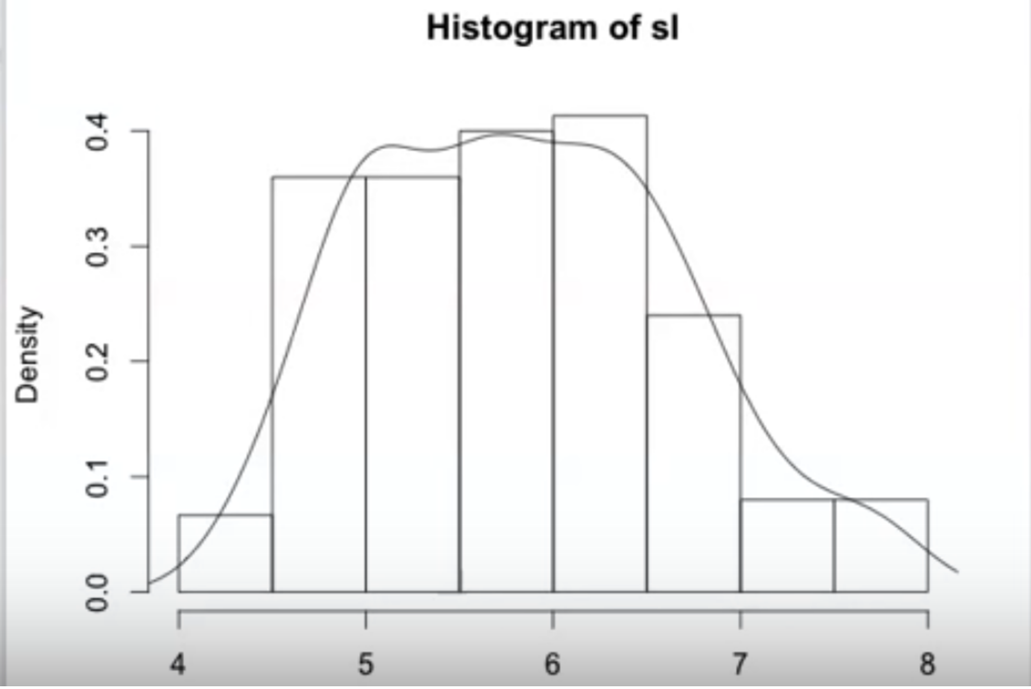
Console ~/Dropbox/HowToR/

```
> pairs(iris[,1:5])
> qqnorm(sl)
> qqline(sl)
> par(mfrow=c(2,2))
> hist(sl,freq=F)
> lines(sl.d)
> boxplot(sl)
> qqnorm(sl)
> qqline(sl)
> barplot(sl)
> par(mfrow=c(1,1))
```

HowToR.Rproj	204 bytes	Sep 5, 2013, 10:36 AM
lesson1_basicFunctions.R	1.9 KB	Sep 10, 2013, 3:31 PM
lesson2_IntrotoWorkingWithData.R	4.1 KB	Sep 10, 2013, 4:05 PM
lesson3_vizualization.R	1.5 KB	Sep 11, 2013, 12:07 PM
myPlot.R	354 bytes	Sep 10, 2013, 5:29 PM

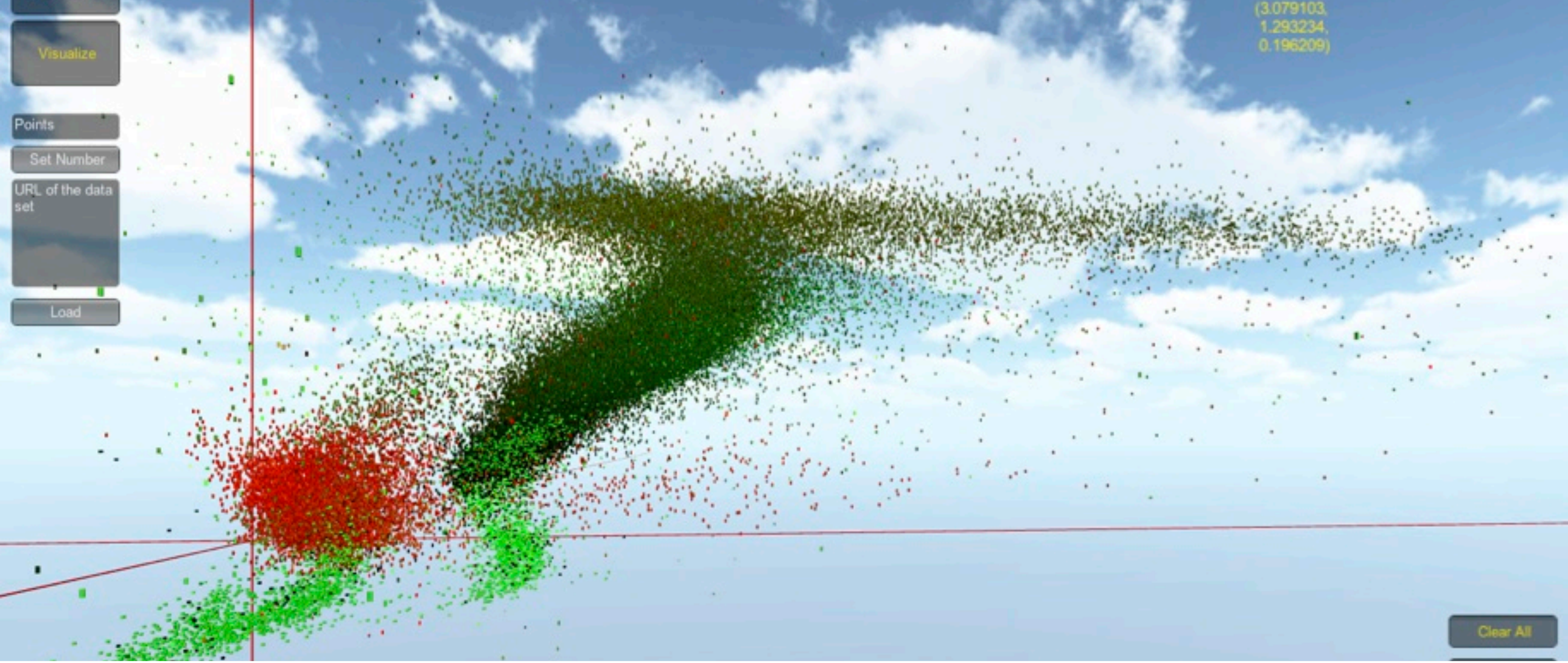
Plots Packages Help

Zoom Export Clear All



Различные библиотеки на Python, R, Java, etc.

библиотеки подходящие для работы с данными в период разработки



Игровые движки

Компоненты игр прекрасно подходят для визуализации

Готовые решения для общих случаев

https://plot.ly
https://datahero.com
http://site.numberpicture.com
http://www.juiceanalytics.com
http://www.oicweave.org
http://datavisu.al
https://www.silk.co
http://www.zoomdata.com
https://www.datawrapper.de
http://www.tableau.com/h2
http://www.clearstorydata.com
https://beyondcore.com
http://www.wolfram.com/mathematica/

http://app.raw.densitydesign.org

Источники данных

http://www.google.com/publicdata/directory

http://data.worldbank.org

www.kaggle.com

Отчеты сканеров

Графические модели

Виды, концепции построения и способы применения

Инструментарий

Библиотеки, платформы и данные

Будущее

Когнитивные технологии, способы взаимодействия, дополненная + виртуальная реальность

Что будет актуально в будущем?

КОГНИТИВНЫЕ ТЕХНОЛОГИИ

Способы улучшения эффективности восприятия информации неспециалистом, интеллектуальный подбор параметров и моделей визуализации, создание концептуально новых графических моделей

ИНТЕРАКТИВНОЕ ВЗАИМОДЕЙСТВИЕ

Новые способы человека-машинного взаимодействия согласно концепции Direct Manipulation (как программные, так и аппаратные средства)

ДОПОЛНЕННАЯ РЕАЛЬНОСТЬ

Использование дополненной реальности, отход визуализации от кибернетических событий к физическим и кибер-физическим.

КОГНИТИВНЫЕ ТЕХНОЛОГИИ

Для представления и впечатления

Аспекты:

Графический дизайн

Lie Factor

Chart Junk

Когнитивный аппарат

Использование машинного обучения

КОГНИТИВНЫЕ ТЕХНОЛОГИИ

Для представления и впечатления

Аспекты:

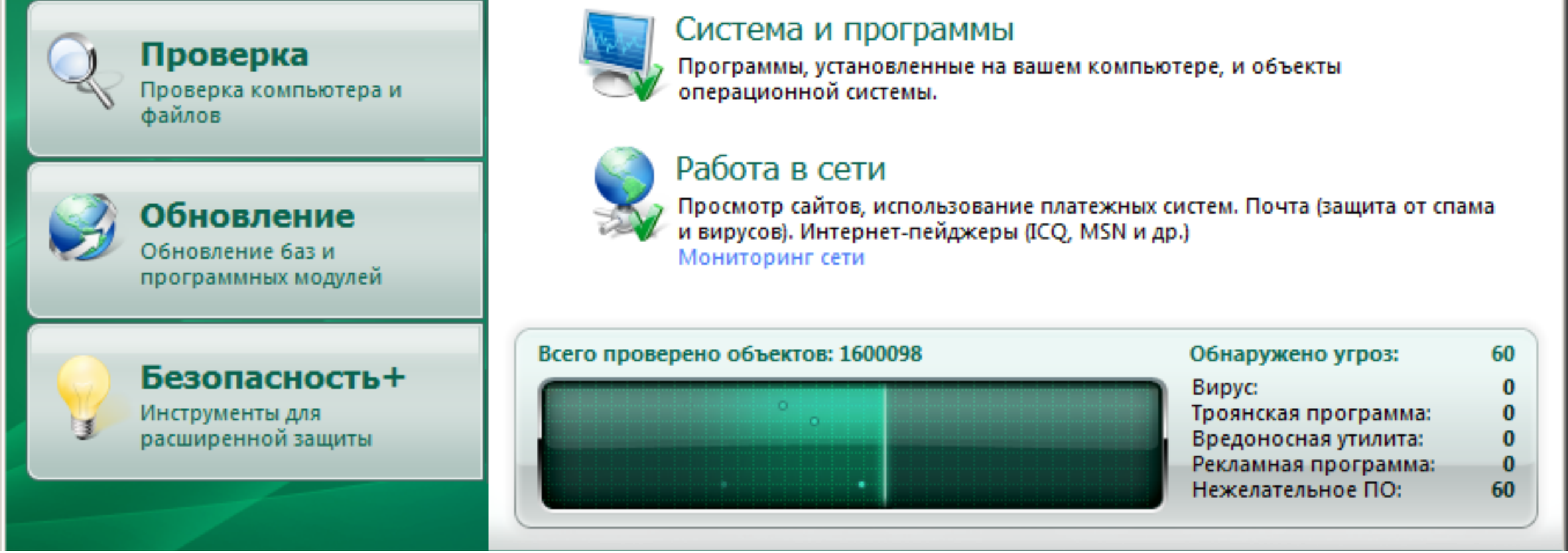
Графический дизайн
Lie Factor
Chart Junk
Когнитивный аппарат
Использование машинного обучения

КОГНИТИВНЫЕ ТЕХНОЛОГИИ

Для представления и впечатления

Аспекты:

Графический дизайн
Lie Factor
Chart Junk
Когнитивный аппарат
Использование машинного обучения



КОГНИТИВНЫЕ ТЕХНОЛОГИИ

Для представления и впечатления

Аспекты:

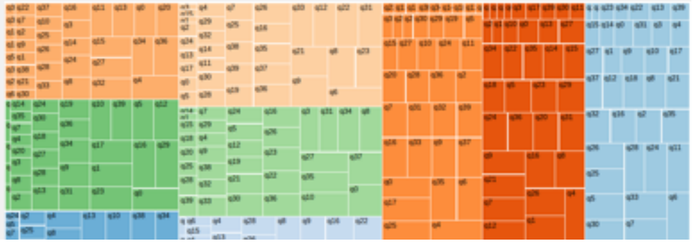
- Графический дизайн
- Lie Factor
- Chart Junk
- Когнитивный аппарат
- Использование машинного обучения

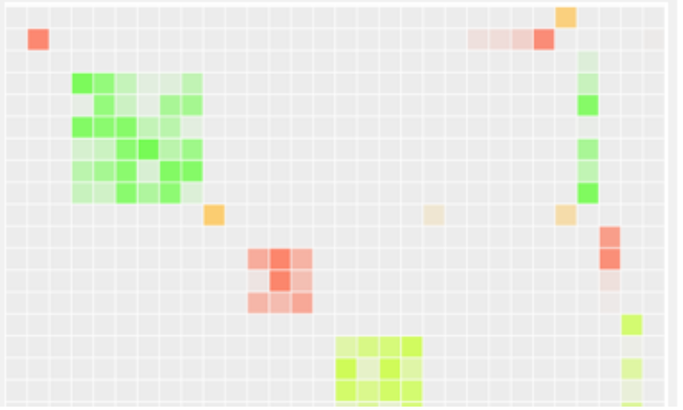
А вполне ли вы уверены, что все эти погремушки и свистульки, все эти потрясающие возможности ваших, так сказать, «мощных» языков программирования имеют отношение к процессу решения, а не к самим задачам

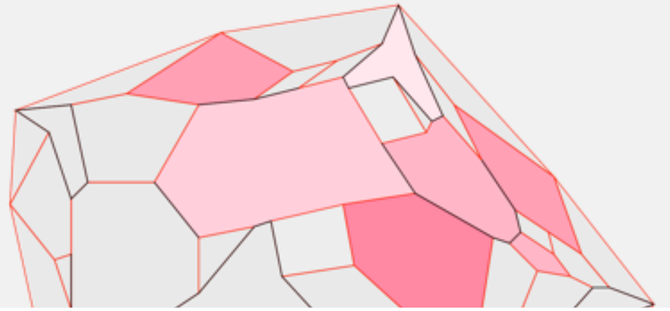
Э. Дейкстра. «Дисциплина программирования», 1976

Document
21.04.2015
Network #4

Scan
17.01.2015
NO_NAME





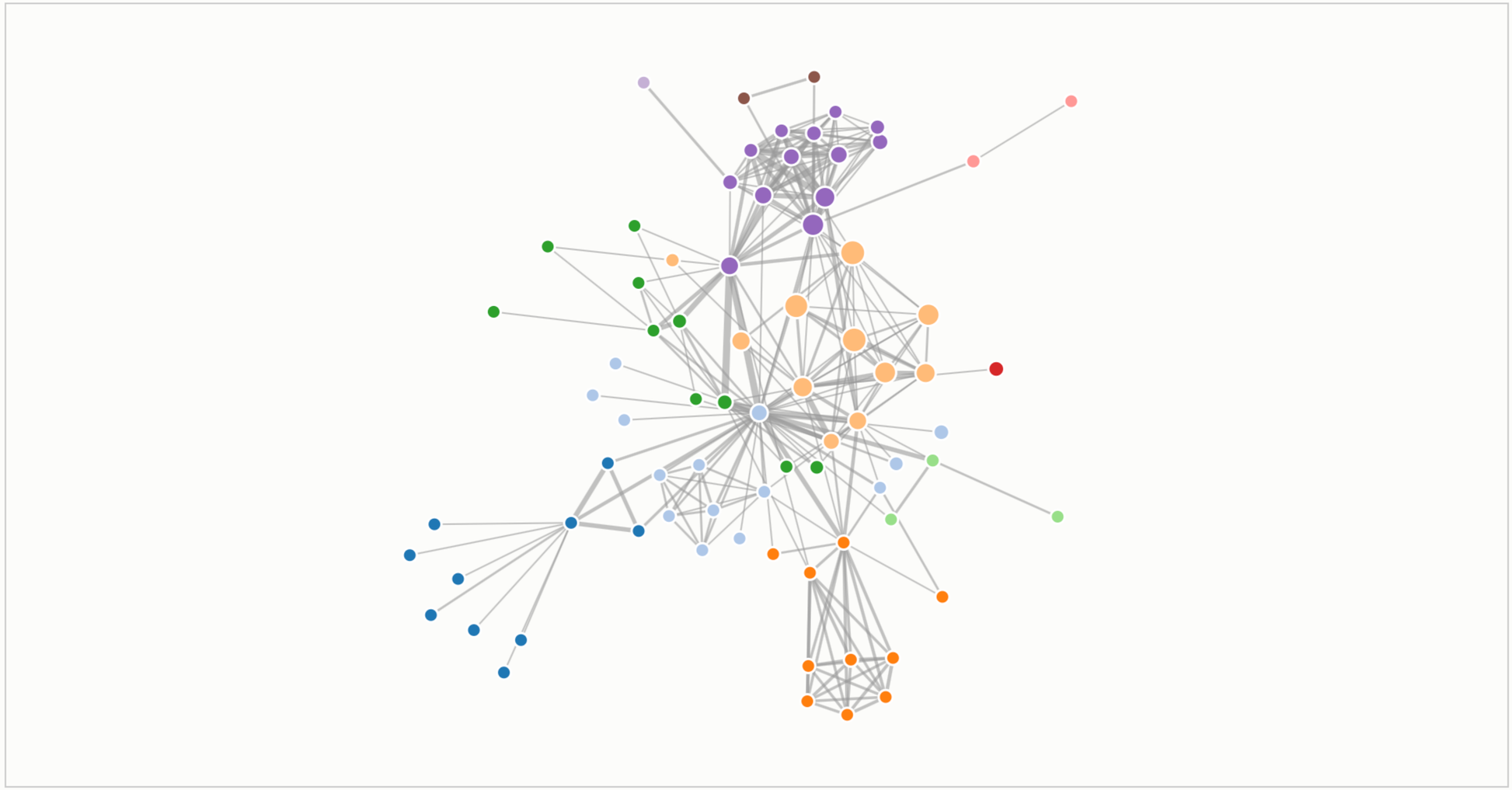


КОГНИТИВНЫЕ ТЕХНОЛОГИИ

Для представления и впечатления

Аспекты:

Графический дизайн
Lie Factor
Chart Junk
Когнитивный аппарат
Использование машинного обучения



ИНТЕРАКТИВНОЕ ВЗАИМОДЕЙСТВИЕ

Для анализа и удобства управления

Аспекты:

- Дополнительные инструменты моделей визуализации
- Direct Manipulation
- Cumputer-Human Interactions

ИНТЕРАКТИВНОЕ ВЗАИМОДЕЙСТВИЕ

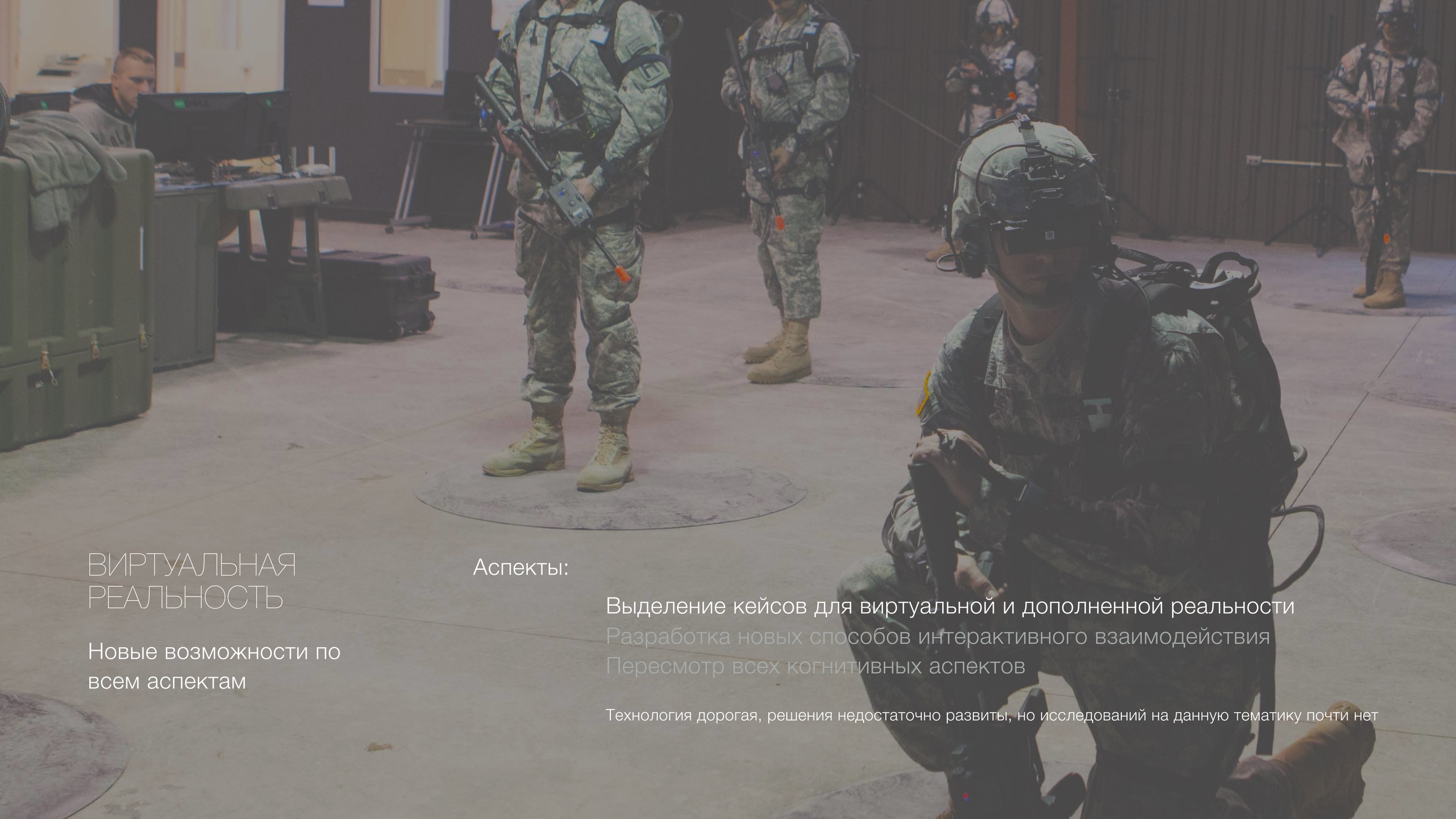
Для анализа и удобства управления

Аспекты:

Дополнительные инструменты моделей визуализации

Direct Manipulation

Cumputer-Human Interactions



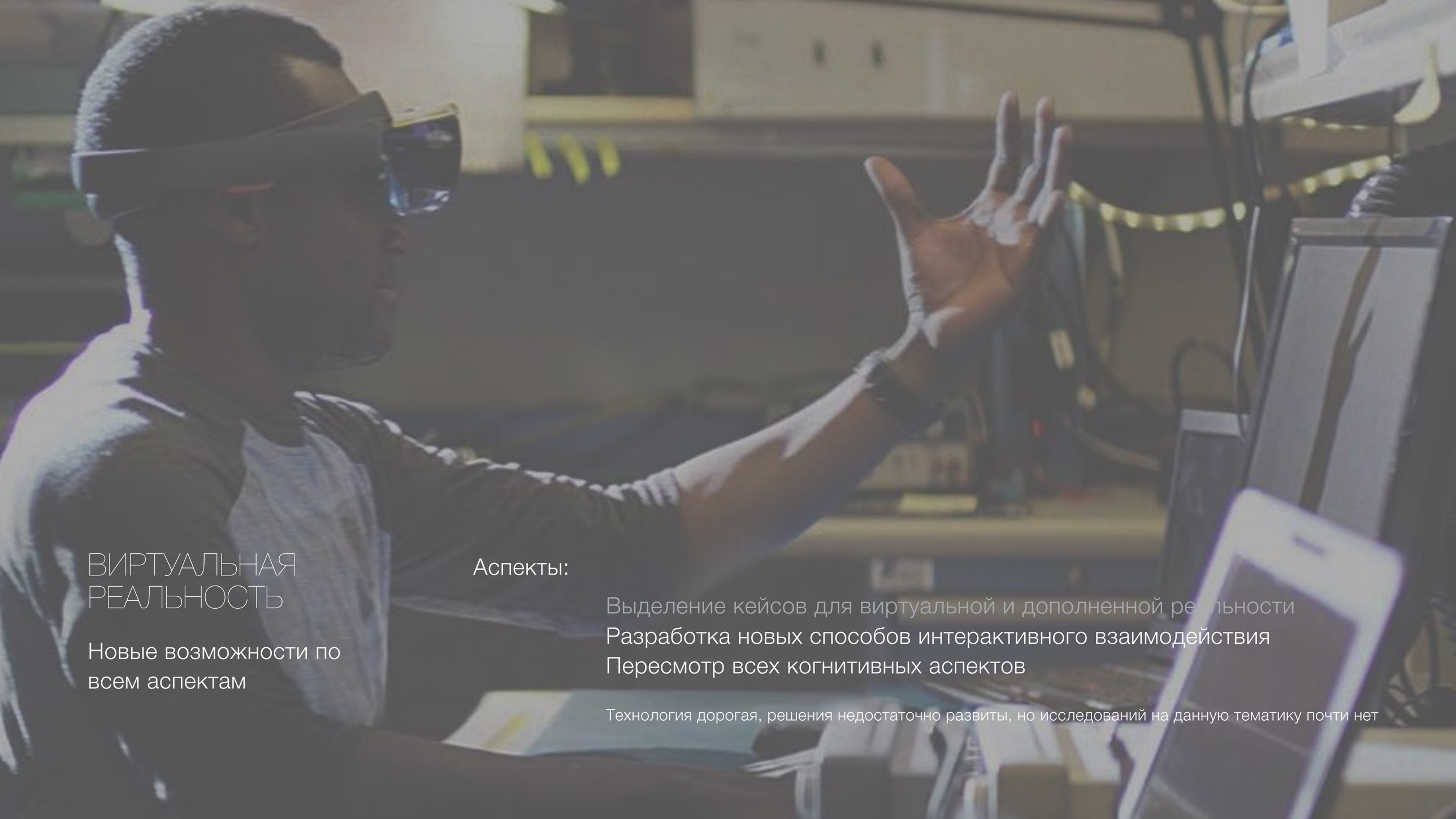
ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ

Новые возможности по всем аспектам

Аспекты:

Выделение кейсов для виртуальной и дополненной реальности
Разработка новых способов интерактивного взаимодействия
Пересмотр всех когнитивных аспектов

Технология дорогая, решения недостаточно развиты, но исследований на данную тематику почти нет



ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ

Новые возможности по всем аспектам

Аспекты:

Выделение кейсов для виртуальной и дополненной реальности

Разработка новых способов интерактивного взаимодействия

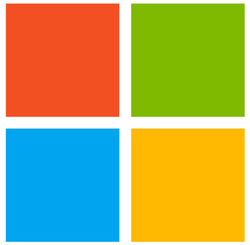
Пересмотр всех когнитивных аспектов

Технология дорогая, решения недостаточно развиты, но исследований на данную тематику почти нет

Cardboard

Daydream

Oculus



Microsoft
HoloLens

С чего начать вам

Разобраться с форматом JSON / CSV

Библиотека C3.js

Что используем мы

D3.js - для создания 2D моделей

THREE.js - для создания 3D моделей

JavaFX - для отладки

Распределенная система - Java EE и JS

Генераторы и отчеты SIEM систем - как источники данных

VizSec - как источник передовых работ в области визуализации данных безопасности

Спасибо за внимание

IM&CTCPA 2016

САНКТ-ПЕТЕРБУРГ, 2016

Коломеец Максим Вадимович
Лаборатория проблем компьютерной безопасности - СПИИРАН
kolomeec@comsec.spb.ru
www.comsec.spb.ru/ru/staff/kolomeec