НТЦ ВУЛКАН

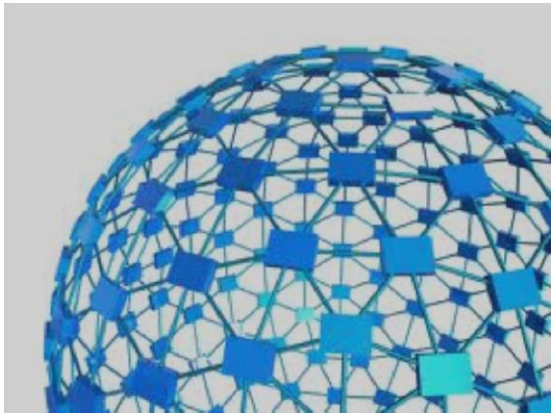
Международный ТБ ФОРУМ 2014 Технологии Безопасности

Инструменты визуального анализа графов в обеспечении информационной и экономической безопасности

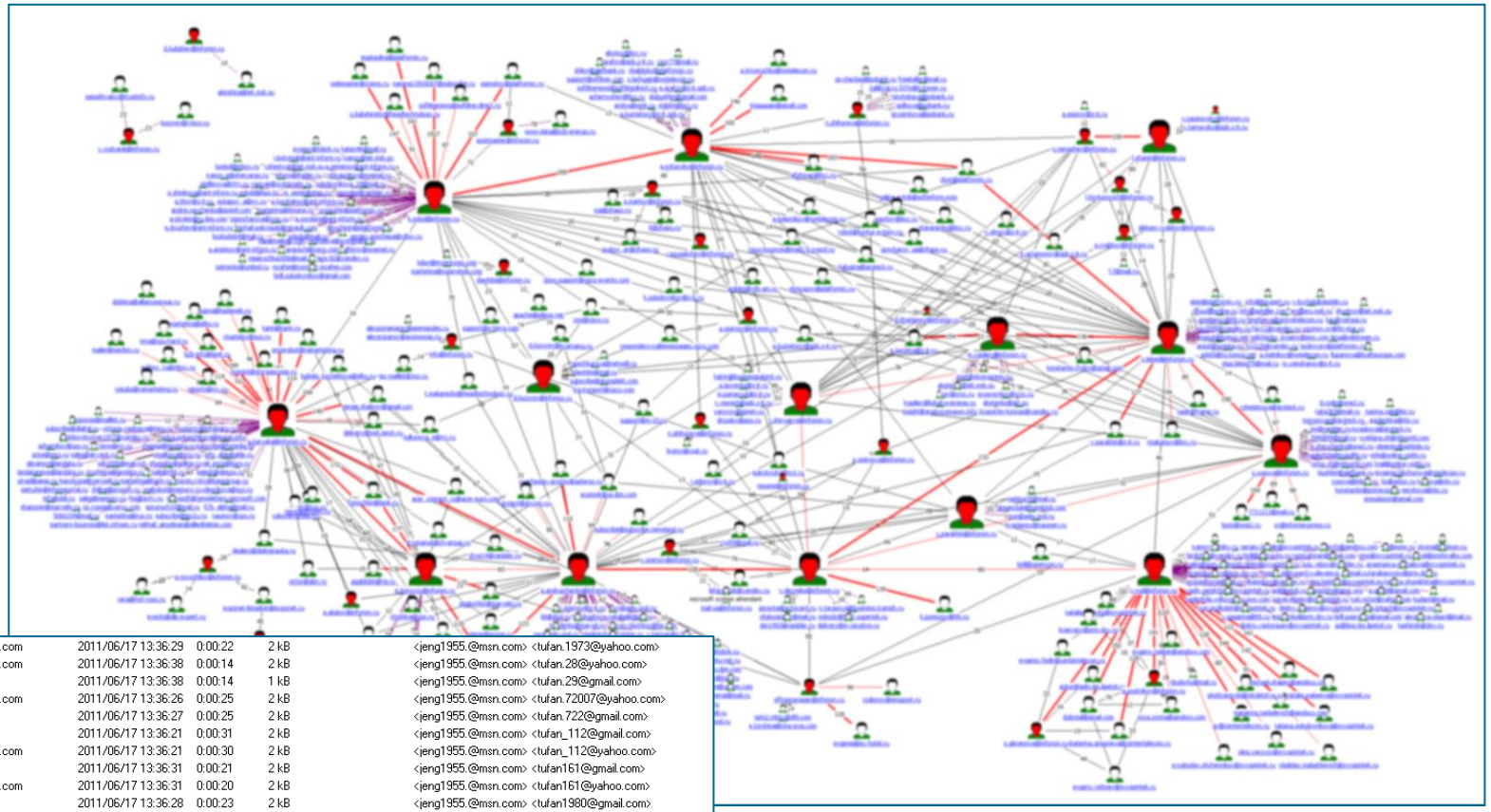
Февраль 2014 г.

«Сетевые» данные

- Внутренние и внешние электронные коммуникации сотрудников
  - Внутренняя телефонная связь
  - Корпоративная мобильная связь
  - Электронная почта
  - Социальные сети
- Сведения о связях партнеров и контрагентов
  - Учредители
  - Дочерние компании
  - Участие в конкурсах
  - Судебные разбирательства



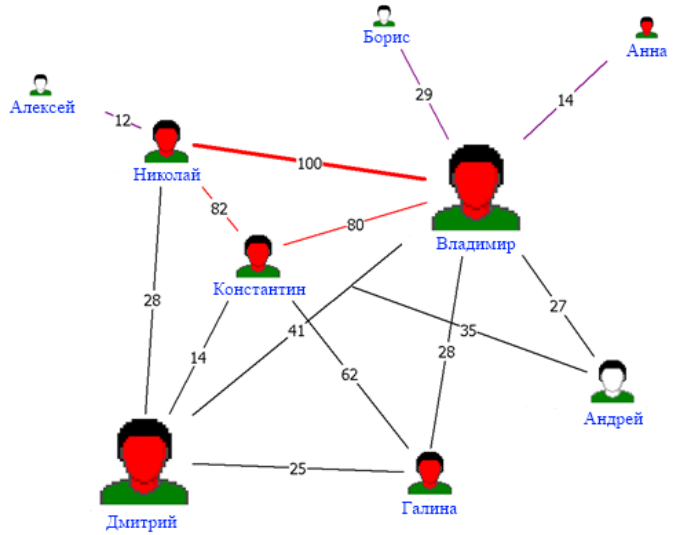
Пример «сети»



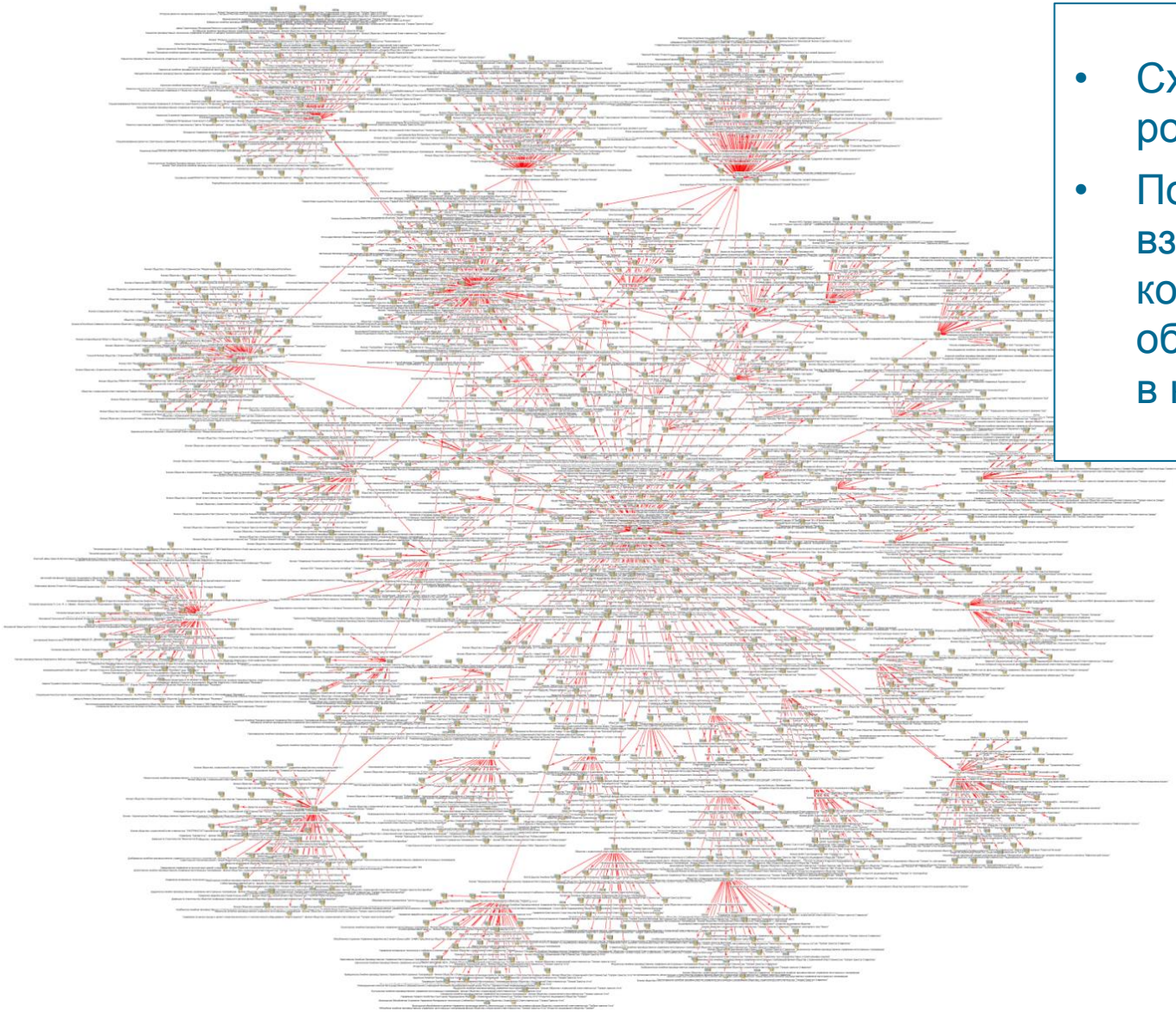
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:29	0:00:22	2 kB	<jeng1955.@msn.com>	<tufan.1973@yahoo.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:38	0:00:14	2 kB	<jeng1955.@msn.com>	<tufan.28@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:38	0:00:14	1 kB	<jeng1955.@msn.com>	<tufan.29@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:26	0:00:25	2 kB	<jeng1955.@msn.com>	<tufan.72007@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:27	0:00:25	2 kB	<jeng1955.@msn.com>	<tufan.722@gmail.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:21	0:00:31	2 kB	<jeng1955.@msn.com>	<tufan_112@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:21	0:00:30	2 kB	<jeng1955.@msn.com>	<tufan_112@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:31	0:00:21	2 kB	<jeng1955.@msn.com>	<tufan161@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:31	0:00:20	2 kB	<jeng1955.@msn.com>	<tufan161@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:28	0:00:23	2 kB	<jeng1955.@msn.com>	<tufan1980@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:28	0:00:23	2 kB	<jeng1955.@msn.com>	<tufan1980@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:28	0:00:24	2 kB	<jeng1955.@msn.com>	<tufan456@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:28	0:00:23	2 kB	<jeng1955.@msn.com>	<tufan456@yahoo.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:31	0:00:20	2 kB	<jeng1955.@msn.com>	<tufan487@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:31	0:00:20	2 kB	<jeng1955.@msn.com>	<tufan488@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:29	0:00:22	2 kB	<jeng1955.@msn.com>	<tufan55@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:29	0:00:22	2 kB	<jeng1955.@msn.com>	<tufan550@gmail.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:30	0:00:21	2 kB	<jeng1955.@msn.com>	<tugay_2211@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:30	0:00:21	2 kB	<jeng1955.@msn.com>	<tugay_2211@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:43	0:00:08	2 kB	<jeng1955.@msn.com>	<tugay_84@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:44	0:00:08	2 kB	<jeng1955.@msn.com>	<tugay_84@yahoo.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:32	0:00:20	2 kB	<jeng1955.@msn.com>	<tugay1976@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:32	0:00:20	2 kB	<jeng1955.@msn.com>	<tugay1977@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:44	0:00:07	2 kB	<jeng1955.@msn.com>	<tugay2007@yahoo.com>
209.85.227.27	wy-in-f27.1e100.net	2011/06/17 13:36:44	0:00:07	2 kB	<jeng1955.@msn.com>	<tugay20070@gmail.com>
98.139.54.60	mta-v3.mail.vip.ac4.yahoo.com	2011/06/17 13:36:32	0:00:19	2 kB	<jeng1955.@msn.com>	<tugay509@yahoo.com>

Типовые цели анализа «сетей» в ИБ

- Выявление неформальных лидеров
- Выявление подозрительных «группировок» в компании
- Выявление возможных каналов утечки информации (ОБС)
- Выявление нежелательных связей между сотрудниками компании



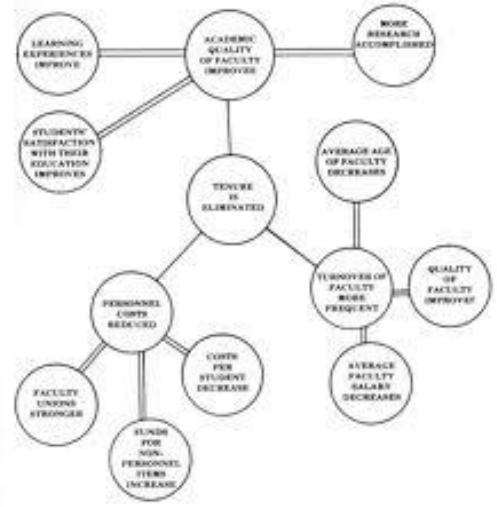
Еще пример сетевой структуры



- Схема ДЗО крупной российской компании
- Показаны 344 взаимосвязанные компании и 352 связи, обозначающие участие в капитале

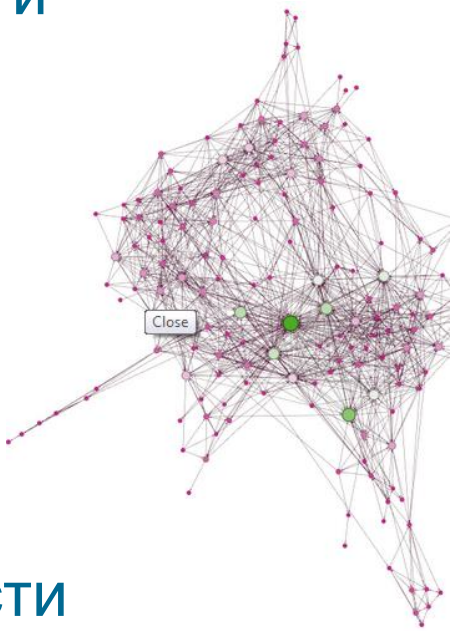
Типовые цели анализа «сетей» в ЭБ

- Понимание финансовых взаимоотношений (в том числе и конкурентов)
- Поиск путей косвенного влияния
- Минимизация затрат на получение влияния
- Противодействие хищениям
- Выделение ключевых активов
- Анализ действий конкурентов



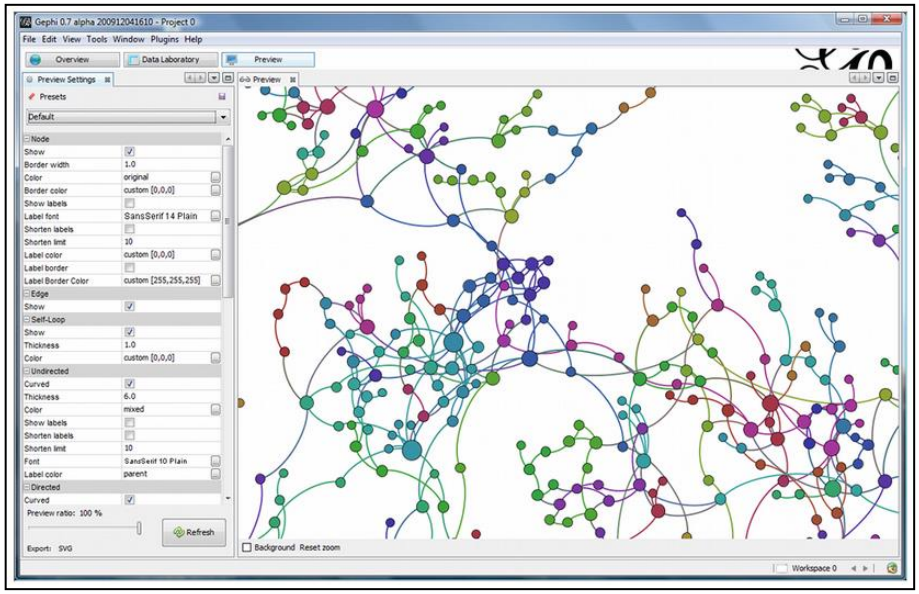
Необходимые возможности

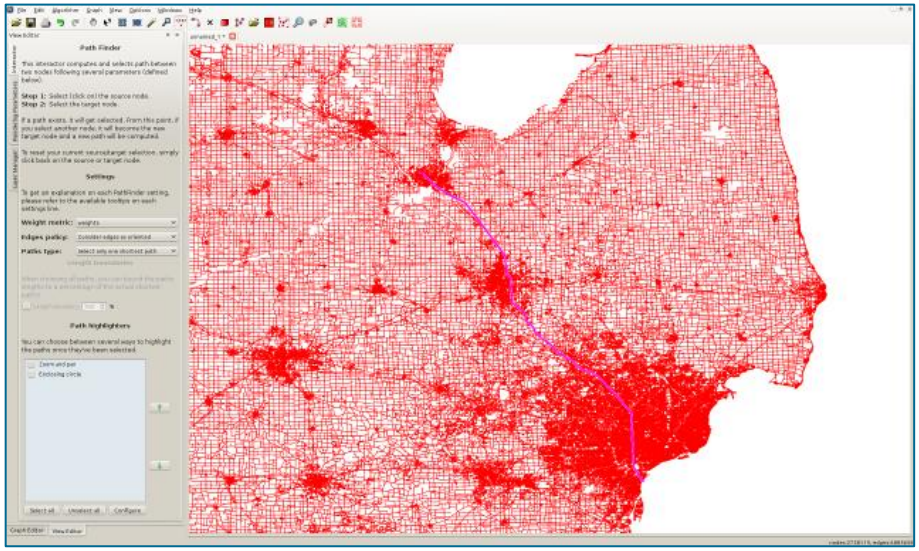
- Визуализация сетевых данных с использованием графических обозначений и различных способов маркировки
- Возможность анализировать данные, полученные из разных источников
- Встроенные поисковые и аналитические инструменты
- Автоматизация типовых задач анализа
- Возможность расширения функциональности ПО анализа данных
- Относительная простота освоения



Бесплатные продукты

- Pajek
- Tulip
- Cytoscape
- Gephi – пожалуй, самый удобный из бесплатных

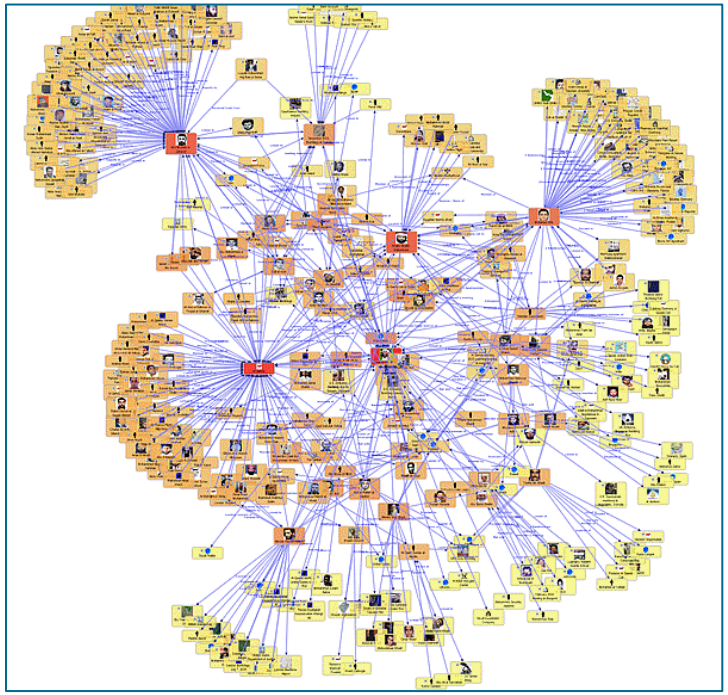




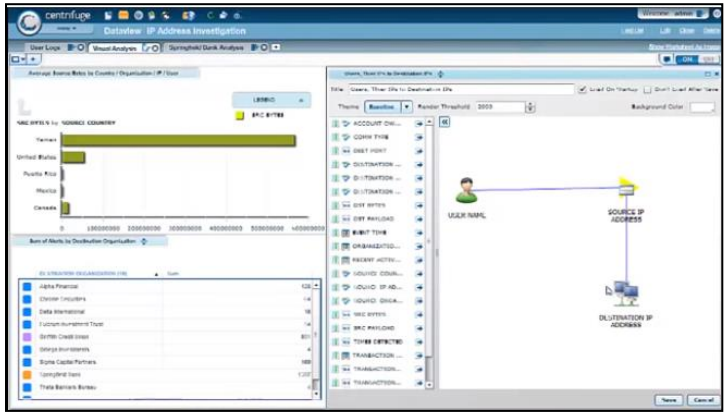
Академические исследовательские инструменты с высоким «порогом входа»

Коммерческие продукты

- Sentinel Visualizer
- VisuaLinks
- NetMiner
- i2 Analyst’s Notebook
- Centrifuge



Большинство таких продуктов – это настольные приложения с возможностью подключения БД



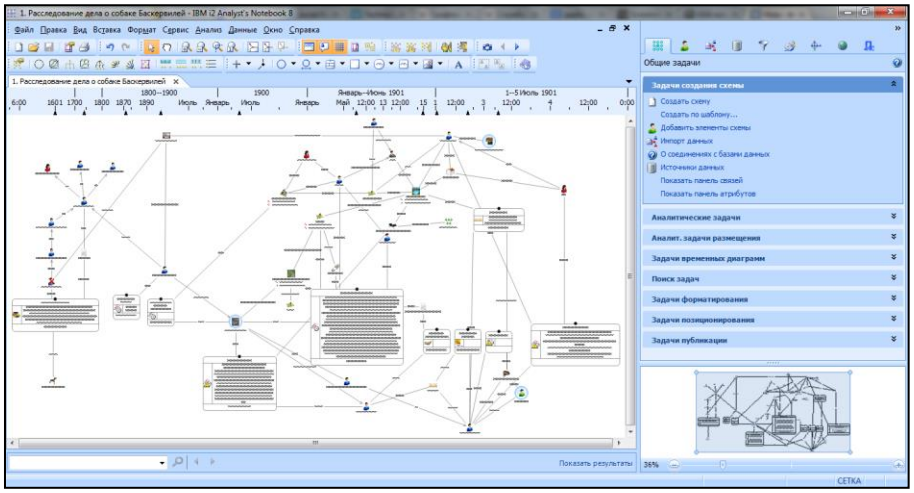
IBM i2 Analyst's Notebook

Достоинства:

- Масса возможностей визуализации статистических данных
- Поддержка различных источников данных
- Простота освоения и использования
- Огромный накопленный опыт применения в десятках стран
- Сопутствующие продукты обеспечивают работу с БД и текстами
- Возможность расширения функциональности через дополнительные модули

Недостатки:

- Затруднена визуализация очень больших графов



Окружение IBM i2 Analyst's Notebook

- IBM i2 iBase – продукт для построения баз данных «с нуля»
- IBM i2 iBridge – продукт для обеспечения доступа аналитика к имеющимся БД под управлением различных СУБД
- IBM i2 TextChart – инструмент для эффективной работы с текстовыми документами в среде Analyst's Notebook

Спасибо за внимание!

НТЦ «Вулкан»
105318 г. Москва, ул. Ибрагимова, д. 31
тел. +7 (495) 663-95-16
info@ntc-vulkan.ru