ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

ПРИМЕНЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АНАЛИЗА БОЛЬШИХ МАССИВОВ ДАННЫХ, СОДЕРЖАЩИХСЯ В РАЗЛИЧНЫХ ИНФОРМАЦИОННЫХ РЕСУРСАХ, С ЦЕЛЬЮ ВЫЯВЛЕНИЯ ОПЕРАТИВНО-ЗНАЧИМОЙ ИНФОРМАЦИИ

Методические рекомендации

Воронеж – 2020

УДК 004.9
ББК 32.973.26-018.2

Мещерякова Т. В. ПРИМЕНЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АНАЛИЗА БОЛЬШИХ МАССИВОВ ДАННЫХ, СОДЕРЖАЩИХСЯ В РАЗЛИЧНЫХ ИНФОРМАЦИОННЫХ РЕСУРСАХ, С ЦЕЛЬЮ ВЫЯВЛЕНИЯ ОПЕРАТИВНО-ЗНАЧИМОЙ ИНФОРМАЦИИ / Т. В. Мещерякова и [др.]. – Воронеж : Воронежский институт МВД России, 2020. – 93 с.

В методических рекомендациях рассматриваются вопросы анализа информации для целей расследования преступлений с использованием современных информационных технологий, рассмотрен программный интерфейс системы аналитической обработки оперативной информации «Виток-3Х», приведены основные методы обработки оперативной информации в специальных аналитических системах.

Работа предназначена для использования в практической деятельности сотрудников заинтересованных подразделений МВД России в части осуществления поиска, анализа и сопоставления больших массивов данных, содержащихся в различных информационных ресурсах.

ББК 32.973.26-018.2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В наши дни наблюдается интенсивное увеличение объема и сложности циркулирующей в обществе информации, необходимость профессионального подхода к ее анализу выдвигает требования к подготовке специалистов МВД России, имеющих соответствующие знания и умения в различных областях функционирования ОВД. Одним из современных направлений является анализ больших данных, и, как частный случай, применительно к ОВД – анализ детализаций использования мобильных устройств и анализ информации из социальных сетей.

В настоящее время социальные сети занимают особое место в повседневной жизни людей.Но наряду с положительными аспектами распространения, появились и отрицательные, например, распространение информации террористического и экстремистского характера, вовлечение молодежи в противоправную деятельность, склонение лиц к самоубийству.

Вследствие этого значительную актуальность приобретает мониторинг открытых источников информации, социальных сетей, информационных сайтов, новостных лент.

1. ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

1.1 Изучение интерфейса программного комплекса «Виток–3х» (lampyre rc 1.0)

Программный комплекс «Виток-3X» (Lampyre RC 1.0) предназначен для сбора и обработки информации, полученной в ходе специальных, поисковых и проверочных мероприятий. В частности, данный программный комплекс позволяет автоматизировать процессы загрузки в хранилище данных (ХД) информации, поступающей от внешних источников, с обеспечением ее последующей оперативной обработки и анализа.

В рассматриваемом программном комплексе предусмотрено эффективное и интуитивно понятное отображение загруженных данных, применение к ним аналитических задач поиска и отображение результатов работы.

Выполнение аналитических задач предусматривает отображение данных в виде:

- графического представления вершин с заданными атрибутами и связями между ними;
- географической карты с нанесенными на нее объектами, связями между ними и траекторией перемещения объектов (ГИС-карта);
- фиксированной таблицы данных с редактируемым пространством таблицы.

Достаточно важно отметить, что для эффективного функционирования программного комплекса «Виток-3X» (Lampyre RC 1.0) необходимы следующее программные средства:

- серверная операционная система Linux Ubuntu Server14.04 и выше;
- операционная система рабочей станции Windows 7 pro и выше;
- Microsoft Office 2010 и выше;
- программная платформа .NET Framework 4.5.1 и выше;
- среда выполнения web-служб NodeJS 7.2.1 и выше;
- провайдердоступакфайлам Excel - Microsoft Access Database Engine 2010 Redistributable;
- драйвер доступа psycopg2 2.6.2 к БД АПК Трал на базе PostgreSQL;
- СУБД InfluxDB 0.10 и выше;
- СУБД Apache Cassandra 3.3;
- СУБД MongoDB 3.2.5;
- СУБД Elastic 2.4.3.

Для запуска клиентского приложения рассматриваемого программного комплекса «Виток-3X» (Lampyre RC 1.0) необходимо по указанному преподавателем пути:

− запустить файл AS.UV.exe (Рисунок 1);

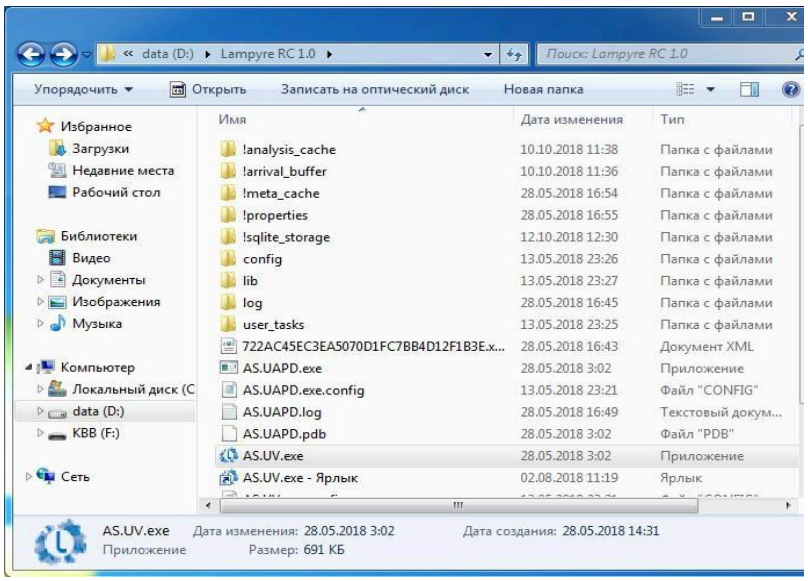


Рисунок 1 – Окно запуска клиентского приложения

− ввести логин и пароль пользователя, указанные преподавателем, нажать кнопку «Войти» (Рисунок 2);

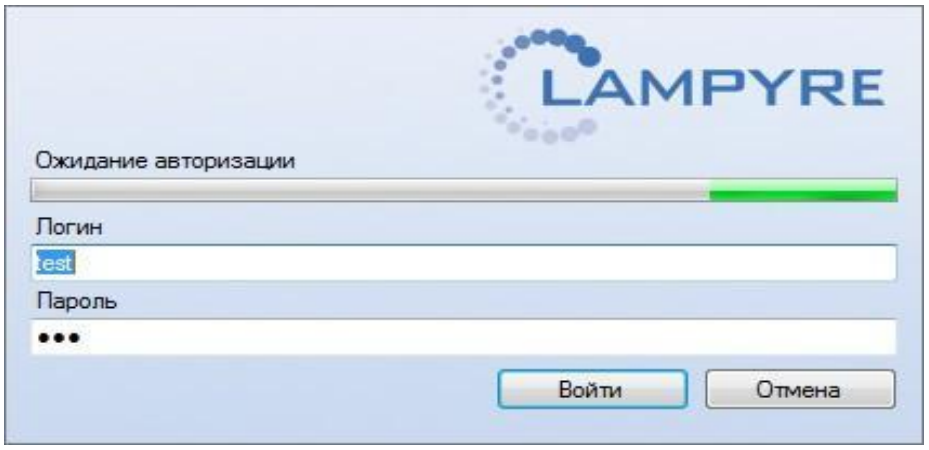


Рисунок 2 – Окно аутентификации пользователя

− дождаться отображения главного окна приложения (Рисунок 3).

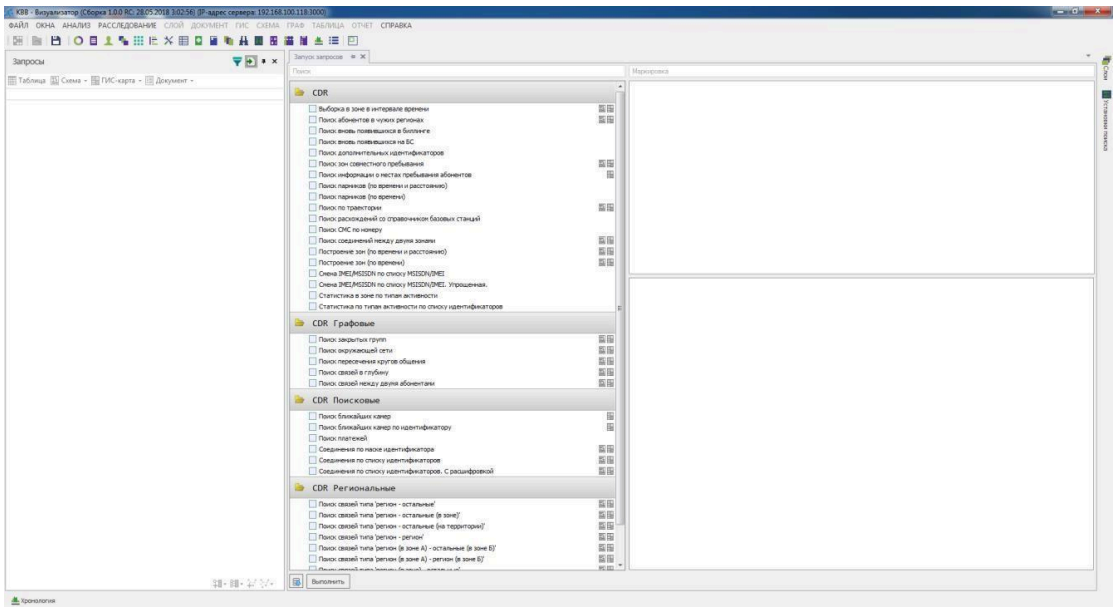


Рисунок 3 – Главное окно приложения

Для начала работы с программным комплексом необходимо создать расследование или открыть существующее. Инструменты для создания нового или открытия расследования доступны в меню «Файл» (Рисуноки 4, 5).

Достаточно важно заметить, что если уже открыто какое-либо расследование (пункт меню «Новое расследование» будет не активным), то необходимо его закрыть нажав кнопку «Закрыть расследование». Если же нет, то следует создать новое расследование. Для этого необходимо выбрать пункт меню «Новое расследование» или чтобы открыть существующее - нажмите «Файл» → «Открыть» и выберите его.

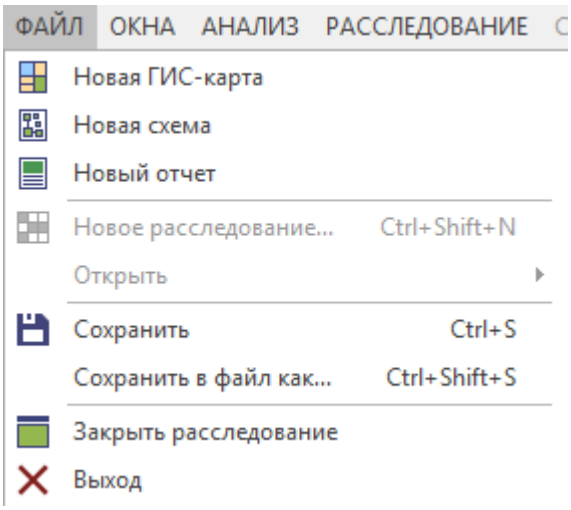


Рисунок 4 – Окно меню «Файл»

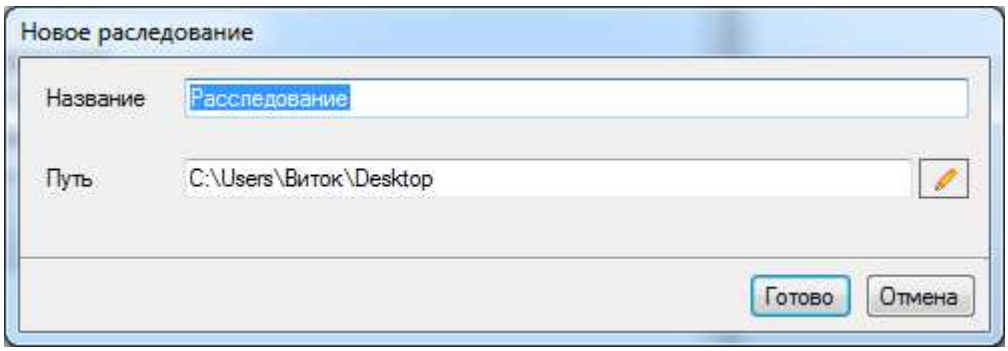


Рисунок 5 – Окно создания нового расследования

Для выполнения поисково-аналитических задач необходимо открыть какое-либо существующее расследование в соответствии с указаниями преподавателя, а также убедиться, что окно «Запросы» доступно в пользовательском интерфейсе (в левой части главного окна). Если оно не доступно, то его необходимо открыть через меню «Окна» (Рисунок 6-8).

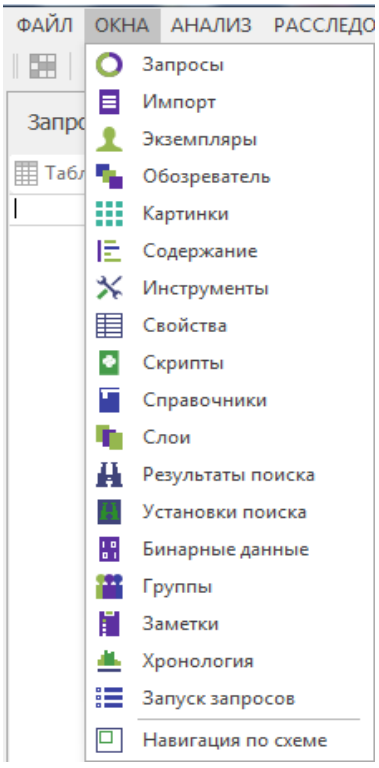


Рисунок 6 – Вкладка «Окна»

Кроме того, для запуска запросов можно воспользоваться комбинацией горячих клавиш Ctrl+Y.

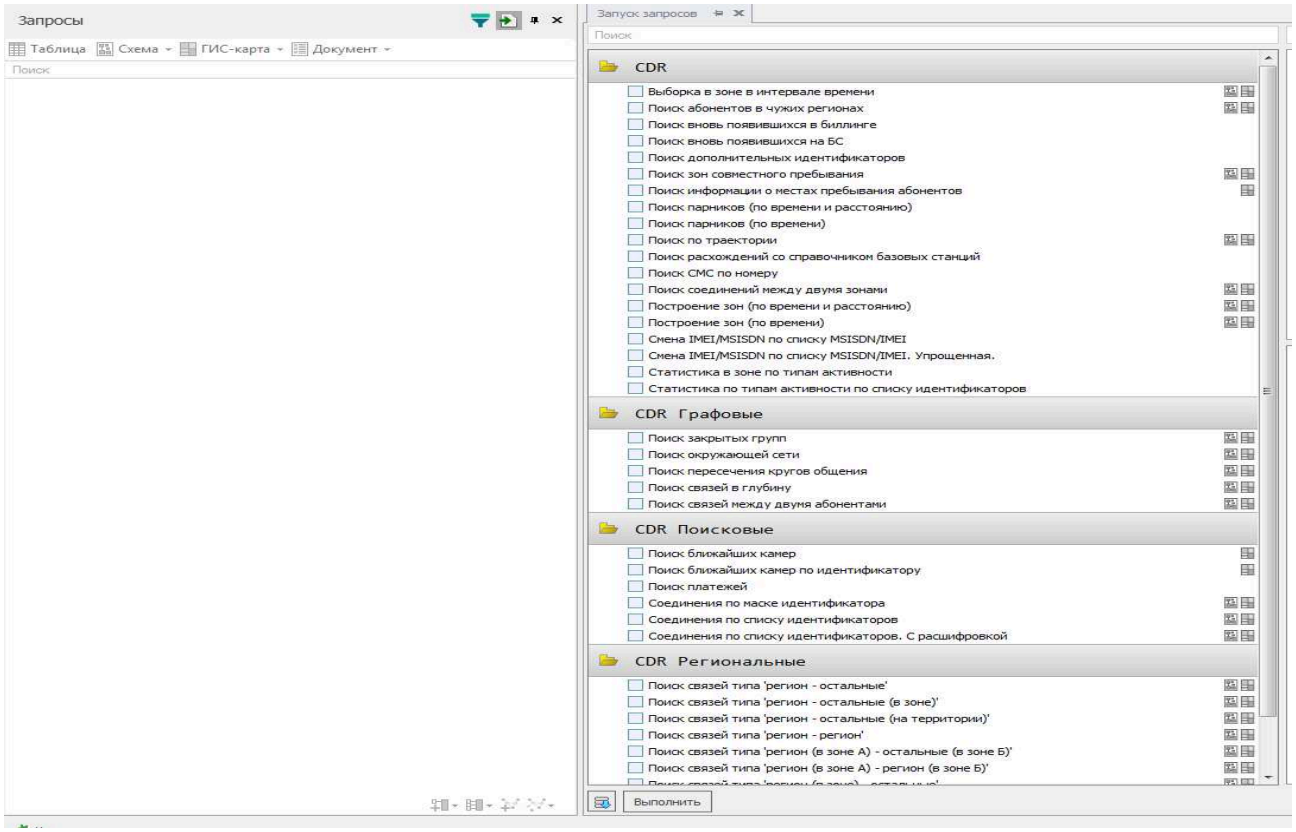


Рисунок 7 – Окно «Запросы»

Для запуска поискового запроса необходимо:

− выбрать поисковую методику в разделе «Поисковые» (установить флаг напротив выбранной методики);

− указать основные поисковые параметры для выбранной методики (временной интервал, тип, номер идентификатора и т.д.);

− во вкладке «Загрузки» выбрать нужные источники данных (установить флаг на необходимых источниках) например, в качестве источника можно взять данные биллинга, в которых осуществляется поиск;

− нажать на кнопку «Выполнить» в нижней части экрана (Рисунок 8).

Результат выполнения запроса отображается в окне «Монитор запросов», которое находится в левой части экрана рассматриваемого программного комплекса. Программный комплекс «Виток-3Х» позволяет различными способами анализировать полученный результат.

Для работы с результатами поискового запроса необходимо выделить интересующий запрос (Рисунок 9), появятся инструменты работы с запросом.

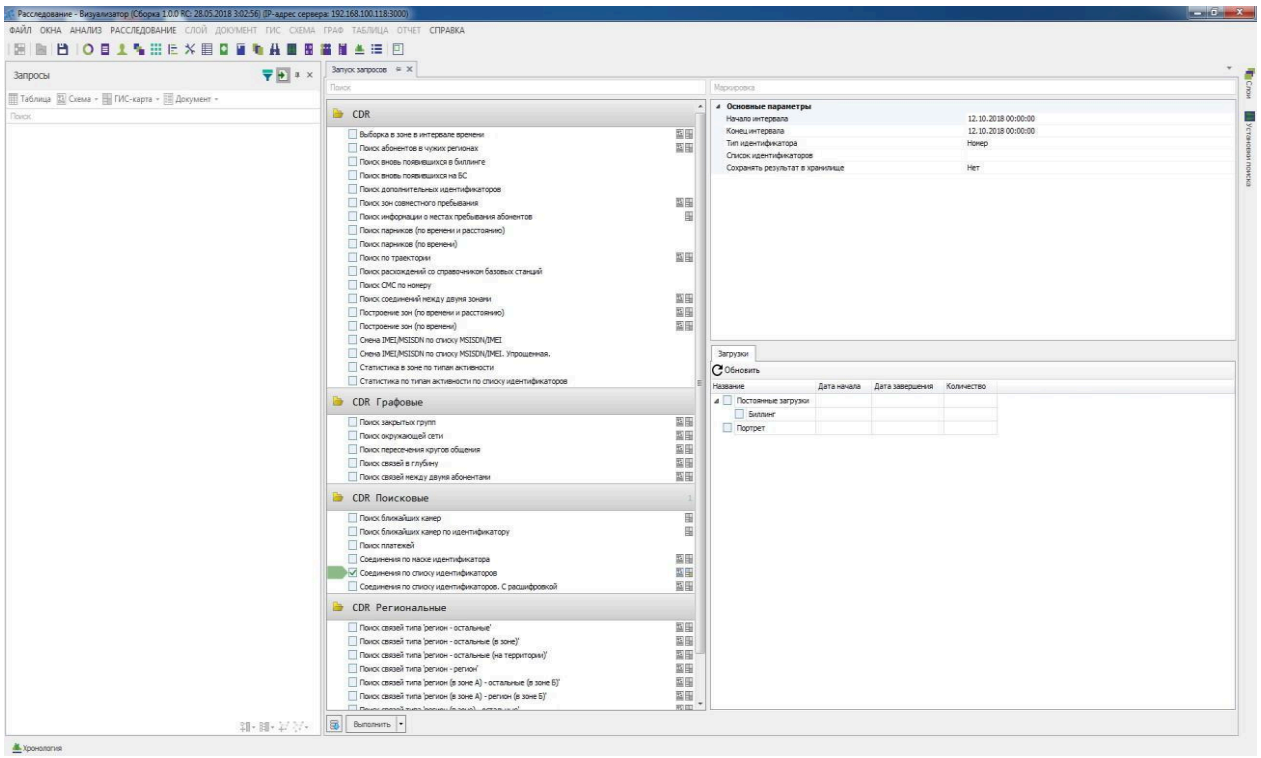


Рисунок 8 – Окно «Запуск запросов»

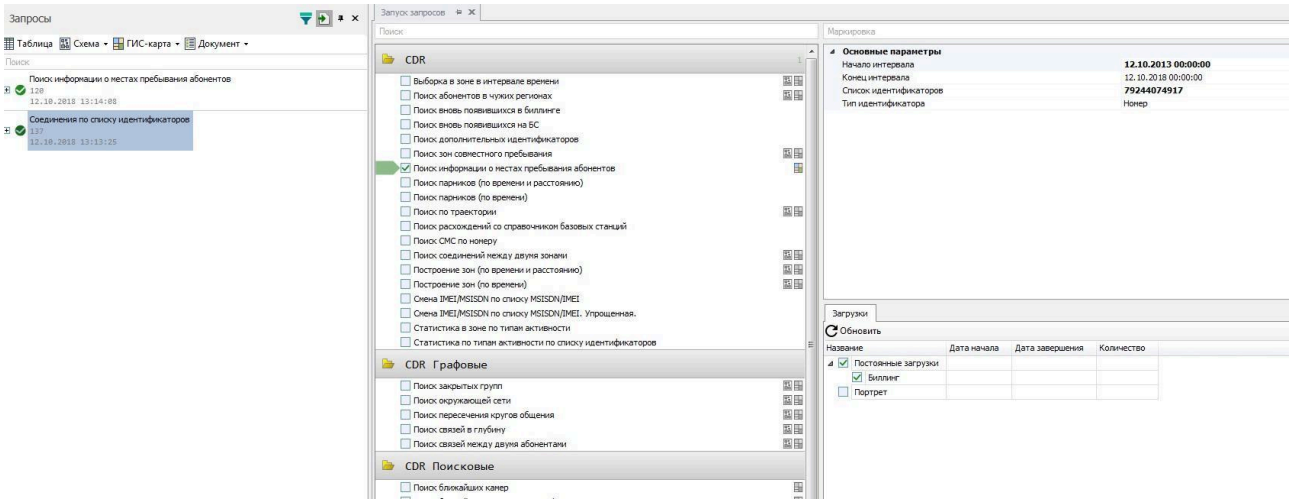
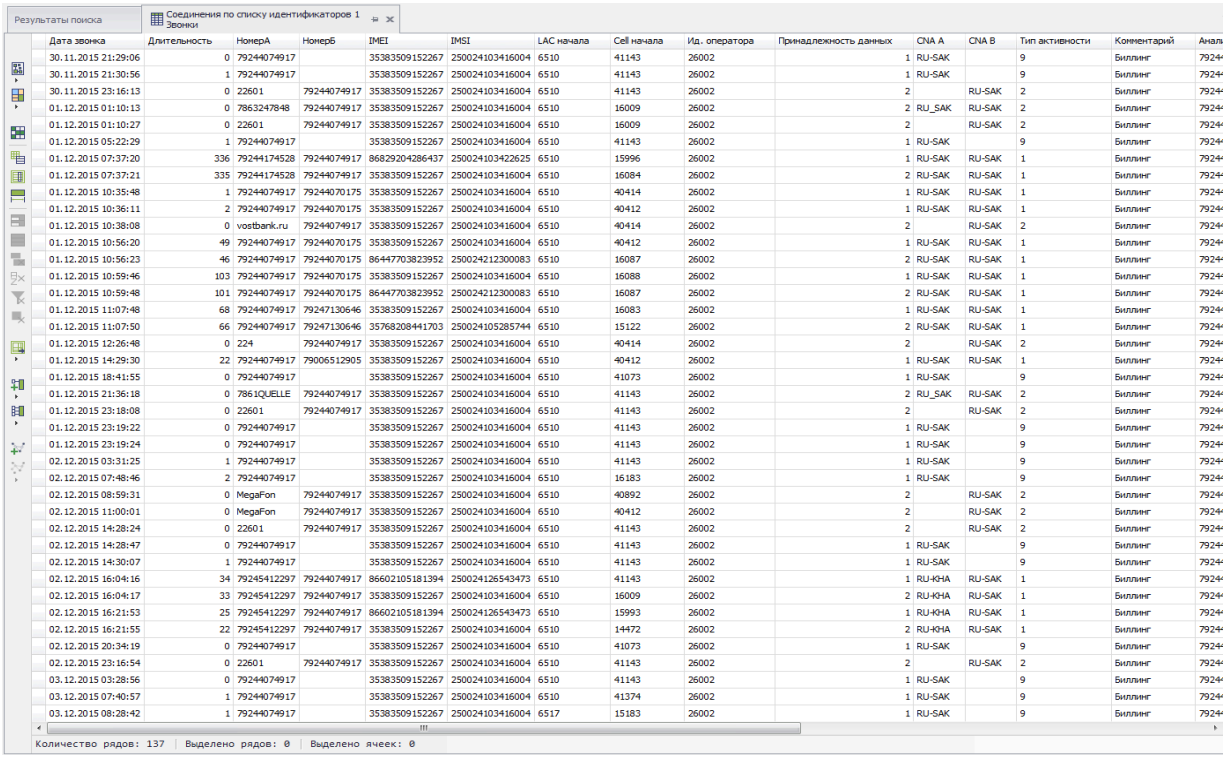


Рисунок 9 – Инструменты работы с поисковым запросом

Результаты выполнения поискового запроса возможно отображать в виде таблиц, схем, связей, на ГИС-карте и документом.

Информация о результатах поискового запроса, представленная в виде таблицы, отображена на рисунке 10.



Результаты поиска | Соединения по списку идентификаторов 1 Звонки

Дата звонка	Длительность	НомерА	НомерБ	IMEI	IMSI	LAC начала	Cell начала	Ид. оператора	Принадлежность данных	CNA A	CNA B	Тип активности	Комментарий	Анал
30.11.2015 21:29:06	0	79244074917		35383509152267	250024103416004	6510	41143	26002	1	RU-SAK		9	Биллинг	7924
30.11.2015 21:30:56	1	79244074917		35383509152267	250024103416004	6510	41143	26002	1	RU-SAK		9	Биллинг	7924
30.11.2015 23:16:13	0	22601	79244074917	35383509152267	250024103416004	6510	41143	26002	2		RU-SAK	2	Биллинг	7924
01.12.2015 01:10:13	0	7863247848	79244074917	35383509152267	250024103416004	6510	16009	26002	2	RU_SAK	RU-SAK	2	Биллинг	7924
01.12.2015 01:10:27	0	22601	79244074917	35383509152267	250024103416004	6510	16009	26002	2		RU-SAK	2	Биллинг	7924
01.12.2015 05:22:29	1	79244074917		35383509152267	250024103416004	6510	41143	26002	1	RU-SAK		9	Биллинг	7924
01.12.2015 07:37:20	336	79244174528	79244074917	86829204286437	250024103422625	6510	15996	26002	1	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 07:37:21	335	79244174528	79244074917	35383509152267	250024103416004	6510	16084	26002	2	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 10:35:48	1	79244074917	79244070175	35383509152267	250024103416004	6510	40414	26002	1	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 10:36:11	2	79244074917	79244070175	35383509152267	250024103416004	6510	40412	26002	1	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 10:38:08	0	vostbank.ru	79244074917	35383509152267	250024103416004	6510	40414	26002	2		RU-SAK	2	Биллинг	7924
01.12.2015 10:56:20	49	79244074917	79244070175	35383509152267	250024103416004	6510	40412	26002	1	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 10:56:23	46	79244074917	79244070175	86447703823952	250024212300083	6510	16087	26002	2	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 10:59:46	103	79244074917	79244070175	35383509152267	250024103416004	6510	16088	26002	1	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 10:59:48	101	79244074917	79244070175	86447703823952	250024212300083	6510	16087	26002	2	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 11:07:48	68	79244074917	79247130646	35383509152267	250024103416004	6510	16083	26002	1	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 11:07:50	66	79244074917	79247130646	35768208441703	250024105285744	6510	15122	26002	2	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 12:26:48	0	224	79244074917	35383509152267	250024103416004	6510	40414	26002	2		RU-SAK	2	Биллинг	7924
01.12.2015 14:29:30	22	79244074917	79006512905	35383509152267	250024103416004	6510	40412	26002	1	RU-SAK	RU-SAK	1	Биллинг	7924
01.12.2015 18:41:55	0	79244074917		35383509152267	250024103416004	6510	41073	26002	1	RU-SAK		9	Биллинг	7924
01.12.2015 21:36:18	0	7861QUELLE	79244074917	35383509152267	250024103416004	6510	41143	26002	2	RU_SAK	RU-SAK	2	Биллинг	7924
01.12.2015 23:18:08	0	22601	79244074917	35383509152267	250024103416004	6510	41143	26002	2		RU-SAK	2	Биллинг	7924
01.12.2015 23:19:22	0	79244074917		35383509152267	250024103416004	6510	41143	26002	1	RU-SAK		9	Биллинг	7924
01.12.2015 23:19:24	0	79244074917		35383509152267	250024103416004	6510	41143	26002	1	RU-SAK		9	Биллинг	7924
02.12.2015 03:31:25	1	79244074917		35383509152267	250024103416004	6510	41143	26002	1	RU-SAK		9	Биллинг	7924
02.12.2015 07:48:46	2	79244074917		35383509152267	250024103416004	6510	16183	26002	1	RU-SAK		9	Биллинг	7924
02.12.2015 08:59:31	0	MegaFon	79244074917	35383509152267	250024103416004	6510	40892	26002	2		RU-SAK	2	Биллинг	7924
02.12.2015 11:00:01	0	MegaFon	79244074917	35383509152267	250024103416004	6510	40412	26002	2		RU-SAK	2	Биллинг	7924
02.12.2015 14:28:24	0	22601	79244074917	35383509152267	250024103416004	6510	41143	26002	2		RU-SAK	2	Биллинг	7924
02.12.2015 14:28:47	0	79244074917		35383509152267	250024103416004	6510	41143	26002	1	RU-SAK		9	Биллинг	7924
02.12.2015 14:30:07	1	79244074917		35383509152267	250024103416004	6510	41143	26002	1	RU-SAK		9	Биллинг	7924
02.12.2015 16:04:16	34	79245412297	79244074917	86602105181394	250024126543473	6510	41143	26002	1	RU-KHA	RU-SAK	1	Биллинг	7924
02.12.2015 16:04:17	33	79245412297	79244074917	35383509152267	250024103416004	6510	16009	26002	2	RU-KHA	RU-SAK	1	Биллинг	7924
02.12.2015 16:21:53	25	79245412297	79244074917	86602105181394	250024126543473	6510	15993	26002	1	RU-KHA	RU-SAK	1	Биллинг	7924
02.12.2015 16:21:55	22	79245412297	79244074917	35383509152267	250024103416004	6510	14472	26002	2	RU-KHA	RU-SAK	1	Биллинг	7924
02.12.2015 20:34:19	0	79244074917		35383509152267	250024103416004	6510	41073	26002	1	RU-SAK		9	Биллинг	7924
02.12.2015 23:16:54	0	22601	79244074917	35383509152267	250024103416004	6510	41143	26002	2		RU-SAK	2	Биллинг	7924
03.12.2015 03:28:56	0	79244074917		35383509152267	250024103416004	6510	41143	26002	1	RU-SAK		9	Биллинг	7924
03.12.2015 07:40:57	1	79244074917		35383509152267	250024103416004	6510	41374	26002	1	RU-SAK		9	Биллинг	7924
03.12.2015 08:28:42	1	79244074917		35383509152267	250024103416004	6517	15183	26002	1	RU-SAK		9	Биллинг	7924

Количество рядов: 137 | Выделено рядов: 0 | Выделено ячеек: 0

Рисунок 10 – Результаты поискового запроса, представленные в виде таблицы

Информация о результатах поискового запроса, представленная в виде схемы отображена на рисунке 11.

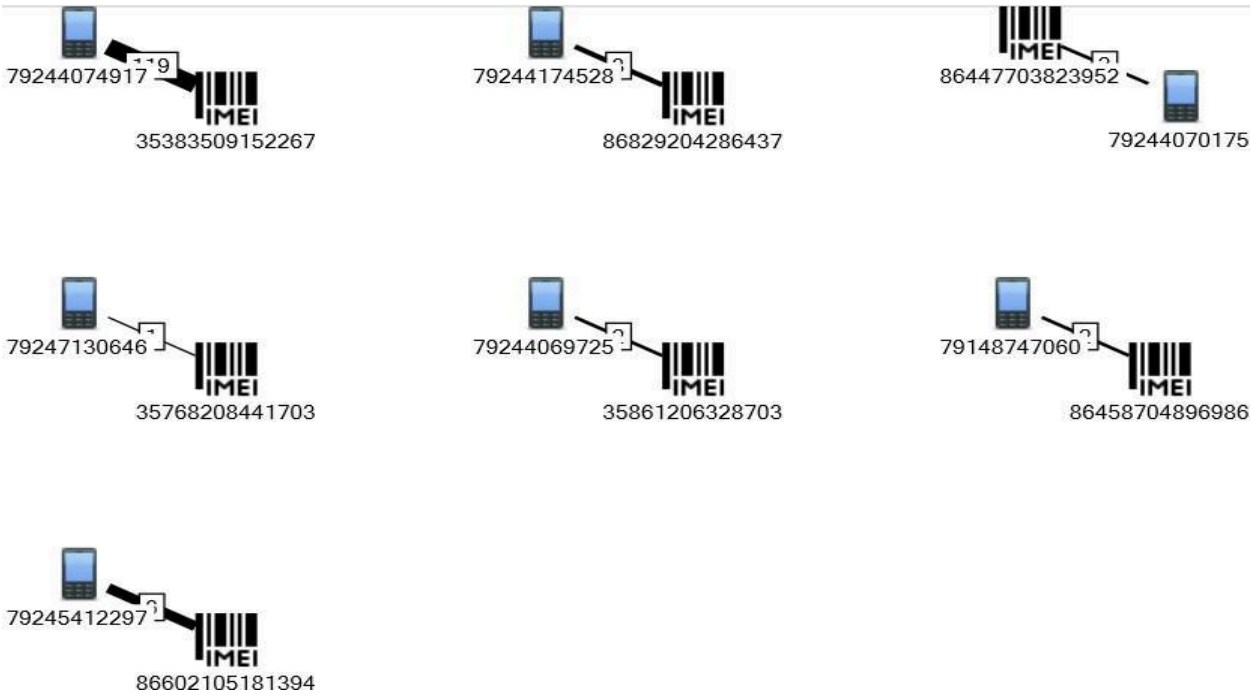


Рисунок 11 – Результаты поискового запроса, представленные в виде схемы

Информация о результатах поискового запроса, представленная в виде карты отображена на рисунке 12.

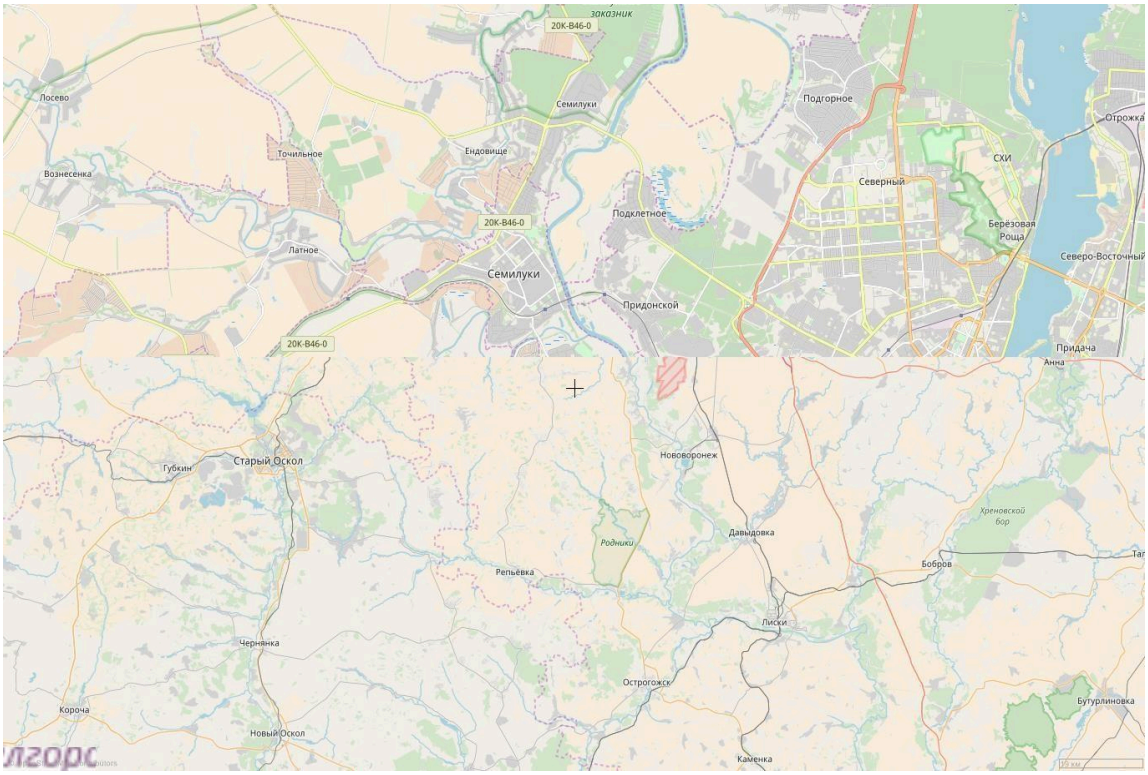


Рисунок 12 – Результаты поискового запроса, представленные в виде ГИС- карты

Информация о результатах поискового запроса, представленная в виде документа отображена на рисунке 13.

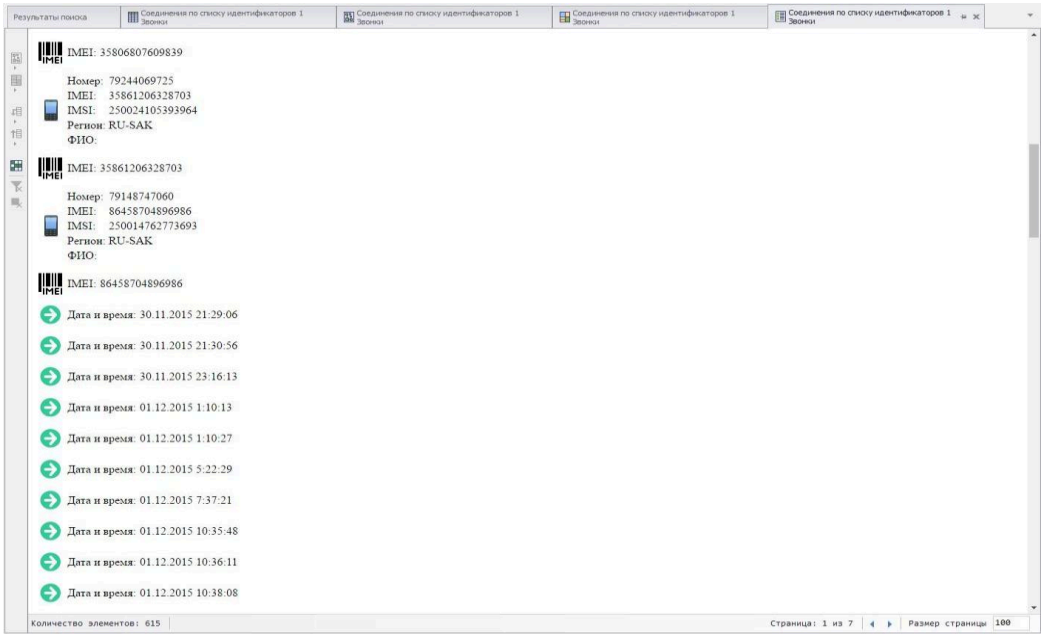
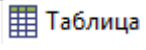


Рисунок 13 – Результаты поискового запроса, представленные в виде документа

1.2. Работа программного комплекса «виток – 3х» с результатами поисковых запросов в виде таблиц

Для отображения результата поисковой задачи в табличном виде

необходимо в окне «Монитор запросов» выбрать интересующий результат и затем нажать кнопку «Таблица» 

. Представляется целесообразным рассмотреть основные способы поиска и фильтрации данных в таблицах.

При работе с таблицами (Рисунок 14) возможны следующие варианты фильтрации:

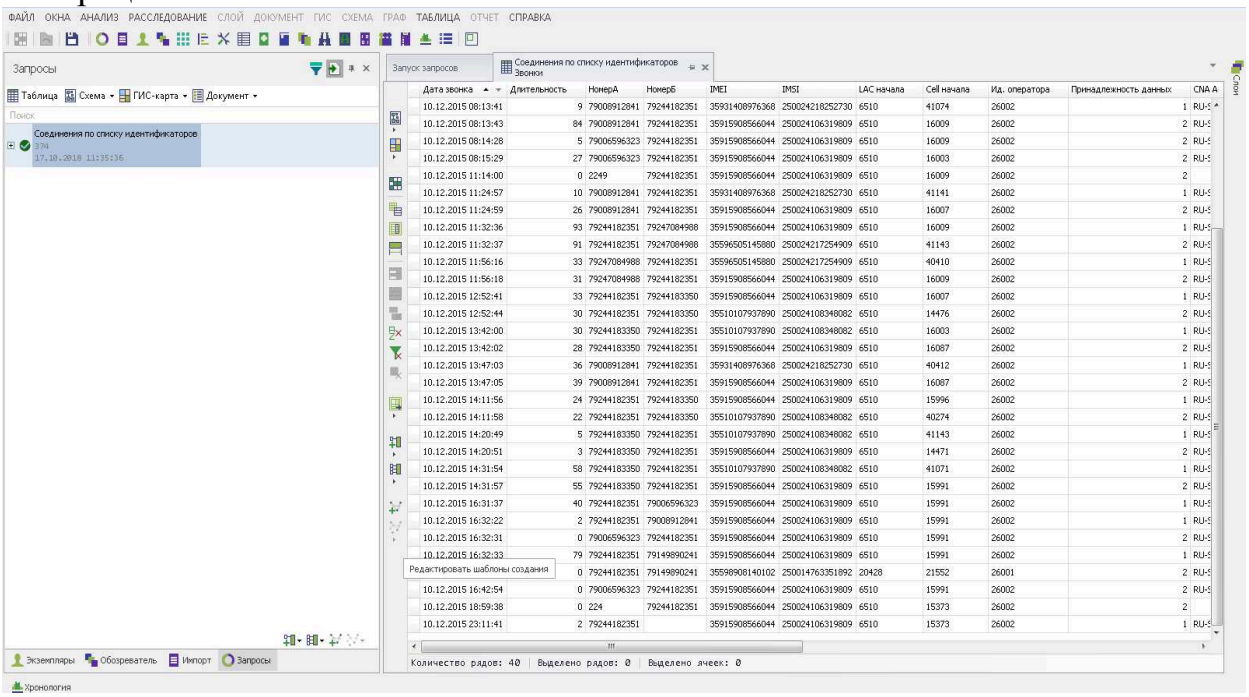


Рисунок 14 – Отображение результата в виде таблицы

1. С помощью фильтра внутри столбца.

Для примера используем столбец таблицы «Дата звонка» (Рисунок 15).

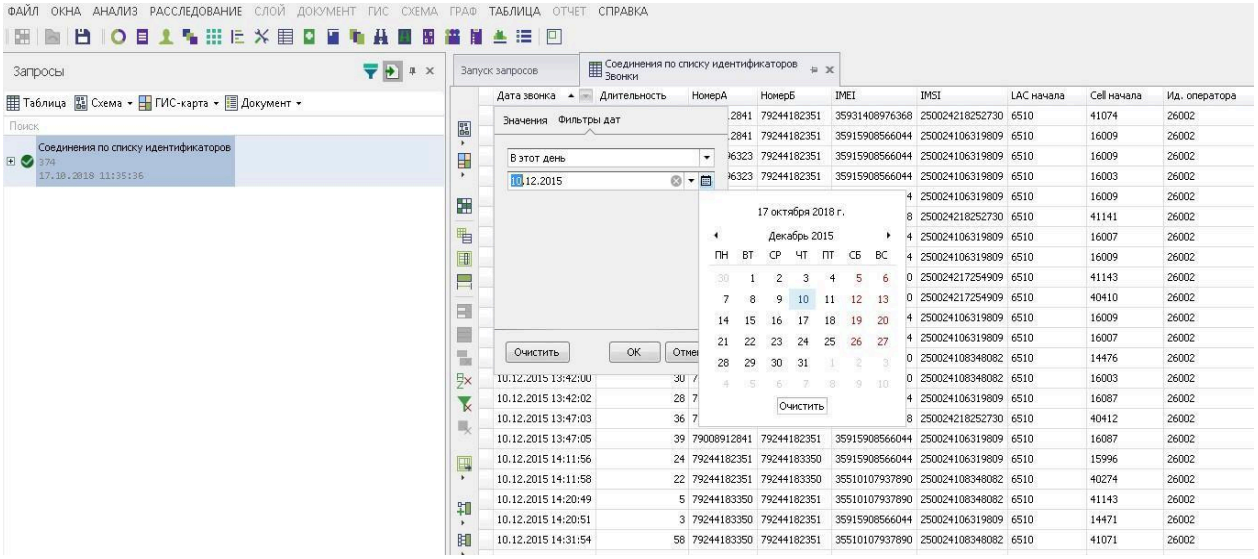
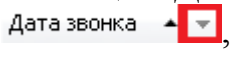


Рисунок 15 – Фильтрация данных столбца таблицы «Дата звонка»

Для фильтрации данных в столбце «Дата звонка» в его правой части необходимо нажать пиктограмму 

, после чего откроется окно для обработки данных рассматриваемого столбца, как представлено на

вышеприведенном рисунке.

Важно отметить, что поиск и фильтрация данных в столбце «Дата звонка» осуществляется с помощью двух параметров: «Значения» и «Фильтры дат», каждый из которых имеет свои критерии (Рисунок 16).

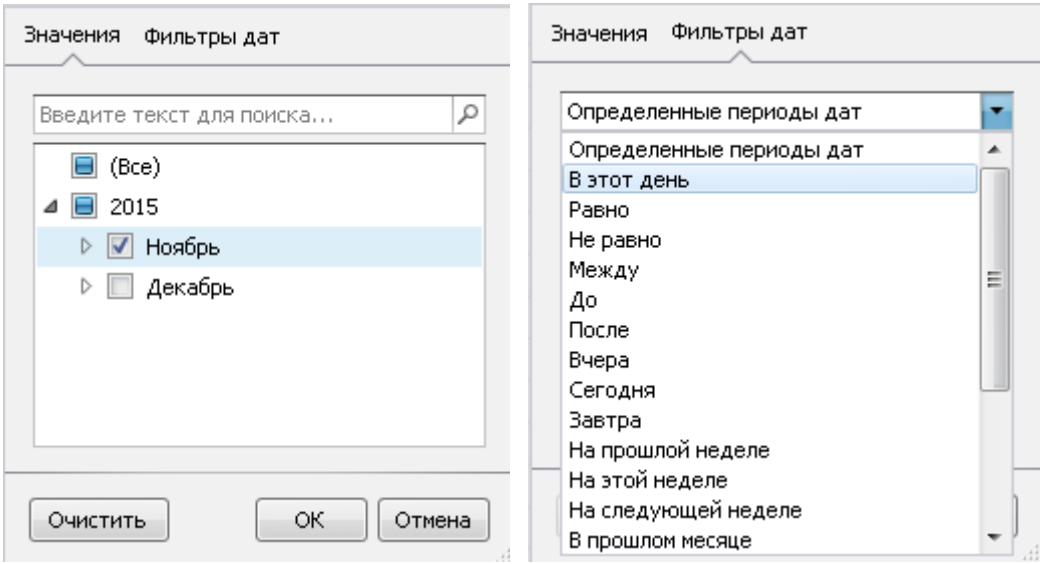


Рисунок 16 – Параметры фильтра столбца таблицы «Дата звонка»

Аналогичным образом можно осуществить фильтрацию внутри других столбцов: выделить столбец и нажать на галочку внутри описательной части столбца. В выпадающем списке выбрать одно из значений, по которому будет произведена фильтрация.

2. Выполнение группировки по столбцам (фильтрация через контекстное меню таблицы).

Для того чтобы произвести типовые действия над столбцами и строками необходимо в заголовке столбца правой клавишей мыши выбрать контекстное меню. При этом необходимо выделить заголовок любого столбца таблицы и нажать правую кнопку мыши. В появившемся контекстном меню выбрать пункт «Показать область группировки» (Рисунок 17).

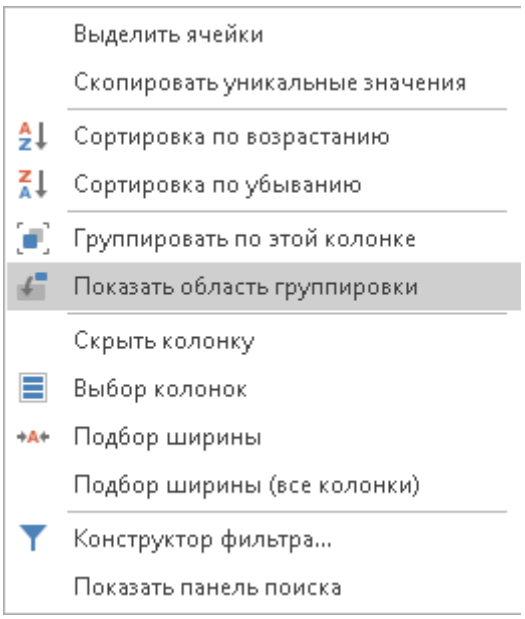


Рисунок 17 – Область группировки

Далее в появившейся верхней части экрана области группировки добавить интересующие заголовки столбцов. Левой клавишей мыши необходимо нажать на заголовке столбца и, не отпуская клавиши мыши, перетащить его в темно-серую область группировки. Возможно группировать по нескольким столбцам.

На представленном ниже рисунке 18 данные исходной таблицы сгруппированы по следующим столбцам:

Дата звонка.

Номер А (кто звонил).

Номер Б (кому звонили).

IMEI.

IMSI.

Контакт целевого идентификатора

Следует заметить, что можно удалить или добавить в область группировки данные из любого столбца. Для удаления столбца из области группировки необходимо его выделить, нажать правую кнопку мыши и выбрать пункт меню «Разгруппировать».

При этом данные в таблице будут перегруппированы без учета информации удаленного столбца. Если разгруппировать все заголовки столбцов, присутствующих в области группировки, то таблица выполненного запроса примет первоначальный вид.

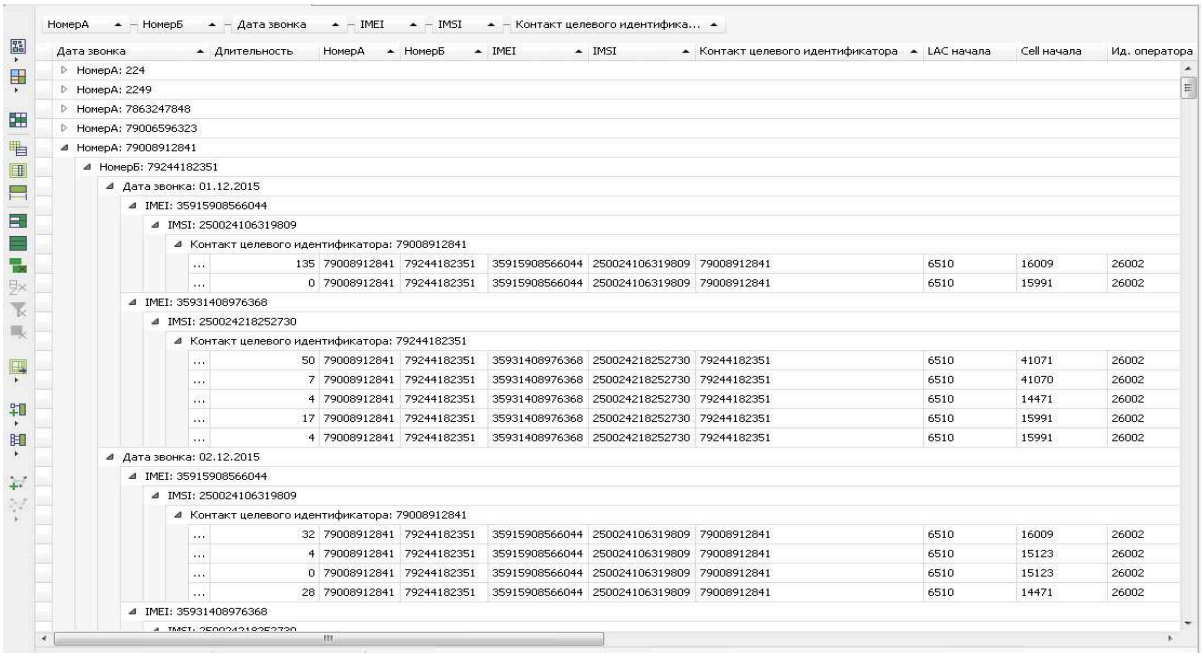
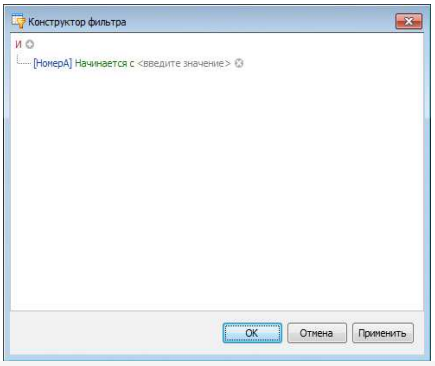


Рисунок 18 – Выполнение группировки по столбцам

3. Фильтрация с помощью конструктора фильтра.

Для этого в контекстном меню таблицы необходимо вызвать пункт «Конструктор фильтра» для настройки сложного условия фильтрации по значениям в таблице (Рисунок 18).



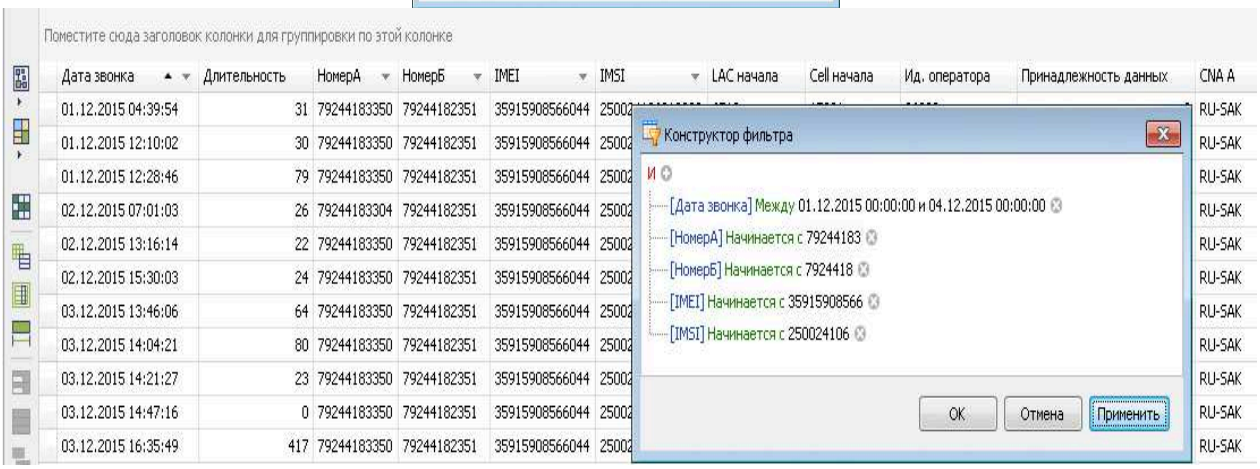


Рисунок 19 - Фильтрация с помощью конструктора фильтра

Для настройки сложного условия фильтрации следует нажать на знак+, рядом с буквой И, появится критерий [дата звонка], нажав на который выбираем любой необходимый заголовок столбца. Следует заметить, что для корректного отображения данных для критерия [дата звонка] необходимо выбирать условие «между» и указывать два временных интервала (Рисунок 19).

Для выполнения различных операций в таблицах также целесообразно использовать набор инструментов для работы с таблицей (Рисунок 20) (доступен сразу после отображения результатов поискового запроса в табличном виде), который включает:

Рисунок 20 – Инструменты работы с таблицей

	показать расследование (при работе со схемой связи);
	выбор столбцов (колонок), для настройки расположения столбцов в таблице
	скрыть пустые столбцы;
	подбор ширины столбцов (по содержимому);
	раскрыть/свернуть ранее сформированные группы по столбцам;
	разгруппировать группу столбцов;
	очистить сортировку (проведенную ранее через контекстное меню, по возрастанию/по убыванию;
	очистить фильтры;
	отменить выделение;
	экспорт таблицы в указанную пользователем локальную директорию;
	добавить, редактировать отображение связей (отображает связи между выбранными столбцами таблицы);
	добавить, редактировать шаблон создания (шаблон отображения информации).

Данные о каждом звонке или нескольких звонках (отображаемые в строке таблицы) возможно перенести на схему связей. Для этого следует выделить необходимые строки в таблице (удерживая левую клавишу мыши) и нажать

кнопку схема на панели инструментов (Рисунки 20, 21).

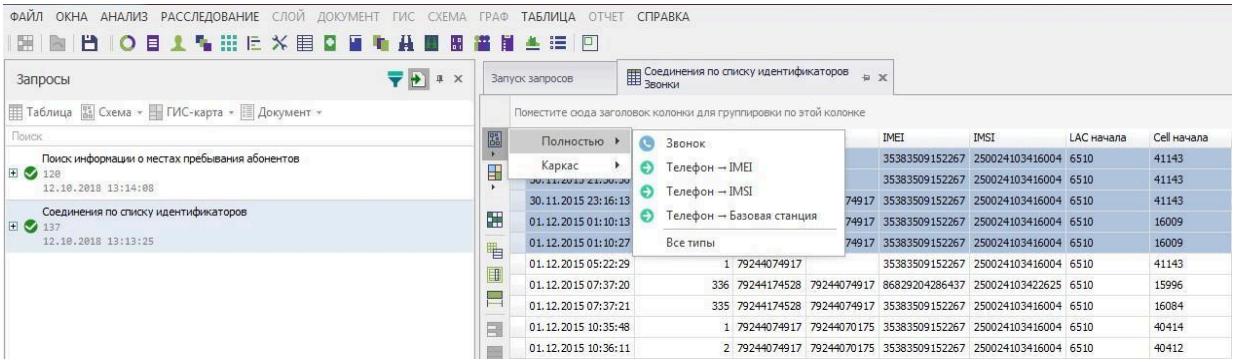


Рисунок 21 – Выделение результатов

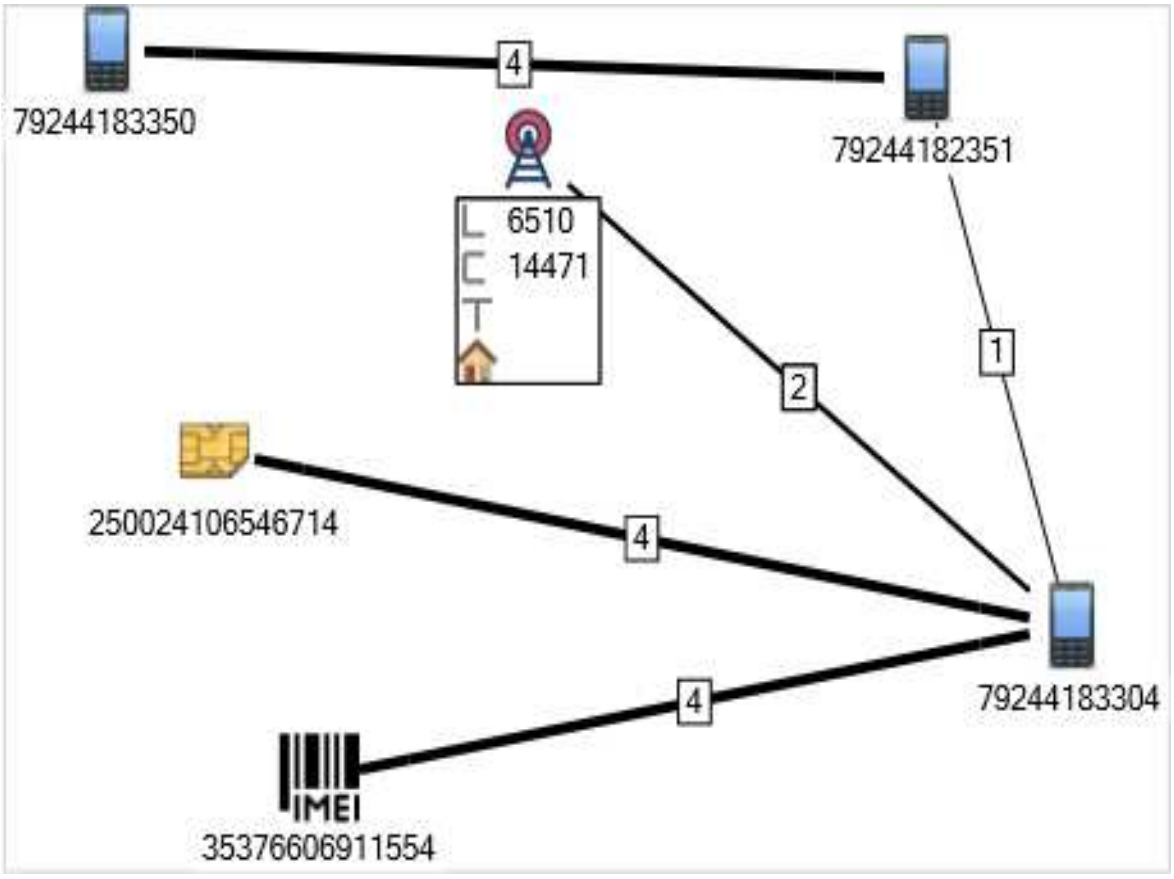


Рисунок 22 – Перенос строк таблицы на схему связей

Таким же образом осуществляется перенос данных о звонках на карту. Для этого следует выделить необходимые строки в таблице (удерживая левую клавишу мыши) и нажать кнопку «Карта» на панели инструментов (Рисунок 23).

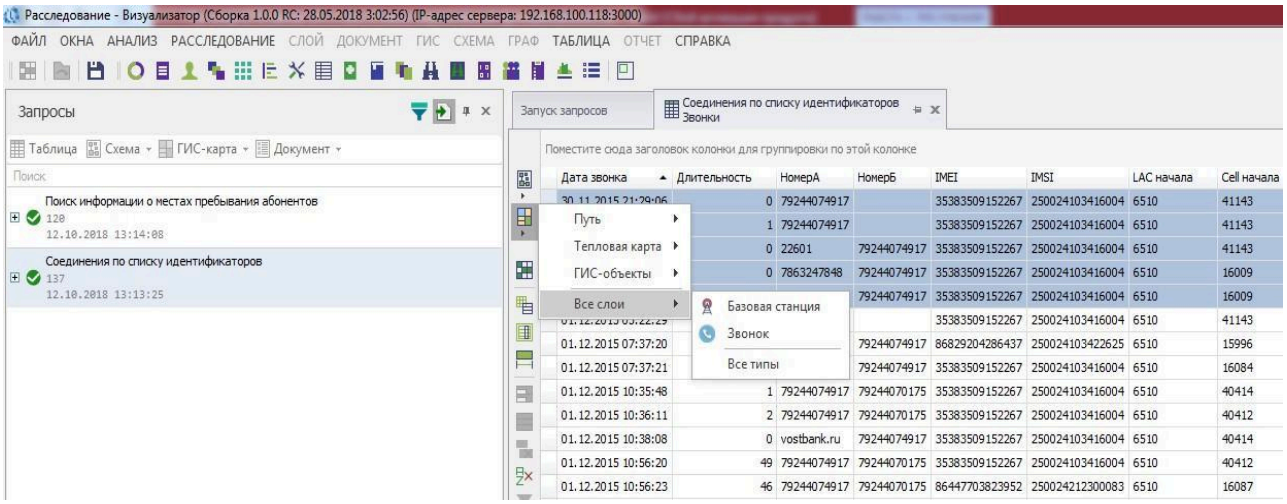


Рисунок 23 – Перенос строк таблицы на карту

Для сохранения результатов поискового запроса, представленных в виде таблицы, необходимо в панели инструментов в меню «ТАБЛИЦА» в разделе «Экспорт» выбрать необходимый формат сохранения поискового запроса (Рисунок 24).

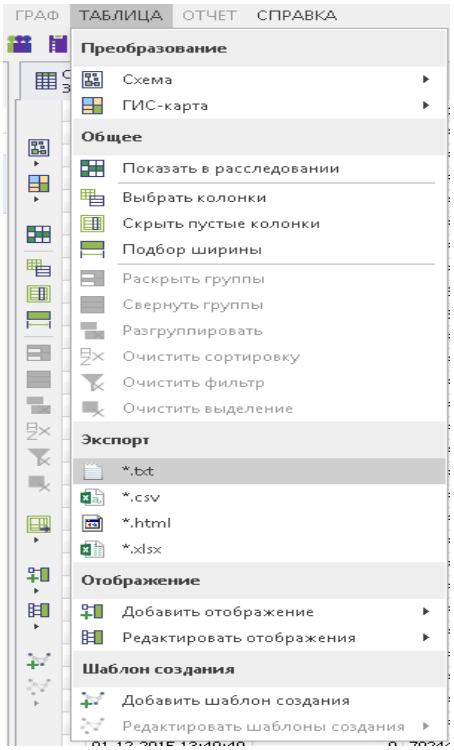


Рисунок 24 – Сохранение таблицы в разных форматах

1.3. Работа программного комплекса «Виток–3х» с результатами поисковых запросов в виде схем и промежуточных отчетов

Для отображения результата в виде схем необходимо в окне «Монитор запросов» выбрать интересующий результат и затем нажать кнопку «Схема»

(из выпадающего списка выбрать необходимый вариант схемы) (Рисунок 25).

В появившейся вкладке выбираем вариант отображения схемы связей:

- «Полностью» – отображает все связи между вершинами;
- «Каркас» – только по одной связи между вершинами.

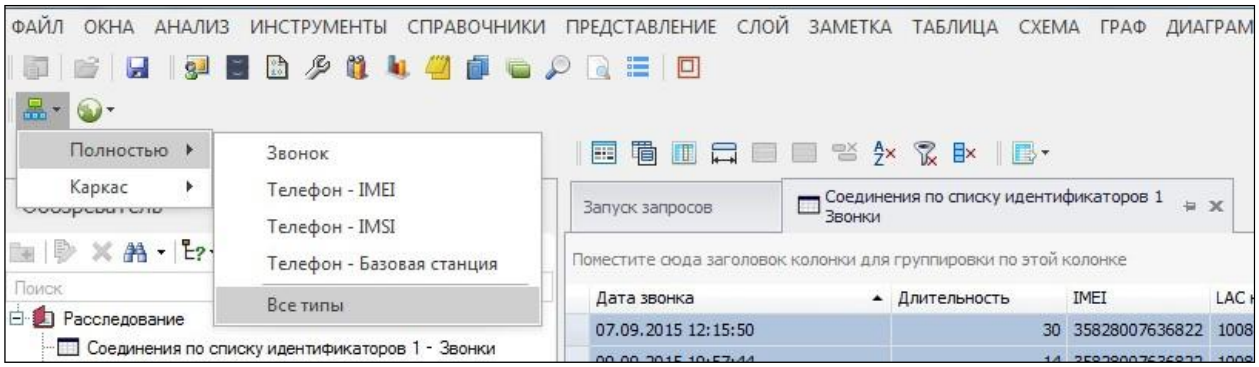


Рисунок 25 – Отображение результата в виде схемы

Вариант отображения схемы связей «Полностью» содержит следующие компоненты меню:

- звонок;
- телефон – IMEI;
- телефон – IMSI;
- телефон – Базовая станция;
- все типы.

При выборе нужного варианта строится схема связей (Рисунок 26).

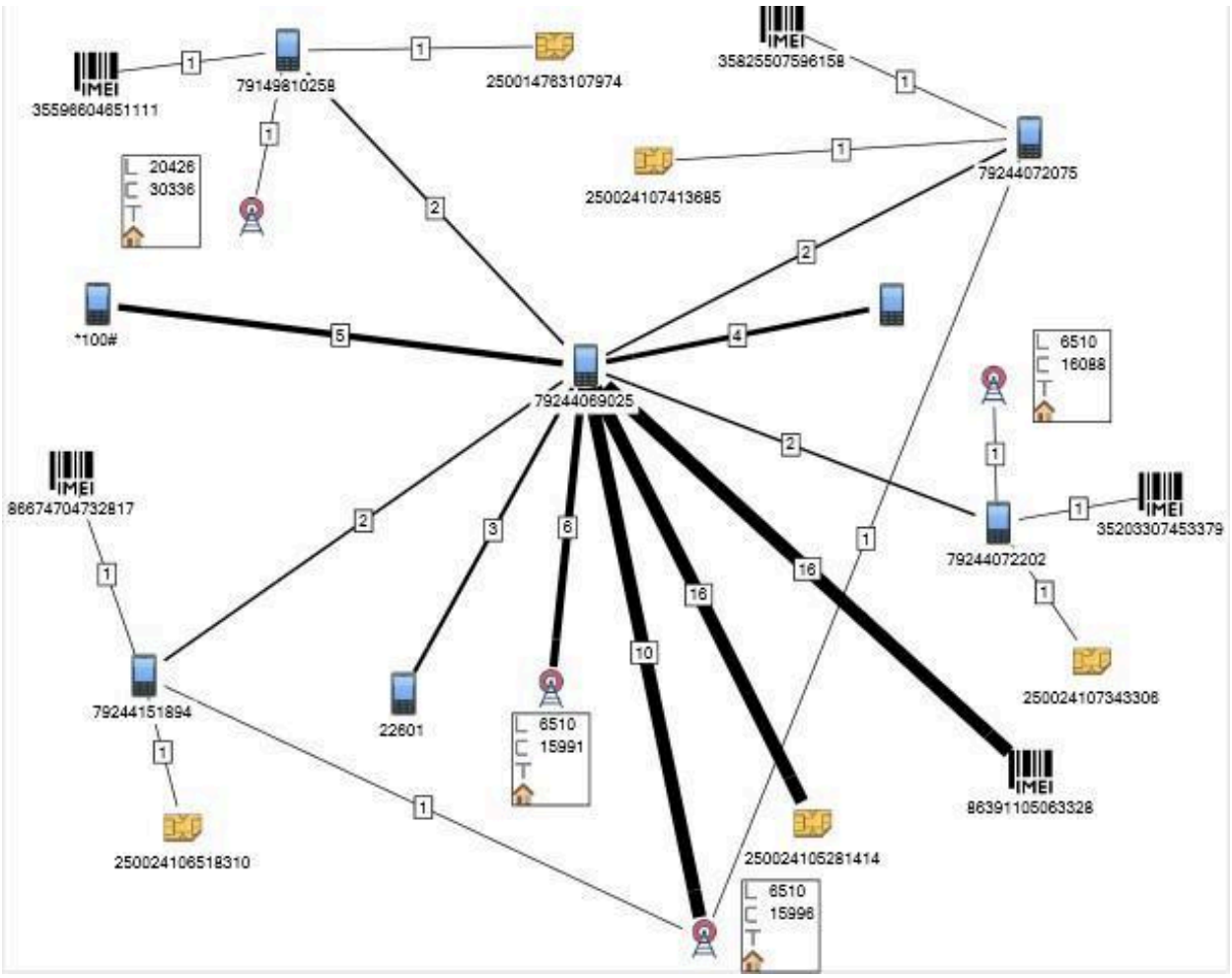


Рисунок 26 – Результаты выполнения поискового запроса в виде схемы связей

Для выбора типа авторазмещения элементов схемы связей, необходимо выбрать в контекстном меню схемы пункт «Авторазмещение» (правый клик мыши на пустом месте графа) (Рисунок 27).

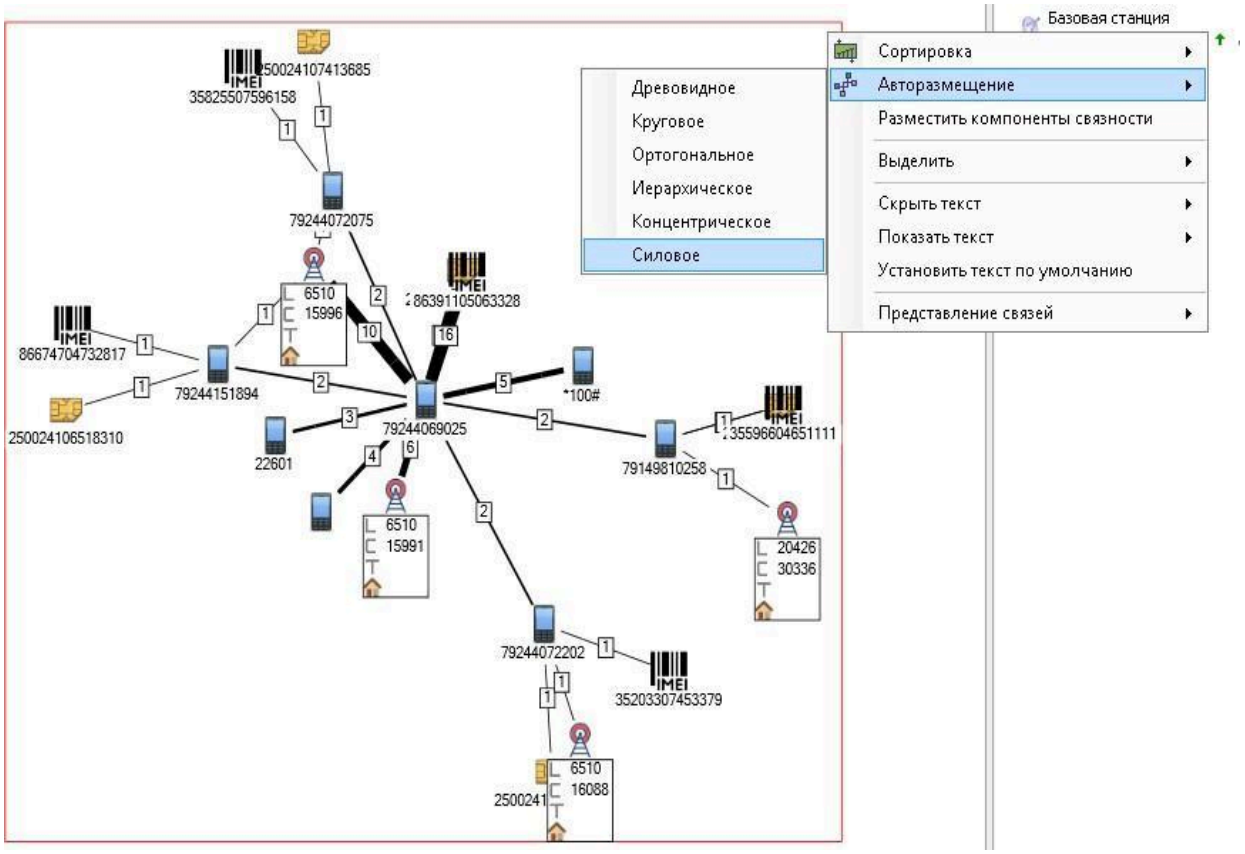


Рисунок 27 – Выбор типа авторазмещения элементов схемы связей

Как показано на представленном выше рисунке, авторазмещение схемы связей биллинговой информации может быть реализовано в программном комплексе «ВИТОК–3Х» такими способами, как:

1. Древовидное.
2. Круговое.
3. Ортогональное.
4. Иерархическое.
5. Концетрическое.
6. Силовое.

Представление данных поискового запроса в виде схемы связей позволяет также осуществлять процедуру поиска. Для реализации указанной процедуры поиска по схеме в данном программном обеспечении следует реализовать представленный ниже алгоритм.

Открыть окно «Результаты поиска» (главное меню – окна – результаты поиска) и нажать кнопку «Настройки» (Рисунок 28).

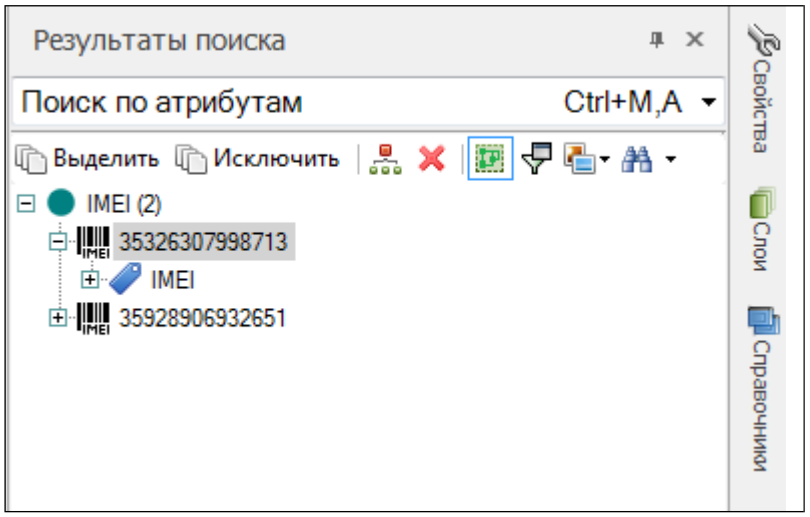


Рисунок 28 – Окно настройки поиска в результатах выполнения запроса

Следует заметить, что вызвать форму настройки поиска возможно и другим образом – через контекстное меню на схеме связей (Рисунок 29).

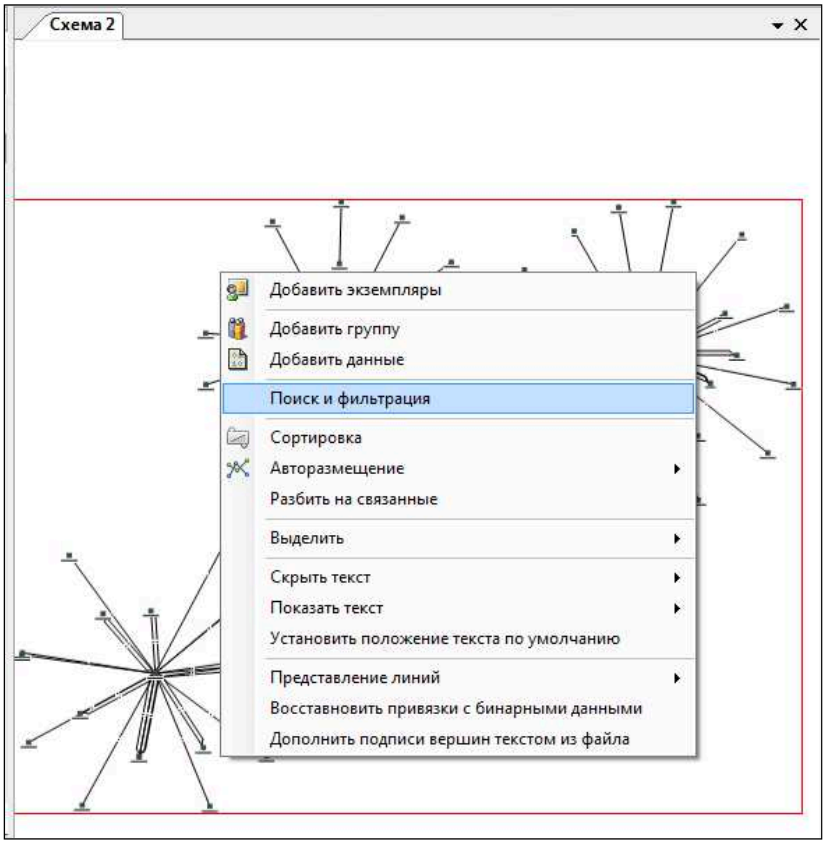


Рисунок 29 – Контекстное меню схемы связей

Кроме того, существует и третий способ, который использует сочетание горячих клавиш (Рисунок 30).

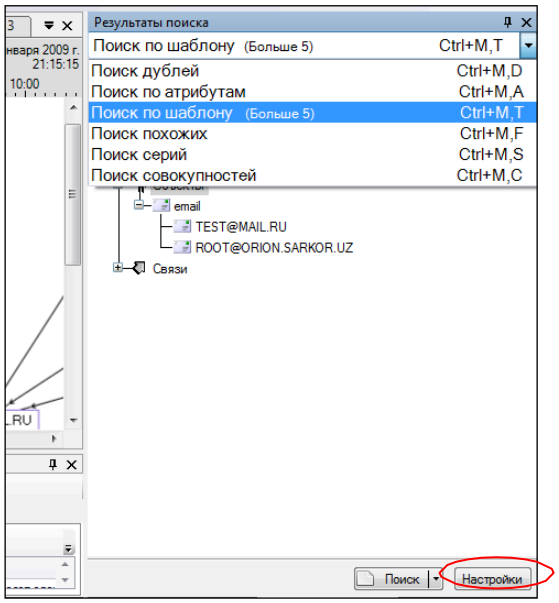


Рисунок 30 – Результаты поиска отображаются списком

При нажатии кнопки «Настройки» должно появиться окно, изображенное на рисунке 31. В данном окне производится задание параметров поиска. Переключение между различными типами поиска производится посредством

кнопки 

.

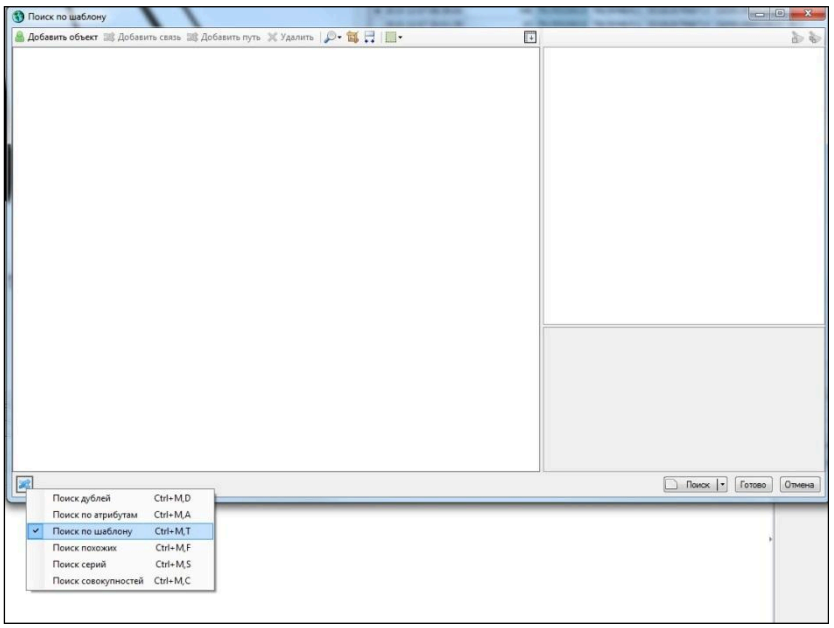


Рисунок 31 – Окно задания параметров поиска

Представляется целесообразным рассмотреть поиск элементов схемы связи на примере типа поиска «По шаблону» (Рисунок 31).

Для создания шаблона поиска необходимо добавить требуемое количество объектов путем нажатия кнопки «Добавить объект» (Рисунок 32).

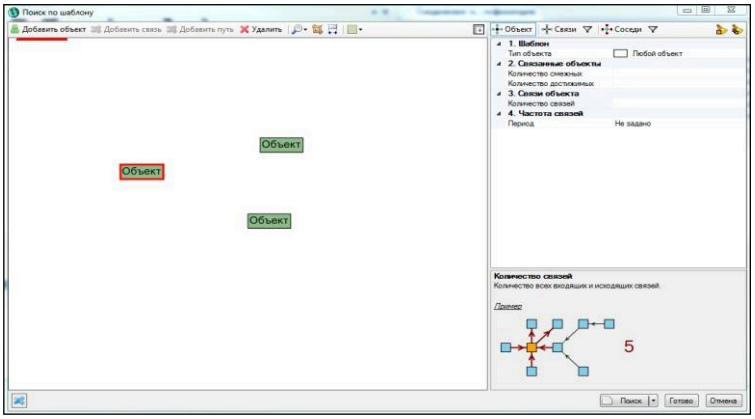


Рисунок 32 – Добавление объектов поиска

Для создания связей между объектами необходимо нажать кнопку «Добавить связь» и удерживая кнопку «Ctrl» выбрать требуемые для схемы связей объекты (Рисунок 33).

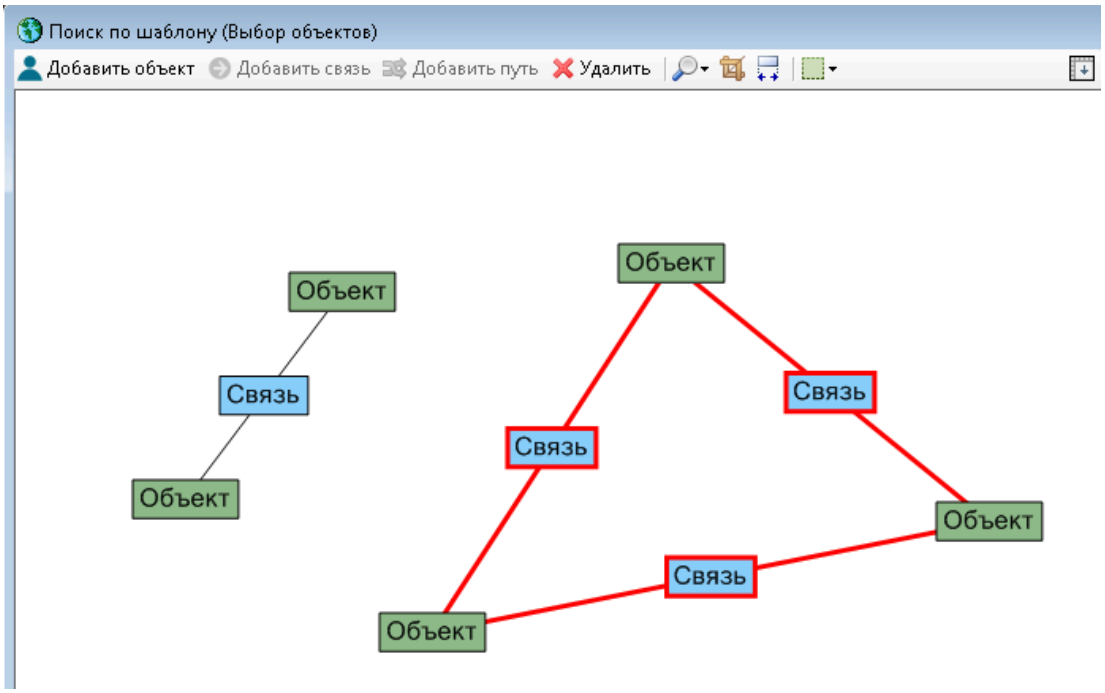


Рисунок 33 – Добавление связей

Достаточно важно заметить, что представленные выше объекты могут иметь вполне конкретные значения:

- звонок;
- телефон – IMEI;
- телефон – IMSI;
- телефон – Базовая станция.

Для задания параметров необходимо выбрать требуемый элемент шаблона, при этом отобразится окно настройки шаблона (Рисунок 34).

Указанные выше категории объекта можно выбрать, изменив параметр «Тип объекта». По умолчанию в программном комплексе выставлена позиция «Любой объект».

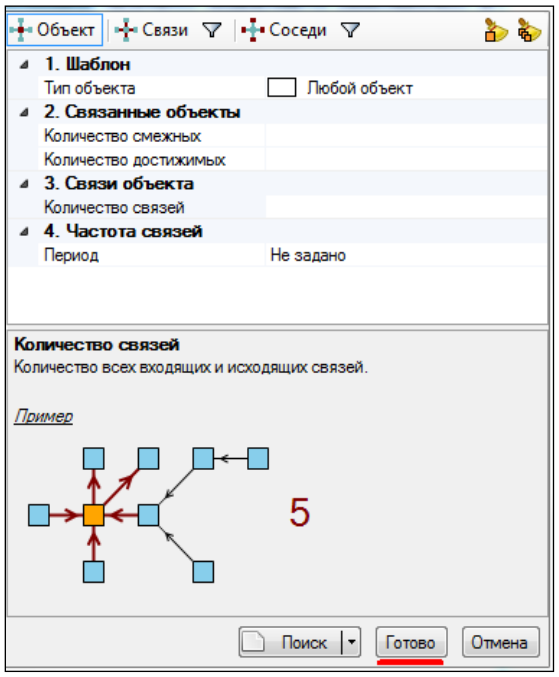


Рисунок 34 – Настройка шаблона

Кроме того, можно выбрать тип связи между объектами, предварительно выделив на схеме связь между объектами (Рисунок 35)

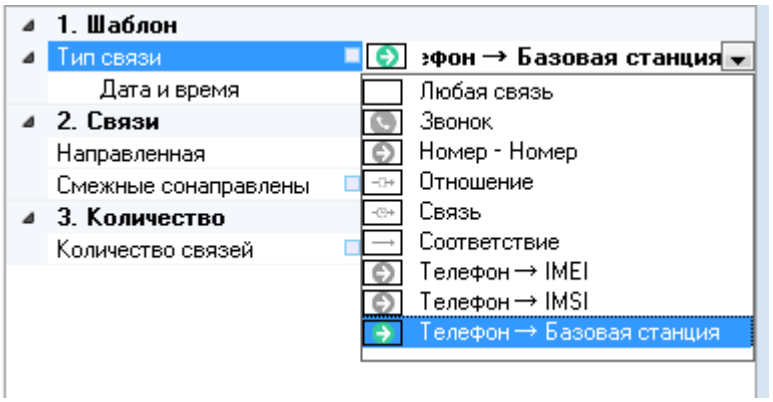


Рисунок 35 – Выбор типа связи между объектами

Если в качестве примера рассмотреть тип связи «Звонок» между двумя телефонами (Рисунок 36), то результат поиска по шаблону будет представлен как на рисунке 37.

Рисунок 36 – Схема связи между двумя телефонами

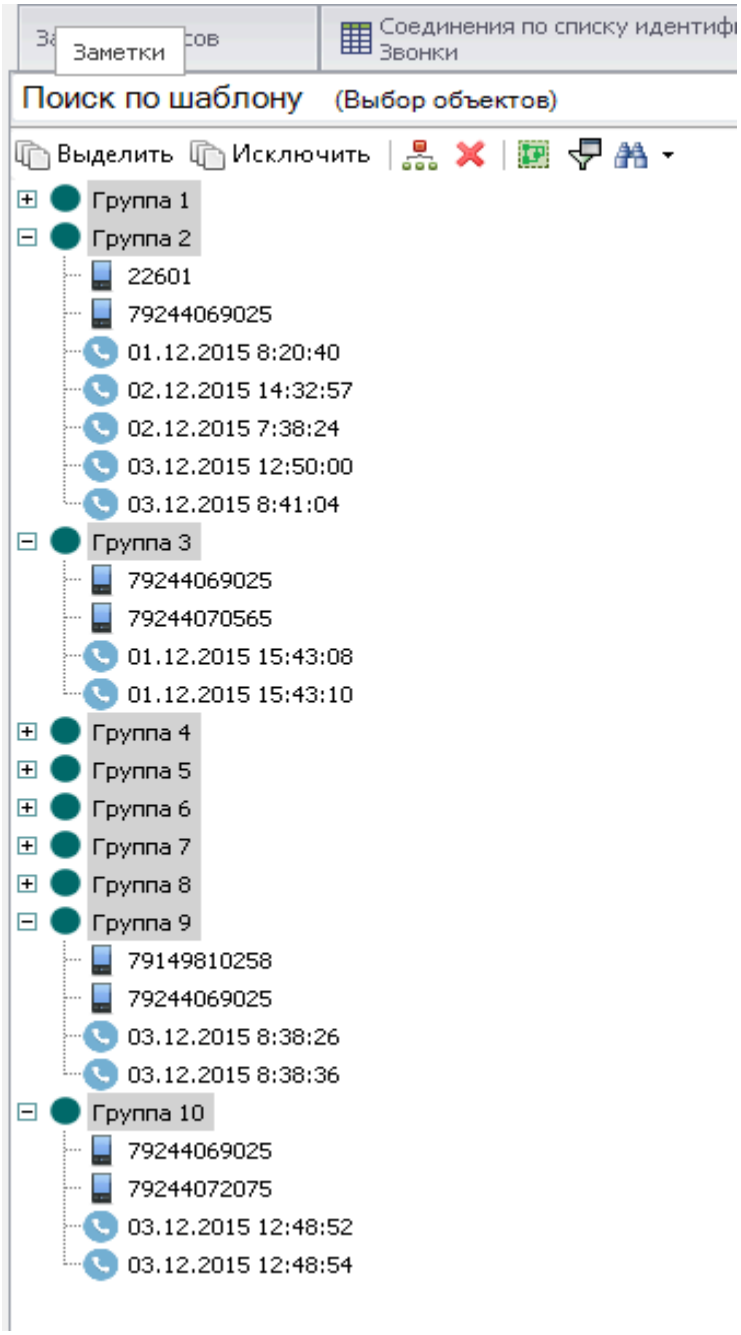


Рисунок 37 – Результат поиска по шаблону

При этом можно выделить конкретные данные двух объектов, между которыми исследуется связь например номера телефонов.

После задания необходимых параметров нажать «Готово». Для редактирования свойств элементов схем, необходимо перейти вокно «Свойства» (Окна – Свойства) (Рисунок 38).

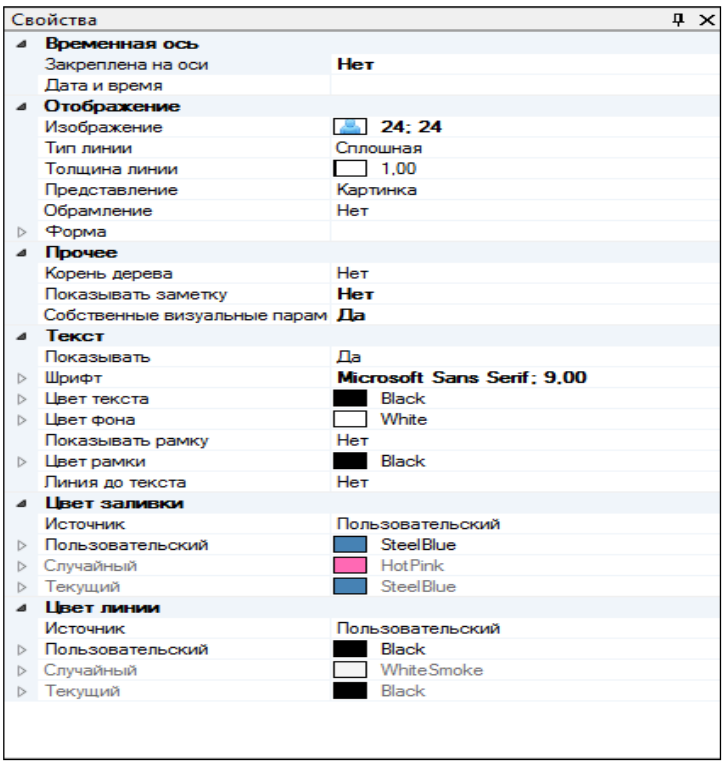


Рисунок 38 – Свойства вершины

Для того чтобы произвести печать текущей схемы необходимо выбрать кнопку «Разбиение на страницы», расположенную на панели инструментов «Схема – Преобразование страницы – Разбиение на страницы» (Рисунок 39).

Рисунок 39 – Панель инструментов для печати

На следующем этапе можно задать разбиение страниц (Рисунок 40).

Рисунок 40 – Разбиение на страницы

Далее необходимо выбрать параметр «Печать» на панели инструментов (Рисунок 41).

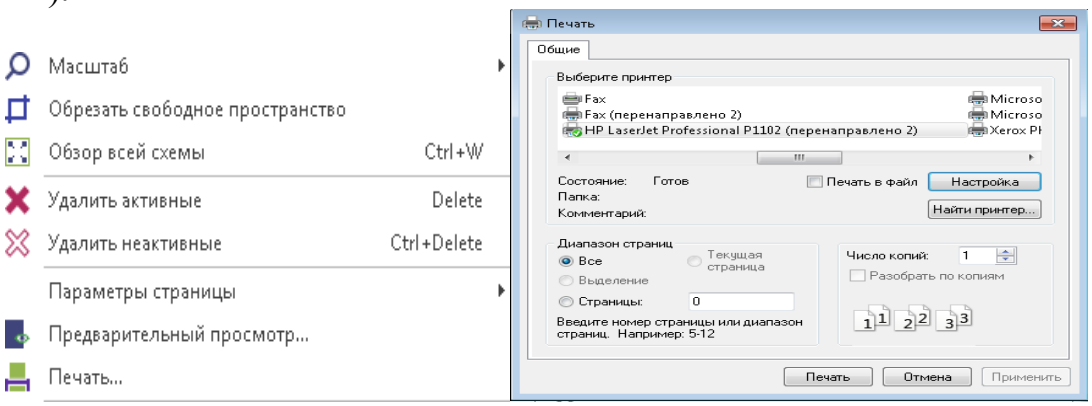


Рисунок 41 – Вывод на печать

Для сохранения схем необходимо выбрать требуемое разрешение в панели инструментов (800x600 – 2560x1600) и нажать кнопку «Сохранить изображение как …» (Рисунок 42).

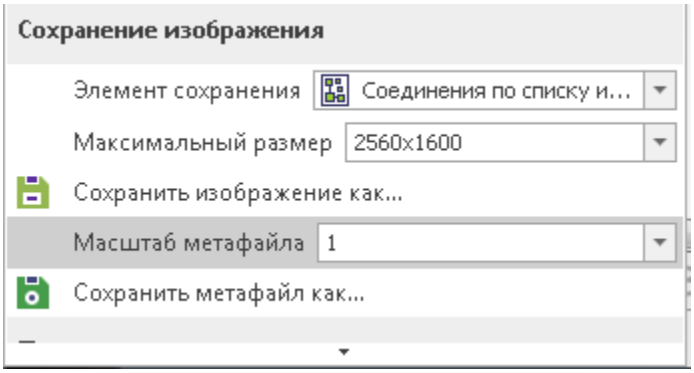


Рисунок 42 – Сохранение схемы связей в виде файла

Сохранить схему в один из растровых форматов (Рисунок 43).

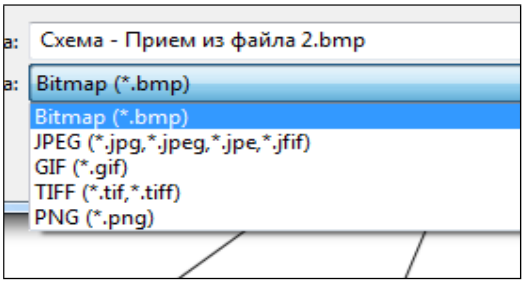


Рисунок 43 – Сохранение схемы в один из растровых форматов

Следует заметить, что если требуется изображение высокого разрешения, то необходимо его сохранить в EMF формат. Для этого необходимо настроить «Коэффициент масштабирования» и нажать кнопку «Сохранить метафайл

как ….» (Рисунок 44).

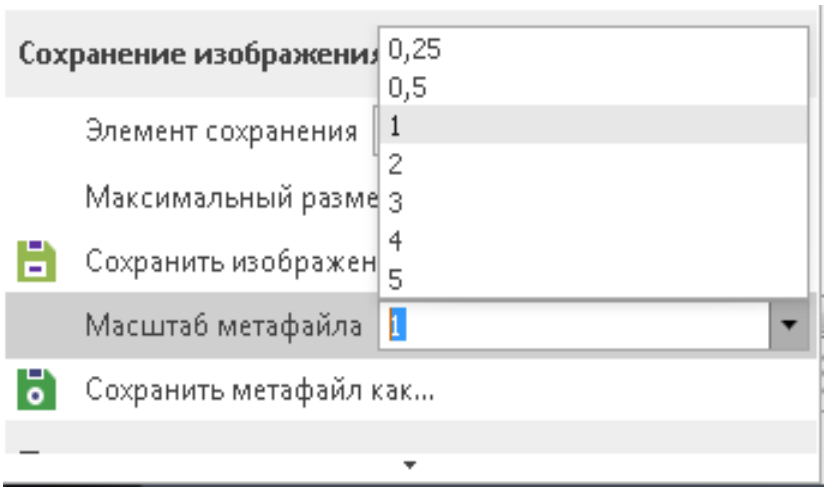


Рисунок 44 – Сохранение изображения в EMF формат

Таким образом, достаточно важно запомнить, что сохранение и печать схемы связей биллинговой информации осуществляется в разделе меню программного обеспечения «Схемы».

1.4. Работа программного комплекса «Виток–3х» с результатами поисковых запросов на ГИС-карте

Результаты поискового запроса в рассматриваемом программном комплексе могут быть представлены в виде таблицы, схемы, документа и ГИС-карты. Для отображения результата на ГИС-карте необходимо в окне «Монитор запросов» выбрать интересующий результат поискового запроса и затем нажать кнопку «ГИС-карта» (Рисунок 45).

При нажатии кнопки «ГИС-карта» предлагается выбор варианта отображения результатов на карте.

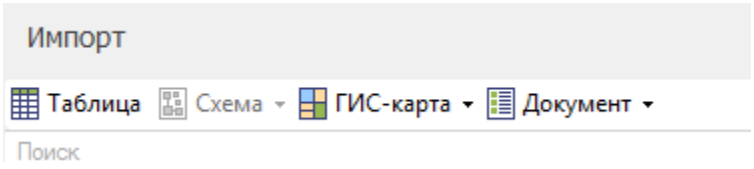


Рисунок 45 – Отображение результата в виде ГИС-карты

Выбрав нужный вариант отображения, получаем результат в виде ГИС-карты (Рисунок 46).

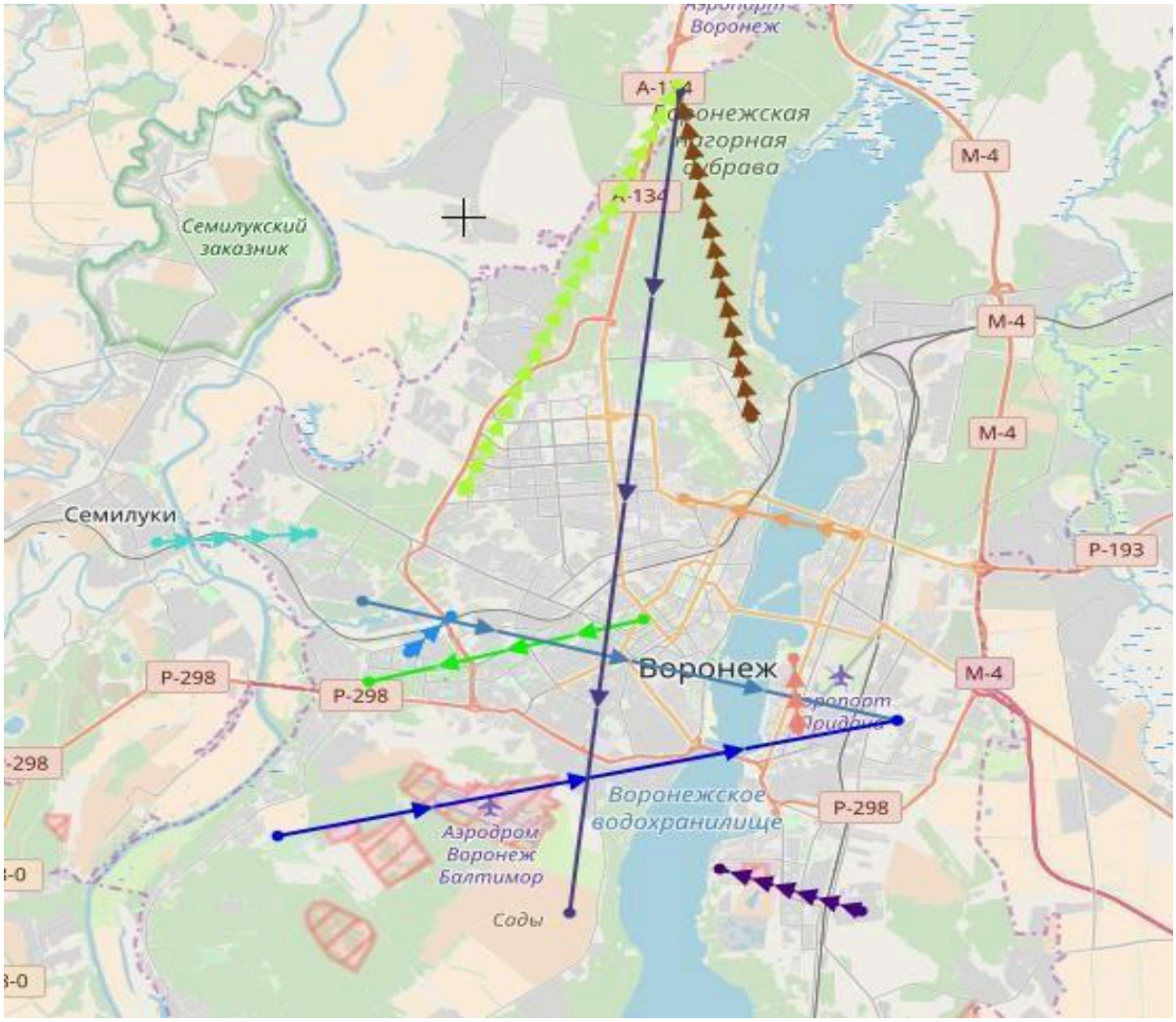


Рисунок 46 – Результат поискового запроса, представленный на ГИС-карте

На карте отобразятся траектории перемещения абонентов, присутствующих в результатах поискового запроса. Для приближения к результатам поиска следует прокрутить колесо мыши, а для перемещения района карты рекомендуется, удерживая правую кнопку мыши, передвигать ее в нужном направлении.

Достаточно важно заметить, что в данном программном комплексе для удобства работы и повышения информативности каждому абоненту из результатов поискового запроса присваивается свой цвет отображения на карте. Соответствие цветов и объектов отображается в окне «Обозреватель» (Рисунок 47).

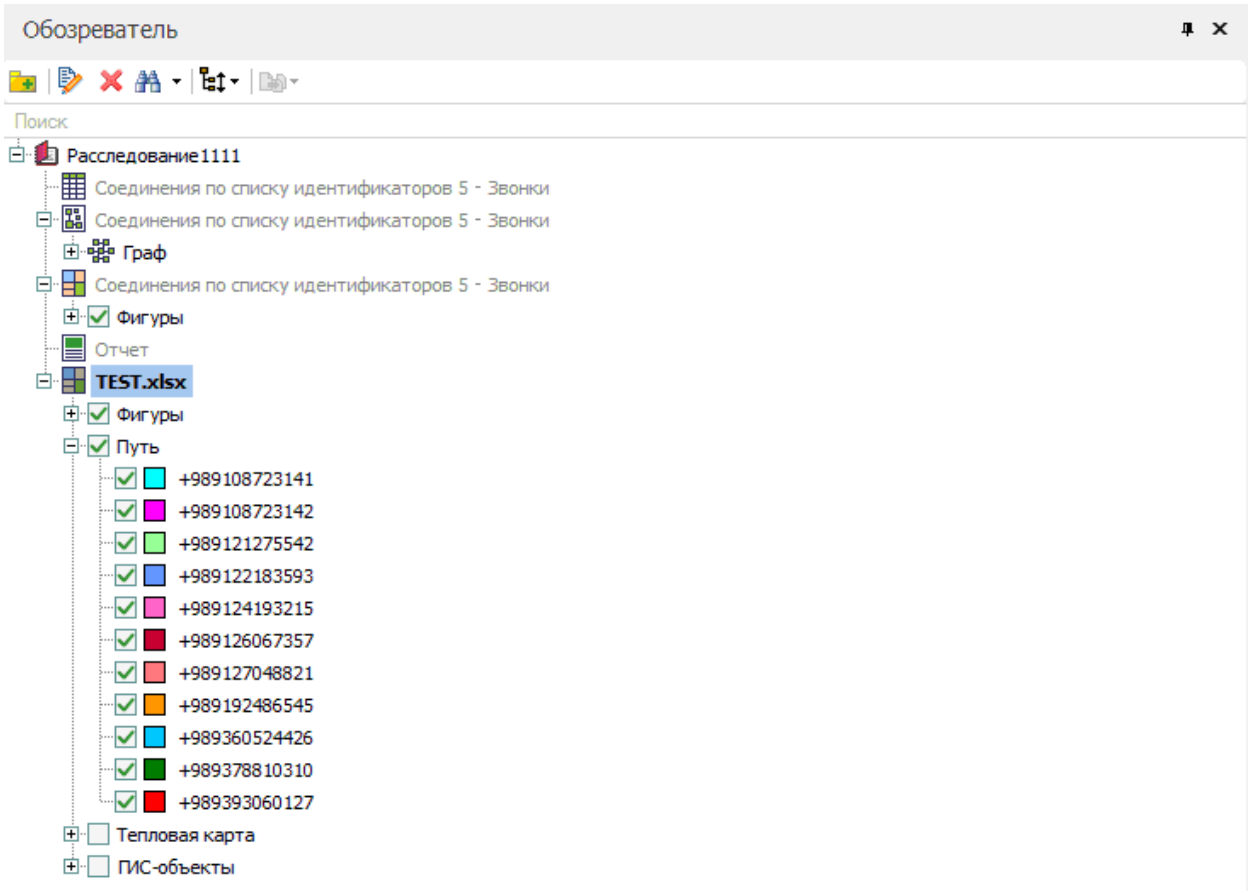


Рисунок 47– Окно «Обозреватель»

Программный комплекс «ВИТОК–3Х» предоставляет широкие возможности работы с ГИС-картой. Данное обстоятельство достаточно актуально при расследовании и раскрытии преступлений.

В частности, для работы с ГИС-картой рассматриваемое программное обеспечение позволяет воспользоваться панелью инструментов, представленной ниже (Рисунок 48).

Рисунок 48 – Инструменты работы с ГИС-картой

Представленная панель инструментов для работы с ГИС-картой позволяет выполнять следующие основные операции:



– удалить активные объекты;


– удалить неактивные объекты;


– уменьшить масштаб;


– увеличить масштаб;


– показать все объекты;

– сохранить как... ;

– выделение;

– возможные действия с выбранным элементом;

– добавить метку на карте.

В целях задания необходимой области на карте используются инструменты  . При этом выбирается требуемый инструмент, затем удерживая левую клавишу мыши, выделяется необходимая область, наносится (рисуется) объект на карту (Рисунки 49,50,51).

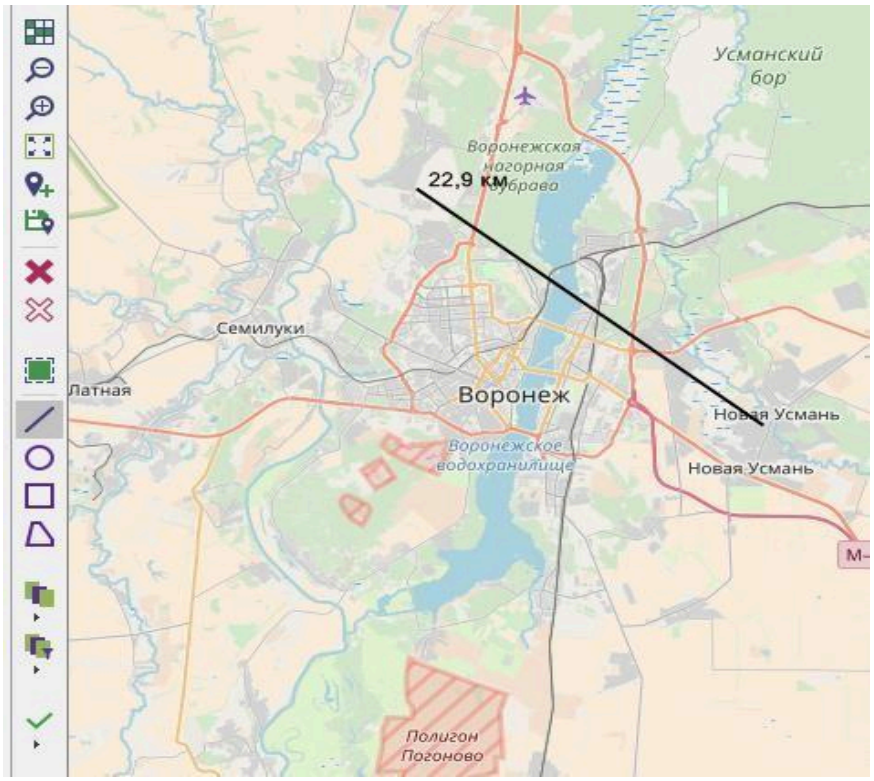


Рисунок 49 – Ломаная линия на карте

Следует заметить, что при проведении расследований по раскрытию преступлений, работая с ГИС-картой, возникает необходимость использовать различные геометрические фигуры (линия, окружность, квадрат, прямоугольник, сложная фигура). Например, при проведении линии на карте показывается расстояние между двумя точками с учетом масштаба карты (Рисунок 49). При нанесении окружности автоматически рассчитывается её радиус (диаметр) (Рисунок 50).

Кроме того, можно вычислить периметр сложной геометрической фигуры (Рисунок 51). Данное обстоятельство может быть полезно при анализе перемещения исследуемого абонента.

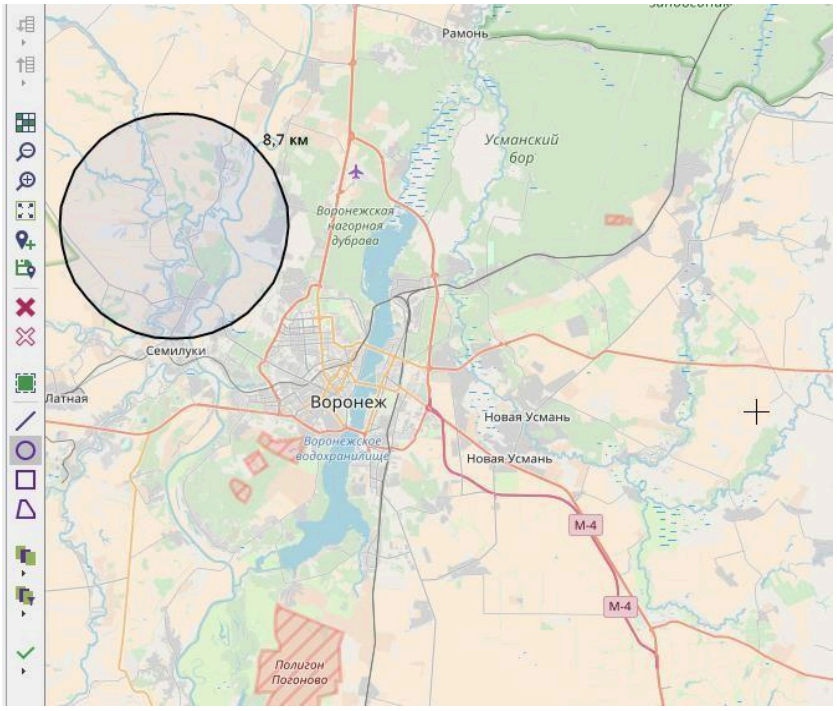


Рисунок 50 – Окружность на карте

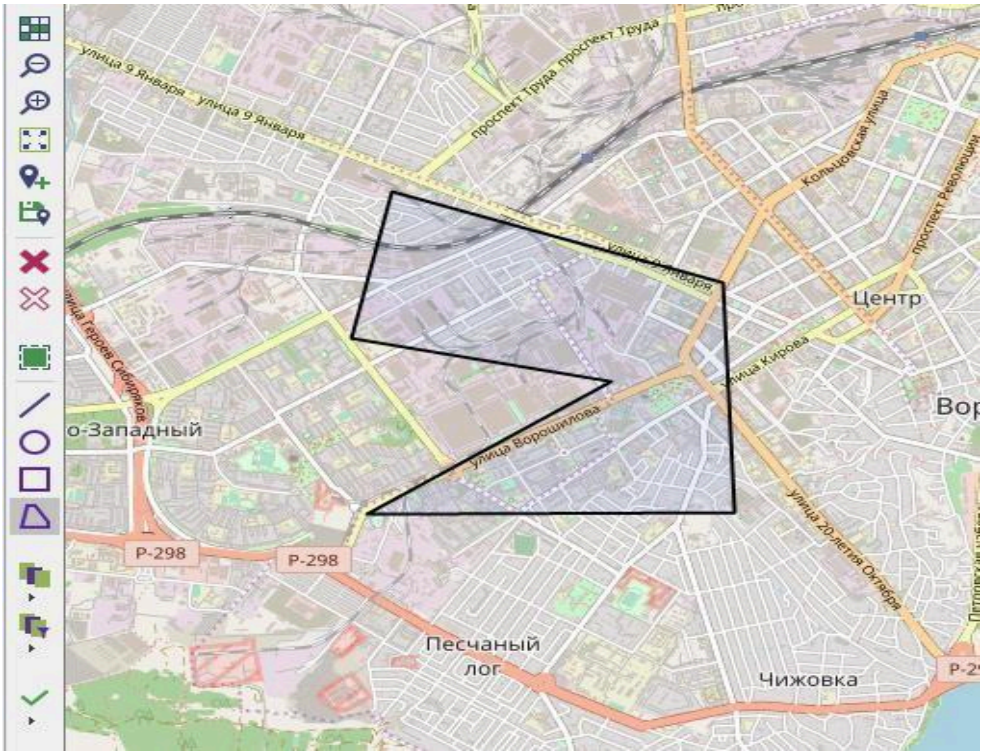


Рисунок 51 – Сложная геометрическая фигура на карте

При работе с геометрическими фигурами на ГИС-карте доступно контекстное меню, позволяющее объединять выделенную область на карте с данными поискового запроса (Рисунок 52).

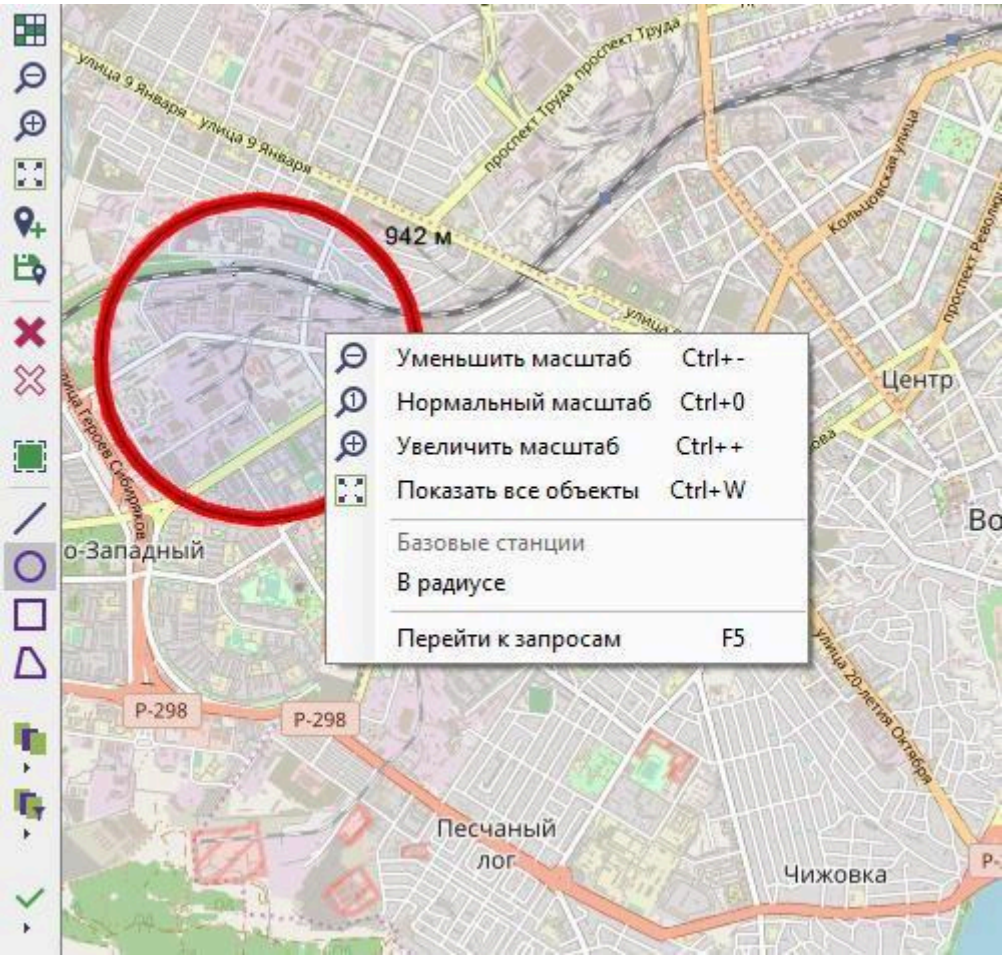


Рисунок 52 – Контекстное меню выбранной области на карте

В области выбранной фигуры, нажимая правой клавишей мыши, открываем контекстное меню, выбираем пункт «Перейти к запросам» (Рисунок 52). При этом открывается окно «Запуск запросов» (Рисунок 53), отображая только те поисковые запросы, которые удовлетворяют заданной на карте области.

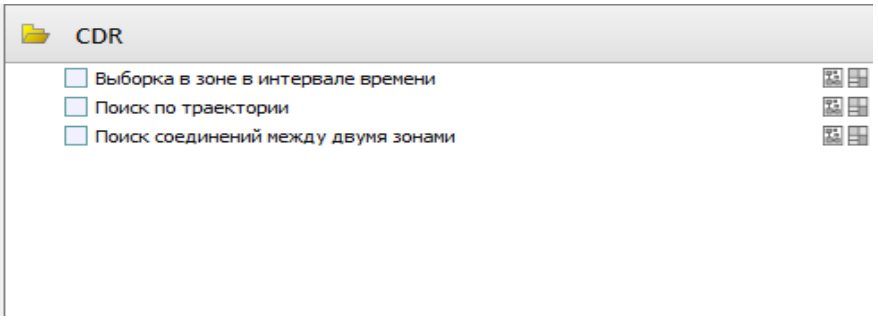


Рисунок 53 – Окно «Запуск запросов»

Для создания слоя на ГИС-карте в главном меню необходимо выбрать «ОКНА – СЛОИ – Добавить новый слой» (Рисунок 54) и присвоить ему название.

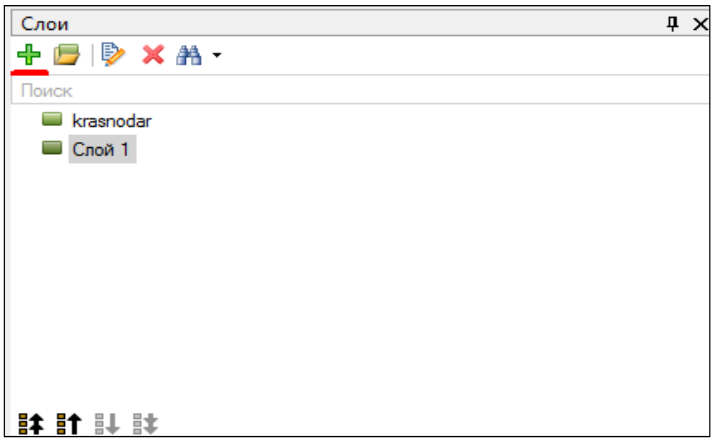


Рисунок 54 – Окно «Слои»

Для работы с созданным слоем дважды кликнуть левой клавишей мыши на названии слоя. Откроется рабочая вкладка с названием созданного слоя (Рисунок 55).

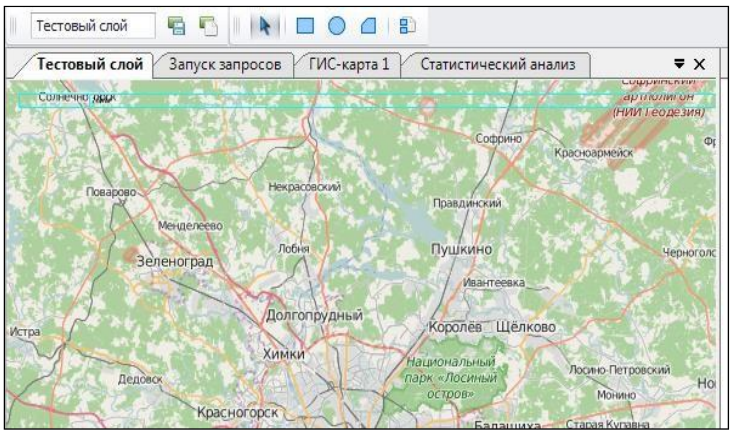


Рисунок 55 – Рабочая вкладка

Для задания областей на карте необходимо воспользоваться инструментами (добавить прямоугольник, круг, многоугольник). После задания необходимых областей, следует нажать на панели инструментов

«Сохранить слой». Созданный слой будет отображаться в «списке созданных слоев». Для работы со слоями ГИС-карты, в панели инструментов выбрать «Слои». При выборе инструмента «Слои» предлагается список созданных слоев. Выбираем нужный слой, после чего выбранный слой отображается на ГИС-карте (Рисунок 56).

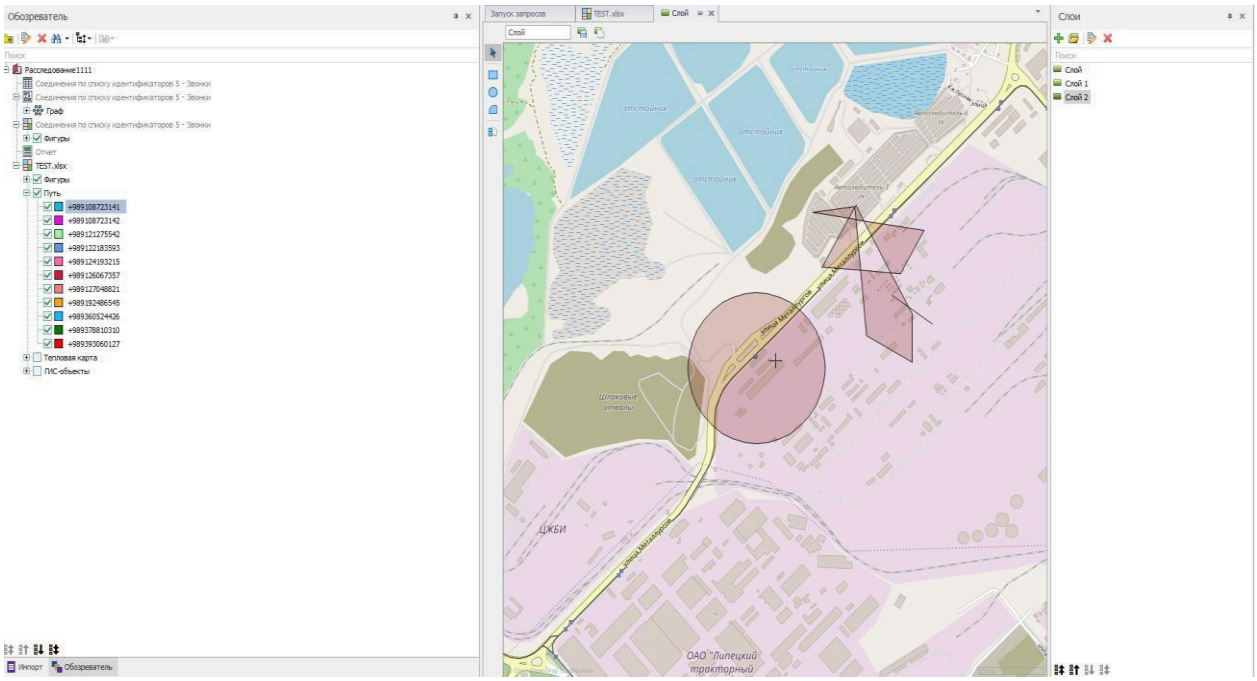


Рисунок 56 – Выбранный слой на ГИС-карте

Для сохранения результатов работы с ГИС-картой необходимо на панели инструментов выбрать пункт «Сохранить как…» и указать путь сохранения (Рисунок 57).

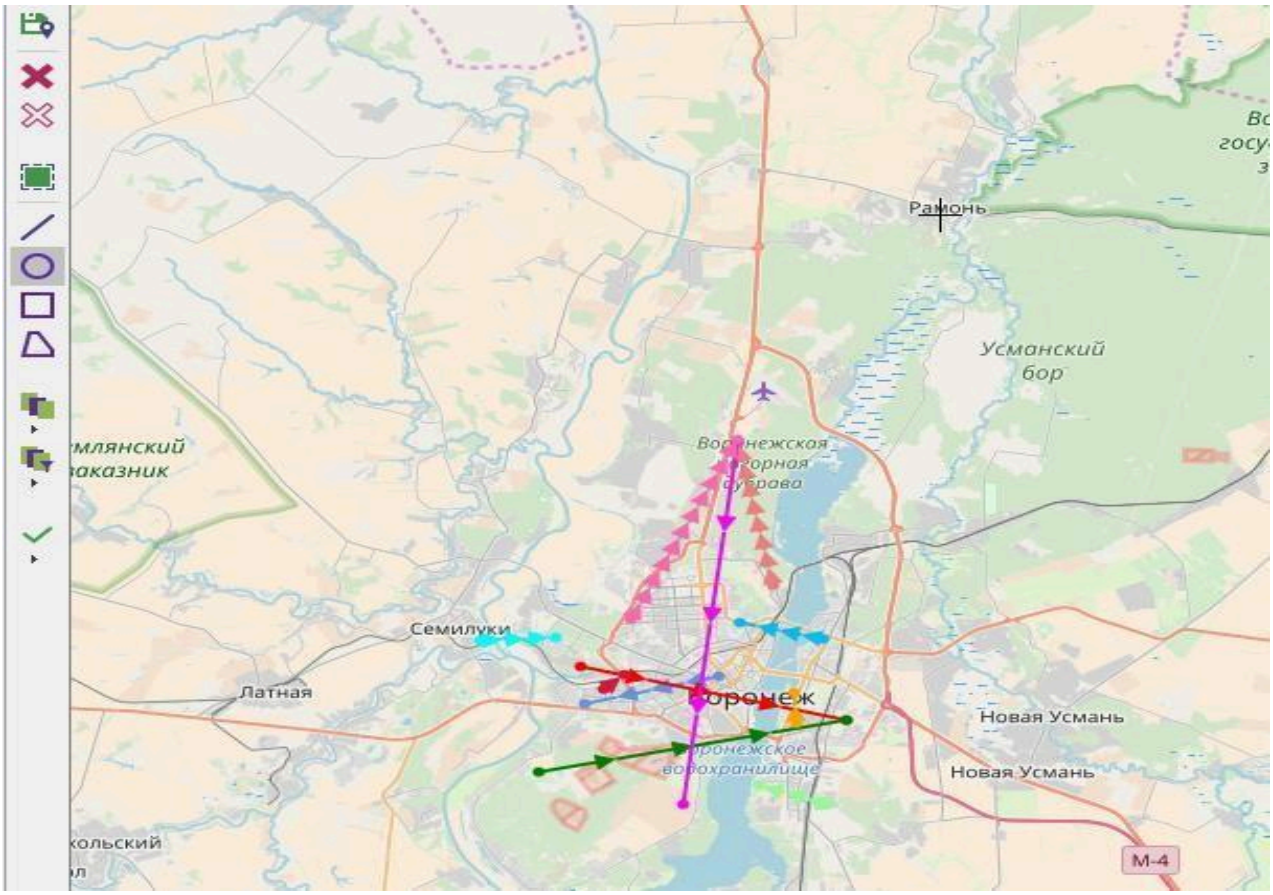
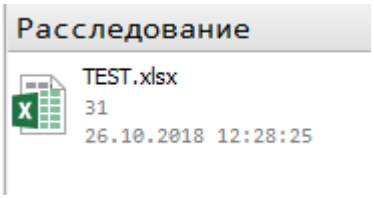


Рисунок 57 – Сохранение ГИС-карты

Следует заметить, что в рассматриваемом программном обеспечении для работы с ГИС-картой необходимо использовать биллинг, содержащий соответствующие данные, которые могут быть нанесены на карту (например, координаты точек – абонентов, базовых станций и т.д).

Представляется целесообразным рассмотреть основные возможности и алгоритм представления визуальных компонентов на ГИС-карте. Для реализации данной цели следует выбрать пункты меню «ОКНА – импорт».

Далее на панели инструментов следует использовать пиктограмму , которая позволяет импортировать файлы. В качестве примера рассмотрим загрузку тестовых данных. После нажатия представленной выше пиктограммы откроется диалоговое окно, в котором следует выбрать файл для загрузки (TEST.xlsx) и нажать кнопку открыть. В том случае если все действия выполнены правильно, то можно будет увидеть выбранный файл с количеством загруженных записей.



Важно отметить, что на данном этапе вывод данных на ГИС-карту пока ещё не возможен. Для вывода данных на ГИС-карту необходимо создать шаблон, на основе которого рассматриваемый программный комплекс будет отображать данные поискового запроса (биллинга) на ГИС-карте.

Для создания шаблона следует выбрать на панели инструментов пиктограмму – «Добавить шаблон создания». После чего откроется окно, в котором и необходимо будет создавать шаблон (Рисунок 58).

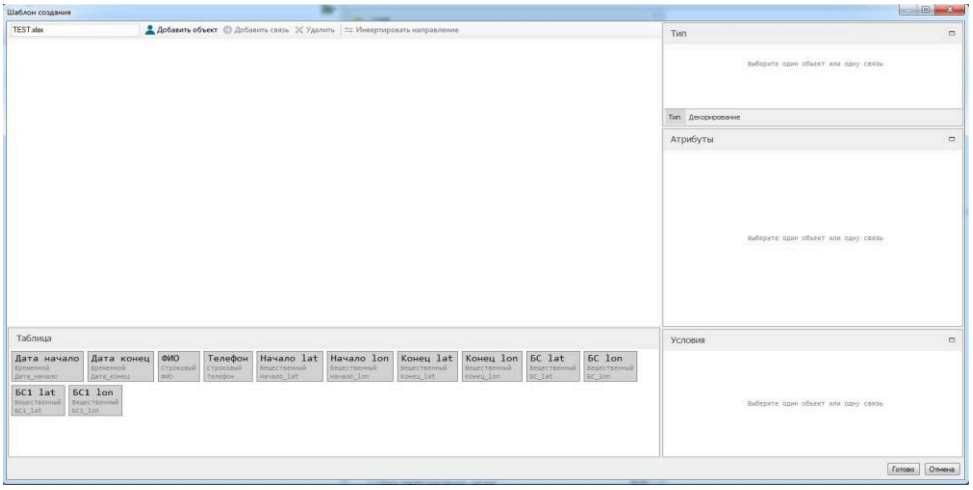


Рисунок 58 – Создание шаблона для работы ГИС-карты

На первом этапе работы с шаблоном создаются объекты и им задаются соответствующие параметры. После нажатия кнопки «Добавить объект». В правом углу откроется дополнительное меню с параметрами объекта.

Созданному объекту следует присвоить имя (например, начальное положение) и задать соответствующие атрибуты. При задании атрибутов необходимо нажать на столбцы, которые следует добавить в объект и перетащить их внутрь объекта. Например, можно использовать такие атрибуты как начальная дата, ФИО, телефон абонента и координаты его положения. При работе с атрибутом координаты местоположения следует выбрать параметр «Точка» в столбце названия (Рисунок 59). Необходимо отметить, что в других случаях при переносе столбцов имя объекта будет присвоено автоматически.

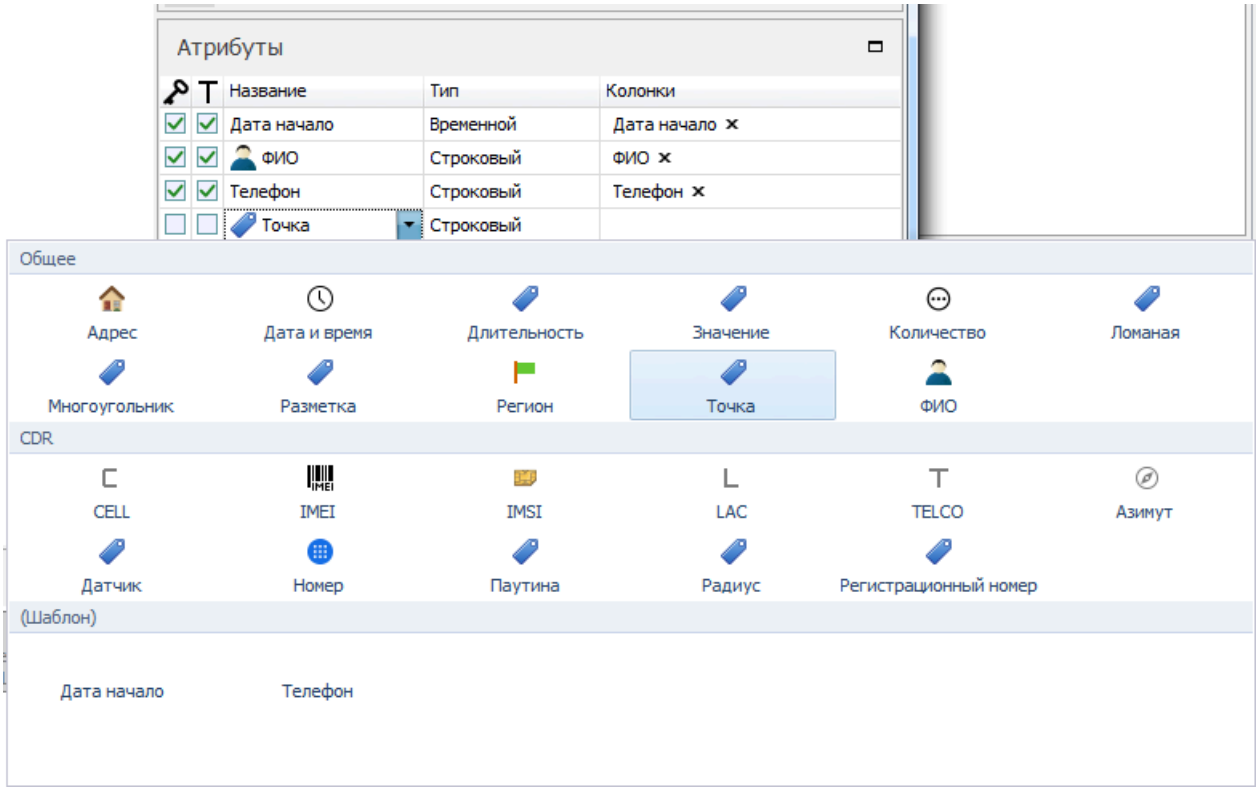


Рисунок 59 – Задание атрибутов объекта

Используя представленную выше методику, представляется целесообразным создать аналогичным образом еще 3 объекта:

- «Конечное положение»;
- «Начальная БС»;
- «Конечная БС».

Таким образом, в рассматриваемом шаблоне заданы начальное и конечное положение анализируемого абонента, а также указаны начальная и конечная базовые станции оператора сотовой связи (Рисунок 60).

После создания шаблона следует нажать кнопку «Готово».

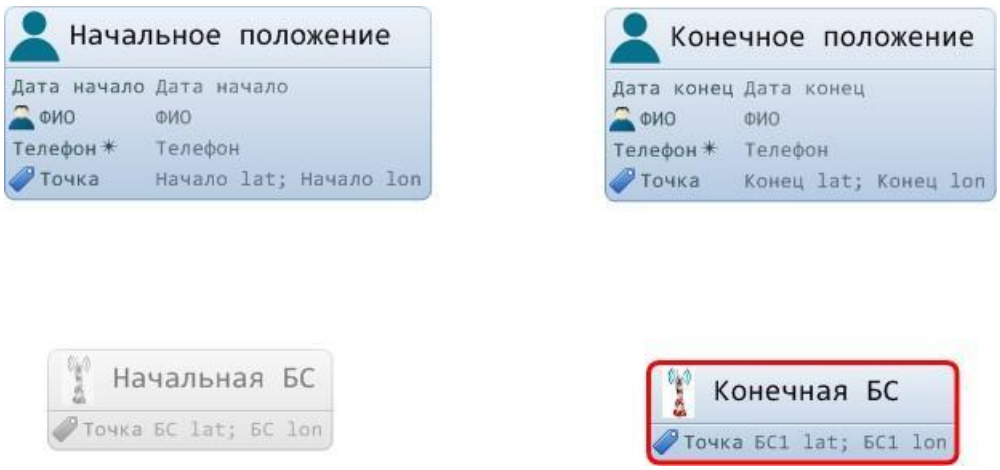


Рисунок 60 – Шаблон для работы с ГИС-картой

В том случае, если все действия выполнены правильно, то вкладка ГИС-карта становится активной. Далее необходимо выбрать созданный шаблон в ГИС-карте. При этом на ГИС-карте будут отображены данные, аналогичные рисунку 61.

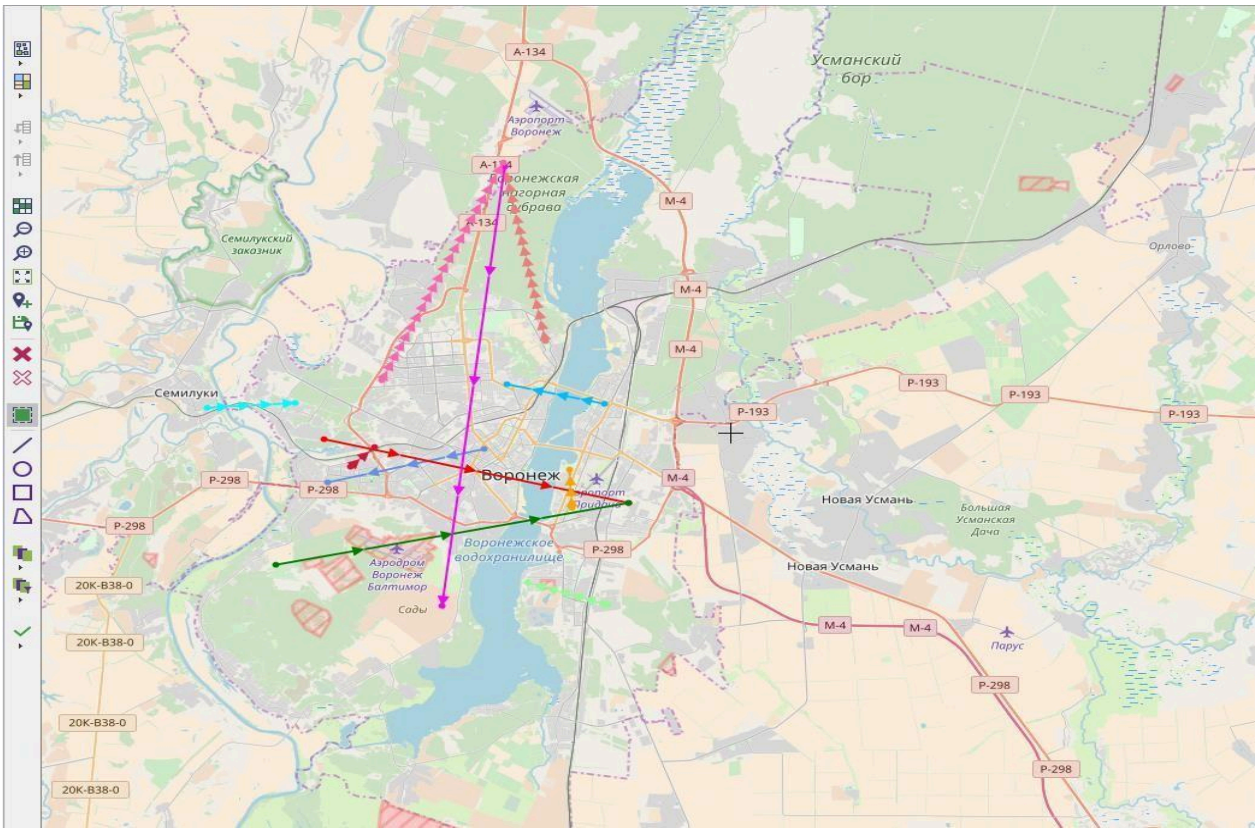


Рисунок 61 – Результат отображения шаблона

Рассматриваемое программное обеспечение позволяет визуализировать места на карте, которые наиболее часто посещал интересующий абонент сотовой связи. Для получения данной информации необходимо использовать так называемую «тепловую карту». При этом необходимо перейти в раздел

«Обозреватель» и посмотреть содержимое. Для удобства отображения и восприятия информации целесообразно снять галочки со всех компонентов «Обозревателя» за исключением пунктов «Фигуры» и «Тепловая карта». Достигнутый результат представлен на рисунке 62.

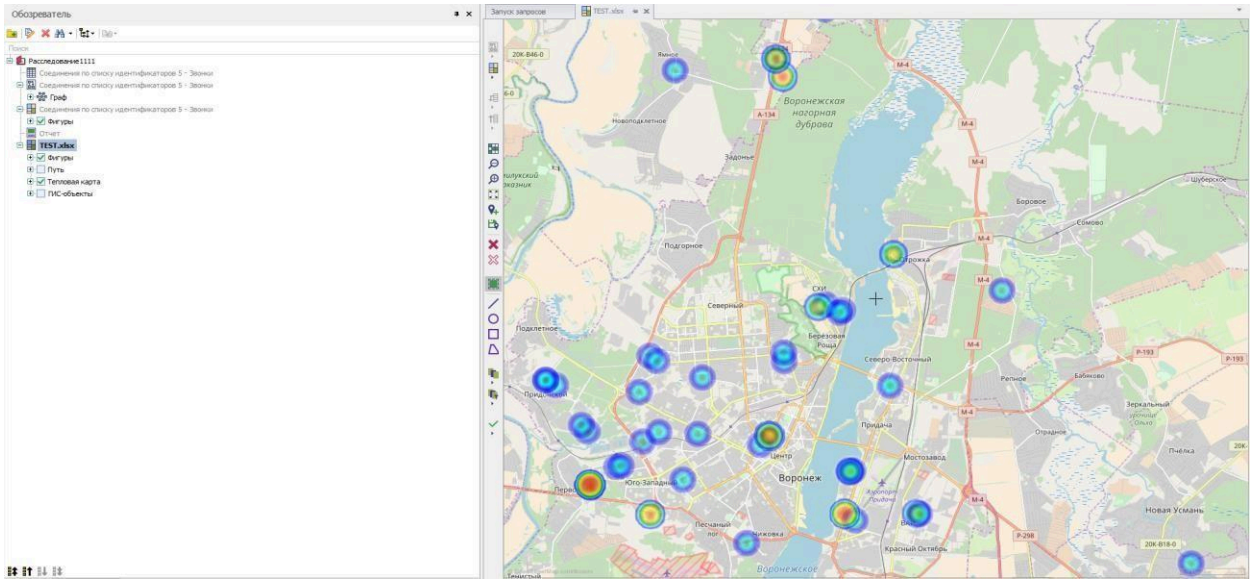


Рисунок 62 – Тепловая карта

Для того чтобы отобразить рассматриваемые данные в виде схемы (графа) необходимо изменить первоначально созданный шаблон. В частности, следует связать объекты. Для создания связи необходимо выделить попарно объекты, как показано на рисунке 63, и нажать кнопку добавить связь. Далее следует указать параметры связи.

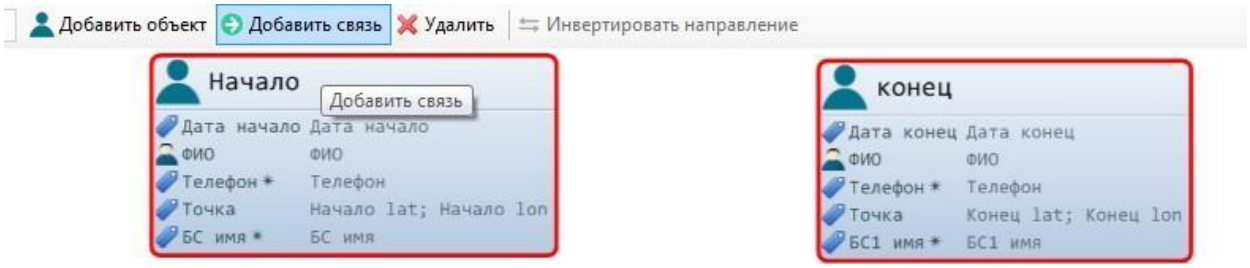


Рисунок 63 – Организация связи двух объектов

Для рассматриваемого шаблона, в качестве примера, укажем тип связи «Телефон» между начальным и конечным положением абонента, а положения абонента свяжем с базовыми станциями типом связи «БС» (Рисунок 64).

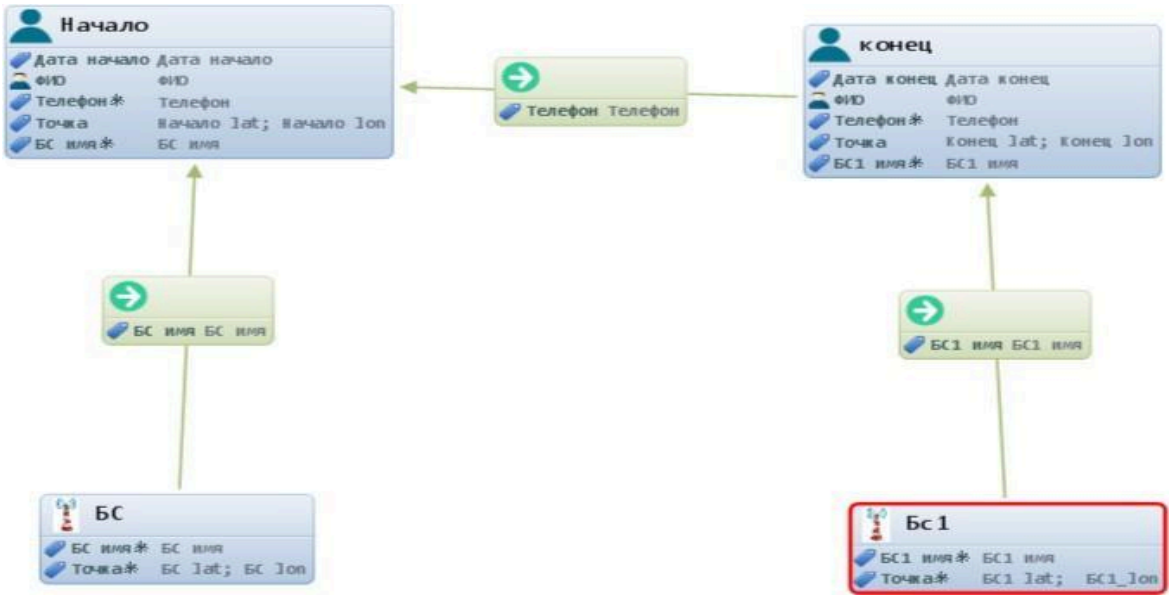


Рисунок 64 – Организация связи объектов шаблона

После создания связей в шаблоне необходимо сохранить результат. При этом вкладка схема станет активной и можно вывести результат на схему (Рисунок 65).

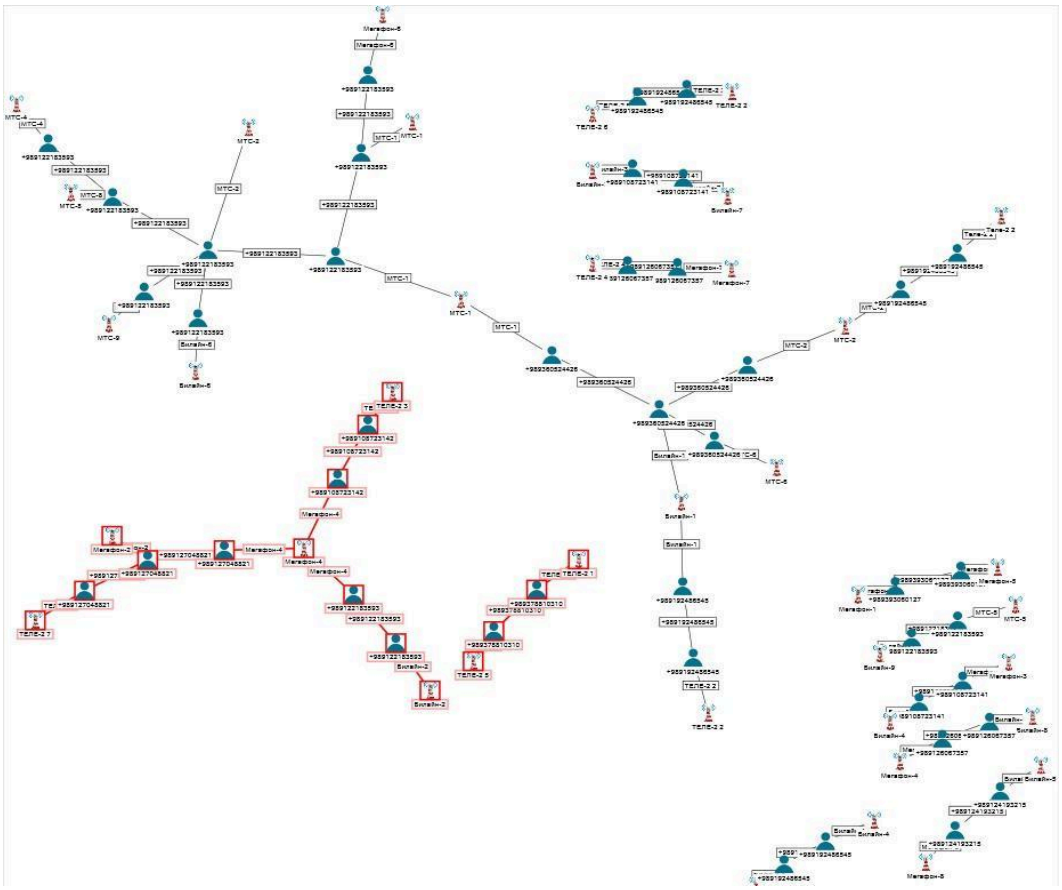


Рисунок 65– Схема связи объектов на основе шаблона

1.5. Статистический анализ биллинговой информации программного комплекса «Виток–3х»

Проведение статистического анализа биллинговой информации позволяет отображать статистику соединений абонента, осуществлять поиск и визуализацию линий поведения абонента и отклонения от них (аномалии), и сохранять полученные результаты в виде файла-отчета в формате .xls.

Входными данными для статистического анализа являются результаты работы аналитических методик, выполненных в рамках созданного расследования. Для выполнения анализа необходимо в главном меню приложения выбрать пункт «Анализ – Статистический анализ» (Рисунок 66).

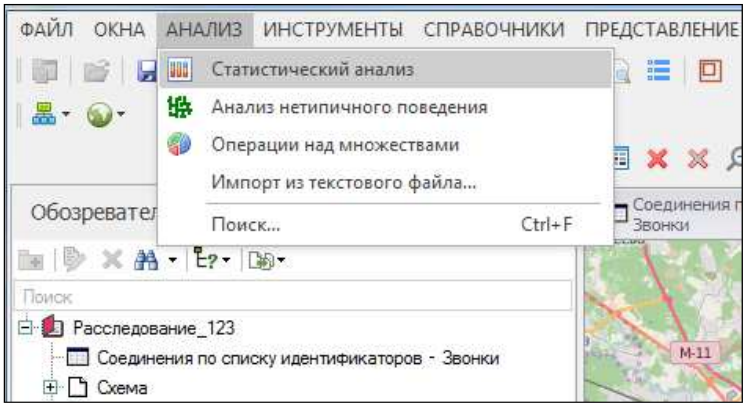


Рисунок 66 – Окно запуска статистического анализа

В открывшемся окне «Задание статистического анализа» (Рисунок 67) необходимо указать название (по умолчанию это «Статистический анализ – Название выбранной методики»), отметить необходимый результат для анализа, выбрать нужный идентификатор и нажать «Создать».

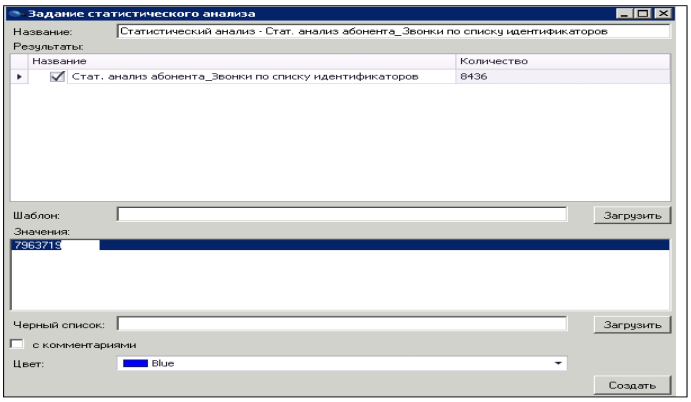


Рисунок 67 – Окно выбора данных для анализа

Для загрузки шаблона ранее созданных и сохраненных настроек отображения статистического анализа необходимо в строке «Шаблон» с помощью кнопки «Загрузить» выбрать соответствующий шаблон.

Для визуально понятного отображения нежелательных номеров из списка анализа предусмотрено применение «Черного списка» – строка - «Черный список – Загрузить» (файл формата .txt, с комментариями или без) из ранее созданного файла вида, изображенного на рисунке 3, с разделителем Tab (флаг «с комментариями» необходимо устанавливать ДО загрузки «Черного списка»).

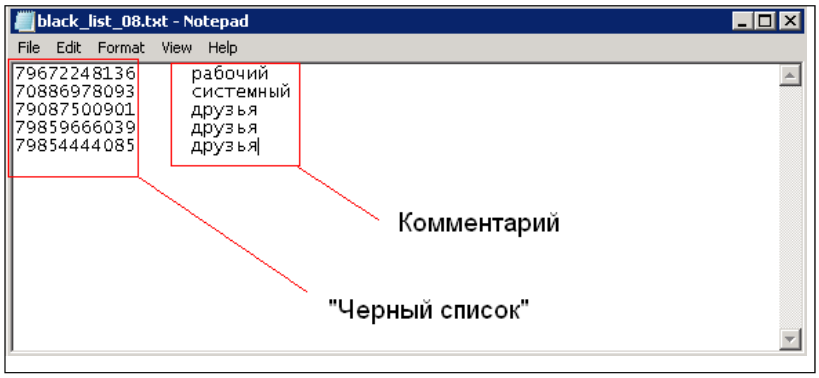


Рисунок 68 – «Черный список» с комментариями

Цвет ячеек с идентификаторами из черного списка определяется также пользователем в строке «Цвет».

После выбора данных для исследования пользователю открывается главное окно анализа, в верхней части которого расположено окно настроек (Рисунок 69).

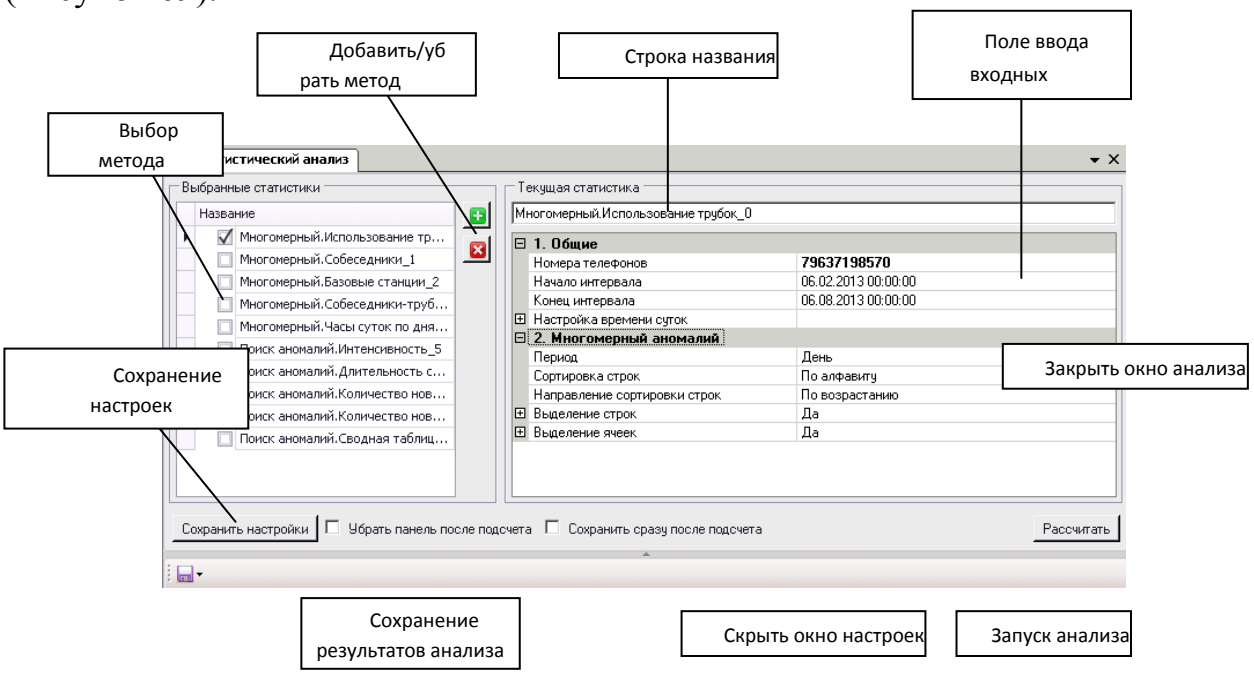


Рисунок 69 – Окно настроек анализа

Для выбора метода анализа необходимо нажать кнопку  .

В открывшемся окне «Выбор статистического анализа» (Рисунок 70) выбрать необходимые статистические методы анализа и нажать «Готово».

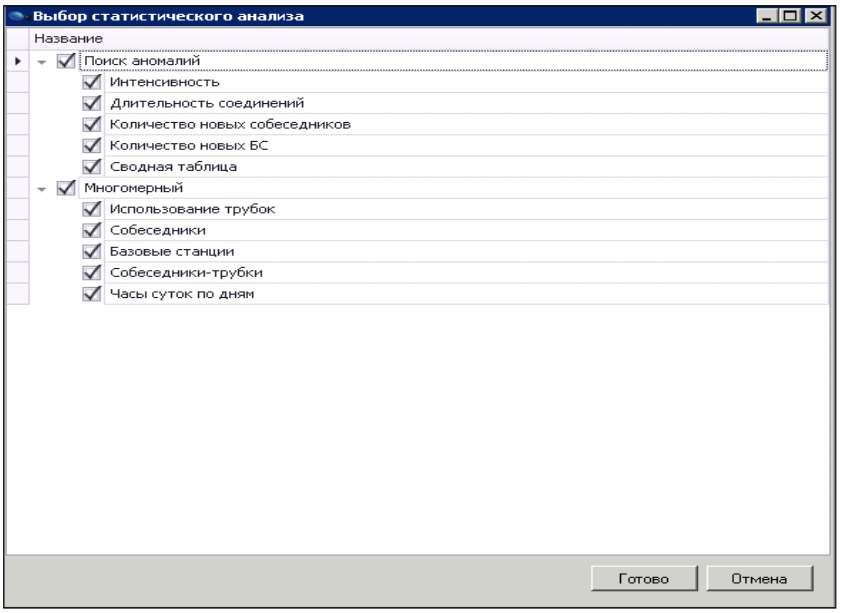
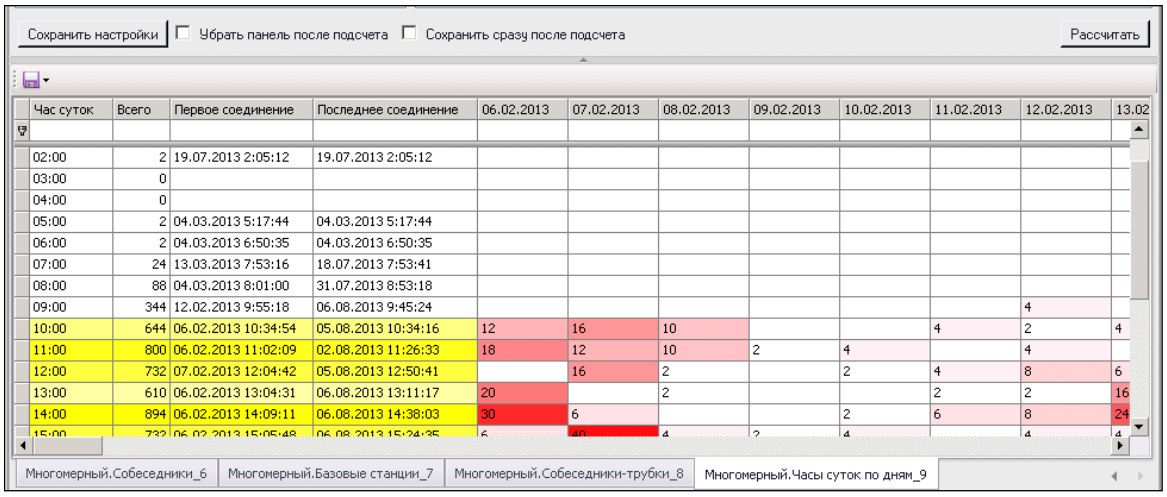


Рисунок 70 – Окно выбора метода статистического анализа

Далее для запуска анализа необходимо нажать «Рассчитать» (Рисунок 4).

При этом после завершения процесса расчета в нижней части главного окна отобразятся результаты анализа в табличном виде (отдельная вкладка для каждого метода анализа (Рисунок 71)).



Час суток	Всего	Первое соединение	Последнее соединение	06.02.2013	07.02.2013	08.02.2013	09.02.2013	10.02.2013	11.02.2013	12.02.2013	13.02
02:00	2	19.07.2013 2:05:12	19.07.2013 2:05:12								
03:00	0										
04:00	0										
05:00	2	04.03.2013 5:17:44	04.03.2013 5:17:44								
06:00	2	04.03.2013 6:50:35	04.03.2013 6:50:35								
07:00	24	13.03.2013 7:53:16	18.07.2013 7:53:41								
08:00	88	04.03.2013 8:01:00	31.07.2013 8:53:18								
09:00	344	12.02.2013 9:55:18	06.08.2013 9:45:24							4	
10:00	644	06.02.2013 10:34:54	05.08.2013 10:34:16	12	16	10			4	2	4
11:00	800	06.02.2013 11:02:09	02.08.2013 11:26:33	18	12	10	2	4		4	
12:00	732	07.02.2013 12:04:42	05.08.2013 12:50:41		16	2		2	4	8	6
13:00	610	06.02.2013 13:04:31	06.08.2013 13:11:17	20		2			2	2	16
14:00	894	06.02.2013 14:09:11	06.08.2013 14:38:03	30	6			2	6	8	24
15:00	732	06.02.2013 15:05:48	06.08.2013 15:24:35	6	40	4	2	4		4	4

Поиск аномалий предназначен для выявления экстремальных периодов поведения абонента, не характерных для его среднестатистического поведения. Представляет собой подробную статистику общения абонента в табличном виде по выбранным пользователем периодам времени.

Для выполнения всех методов поиска аномалий необходимо указать входные параметры (параметры группы «Общие» в поле ввода входных параметров (Рисунок 72) одинаковы и обязательны для всех методов поиска статистического анализа).

Ниже рассмотрены методы поиска аномалий, входные данные для них и результаты анализа.

«Поиск аномалий. Интенсивность» – отображает периоды аномальной интенсивности общения абонента в указанном интервале времени. Для выполнения анализа необходимо выполнить действия представленные ниже.

В окне «Выбор статистического анализа» (Рисунок 70) установить флаг «Поиск аномалий – Интенсивность», нажать «Готово».

Выделить метод анализа в поле выбора метода анализа (Рисунок 69), нажать «Рассчитать». При этом в поле ввода входных параметров отобразятся необходимые для заполнения поля (по умолчанию указаны «средние» значения параметров):

– «Номера телефонов» - поле для ввода номера(-ов) телефонов для анализа. Номера, возможно указывать списком с загрузкой из стороннего файла (инструмент «Добавить из файла») с выбранным пользователем разделителем и удалением пустых и повторяющихся строк (Рисунок 72);

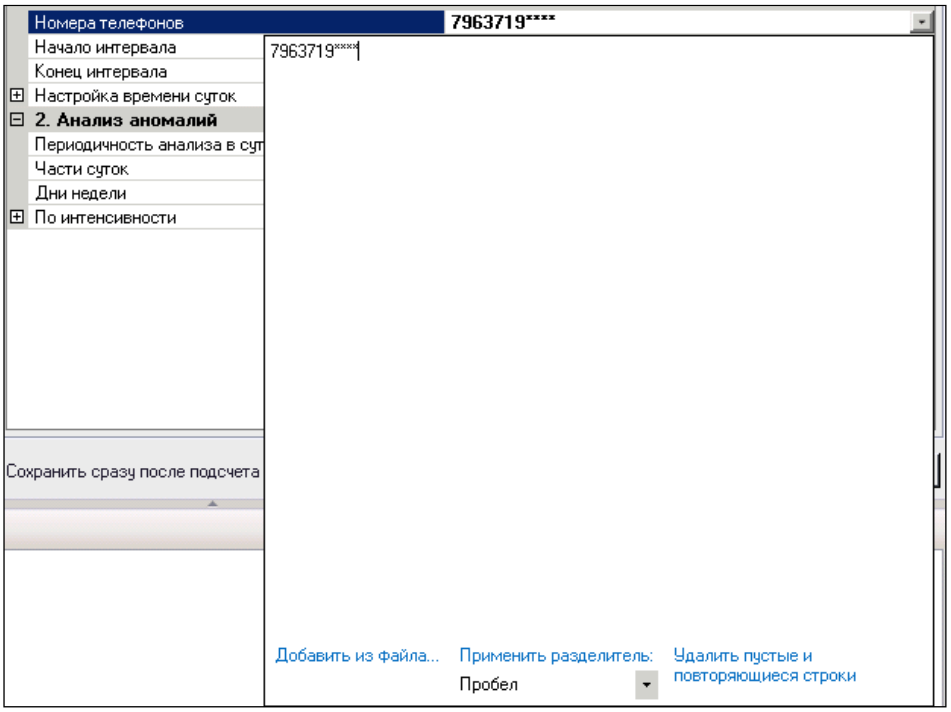


Рисунок 72 – Окно ввода номера телефона для анализа

– «Начало интервала» и «Конец интервала» - задает период времени, по которому будет производиться анализ. По умолчанию автоматически выбирается период с первой записи об активности абонента до последней. Ввод возможен как вручную в строке, так и с использованием интерактивного календаря;

– «Настройка времени суток» - позволяет указывать время начала той или иной части суток (ночь, утро, день, вечер) (Рисунок 73);

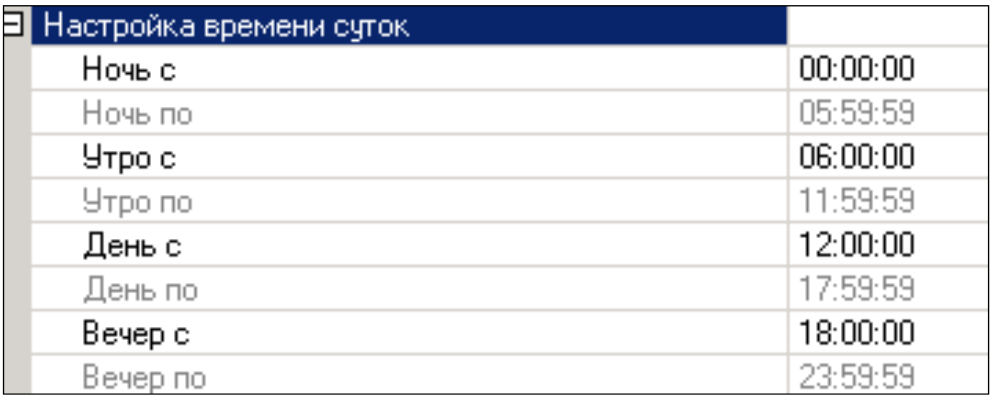


Рисунок 73 – Окно настройки времени суток

– «Периодичность анализа в сутках» - позволяет делать поправку на периодичность в поведении абонента. Используется при известной устойчивой периодичности в поведении абонента. Например, при недельной периодичности значение параметра равно семи;

– «Части суток» - указывает, какие части суток исключить/использовать в анализе. Может применяться для анализа определенной части дня, например рабочего времени абонента (Рисунок 74);

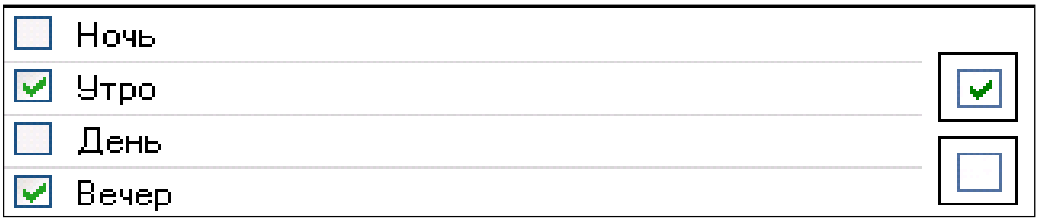


Рисунок 74 – Окно выбора периода суток для анализа

– «Дни недели» - указывает, какие дни недели исключить/использовать в анализе. Может применяться для анализа определенных дней недели, например, только будни, или только выходные (Рисунок 75);

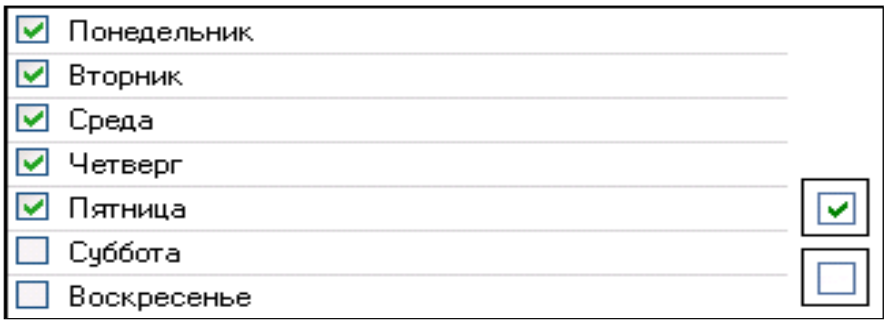


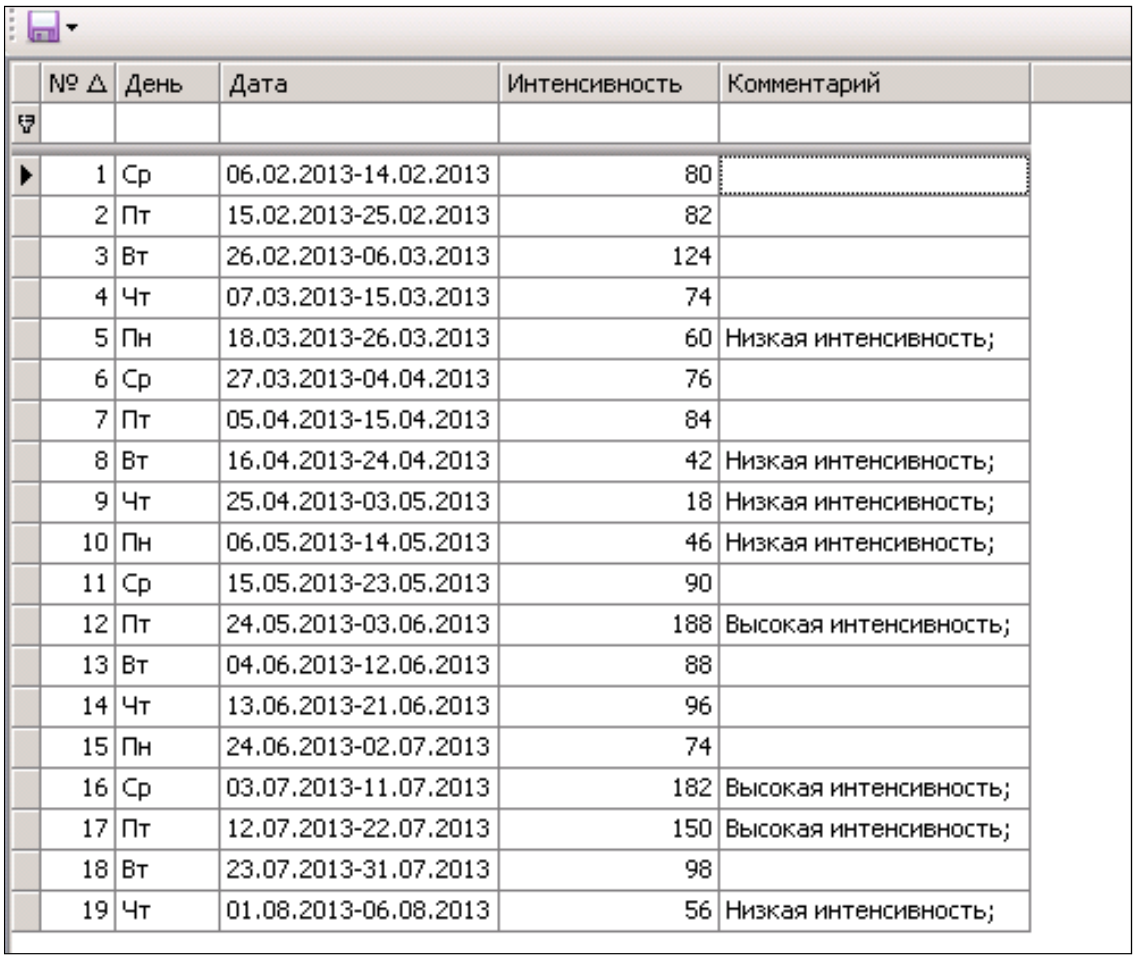
Рисунок 75 – Окно выбора дней недели для анализа

– «Наиболее интенсивные» (да/нет, составляющие % трафика) - отмечает/не отмечает периоды с наибольшей активностью, сумма интенсивностей которых не меньше значения параметра «Составляющие %

трафика»;

– «Наименее интенсивные» (да/нет, составляющие % трафика) – отмечает/ не отмечает периоды с наименьшей активностью, сумма интенсивностей которых не больше значения параметра «Составляющие % трафика».

Результатом анализа будет таблица за указанный интервал времени с указанной периодичностью с отмеченными периодами интенсивности, согласно установленным значениям (Рисунок 76).



№ Δ	День	Дата	Интенсивность	Комментарий
1	Ср	06.02.2013-14.02.2013	80	
2	Пт	15.02.2013-25.02.2013	82	
3	Вт	26.02.2013-06.03.2013	124	
4	Чт	07.03.2013-15.03.2013	74	
5	Пн	18.03.2013-26.03.2013	60	Низкая интенсивность;
6	Ср	27.03.2013-04.04.2013	76	
7	Пт	05.04.2013-15.04.2013	84	
8	Вт	16.04.2013-24.04.2013	42	Низкая интенсивность;
9	Чт	25.04.2013-03.05.2013	18	Низкая интенсивность;
10	Пн	06.05.2013-14.05.2013	46	Низкая интенсивность;
11	Ср	15.05.2013-23.05.2013	90	
12	Пт	24.05.2013-03.06.2013	188	Высокая интенсивность;
13	Вт	04.06.2013-12.06.2013	88	
14	Чт	13.06.2013-21.06.2013	96	
15	Пн	24.06.2013-02.07.2013	74	
16	Ср	03.07.2013-11.07.2013	182	Высокая интенсивность;
17	Пт	12.07.2013-22.07.2013	150	Высокая интенсивность;
18	Вт	23.07.2013-31.07.2013	98	
19	Чт	01.08.2013-06.08.2013	56	Низкая интенсивность;

Рисунок 76 – Результат анализа интенсивности абонента

В данном примере в анализе учитывался трафик с недельной периодизацией в будни. Отмечены недели с аномально высокой и низкой интенсивностью.

«Поиск аномалий. Длительность соединений» – отображает периоды с аномальной длительностью соединений абонента в указанном интервале времени. Для выполнения анализа необходимо:

− в окне «Выбор статистического анализа» (Рисунок 70) установить флаг «Поиск аномалий – Длительность соединений», нажать «Готово»;

− выделить метод анализа в поле выбора метода анализа. При этом в поле ввода входных параметров отобразятся необходимые для заполнения поля (по умолчанию указаны «средние» значения параметров):

1) параметры группы «Общие» (см. «Поиск аномалий. Интенсивность»);

2) параметры «Периодичность анализа в сутках», «Части суток», «Дни недели» (см. «Поиск аномалий. Интенсивность»);

– «Наиболее длительные» – отмечает/не отмечает периоды с наибольшей продолжительностью, сумма длительностей которых не меньше значения параметра «Составляющие % трафика»;

– «Наименее длительные» – отмечает/не отмечает периоды с наименьшей продолжительностью, сумма длительностей которых не больше значения параметра «Составляющие % трафика».

Результатом анализа будет таблица за указанные интервал времени с указанной периодичностью с отмеченными периодами длительности, согласно установленным значениям (Рисунок 77).

№	День	Дата	Длительность	Комментарий
85	Ср	01.05.2013	6812	
86	Чт	02.05.2013	21940	Высокая длительность;
87	Пт	03.05.2013	13550	
88	Сб	04.05.2013	828	
89	Вс	05.05.2013	310	Низкая длительность;
90	Пн	06.05.2013	1750	
91	Вт	07.05.2013	1566	
92	Ср	08.05.2013	6828	
93	Чт	09.05.2013	1258	
94	Пт	10.05.2013	872	
95	Сб	11.05.2013	7910	
96	Вс	12.05.2013	8028	
97	Пн	13.05.2013	11534	
98	Вт	14.05.2013	5850	
99	Ср	15.05.2013	4998	

Рисунок 77 – Результат анализа длительности соединений абонента

− «Поиск аномалий. Собеседники» – отображает периоды с аномально большим числом новых и несущественных собеседников в указанном интервале времени. Новым собеседником считается впервые появившийся в данные сутки. Для выполнения анализа необходимо:

− в окне «Выбор статистического анализа» (Рисунок 70) установить флаг «Поиск аномалий – Собеседники», нажать «Готово»;

− выделить метод анализа в поле выбора метода анализа. При этом в поле ввода входных параметров отобразятся необходимые для заполнения поля (по умолчанию указаны «средние» значения параметров):

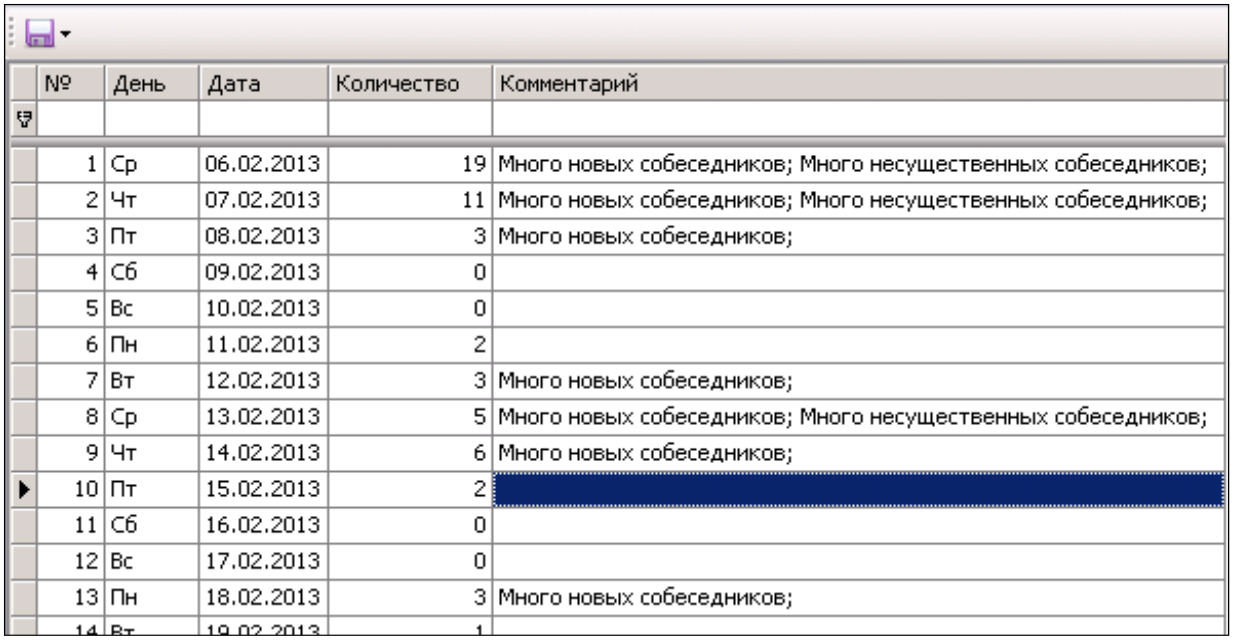
1) параметры группы «Общие» (см. «Поиск аномалий. Интенсивность»);

2) параметры «Периодичность анализа в сутках», «Части суток», «Дни недели» (см. «Поиск аномалий. Интенсивность»);

− «По числу новых собеседников» – отмечает/не отмечает периоды с появлением новых собеседников с установленной чувствительностью. Минимальная чувствительность – отмечает периоды с появлением новых собеседников больше среднего арифметического от общего числа новых собеседников; нормальная чувствительность – отмечает периоды с появлением новых собеседников больше среднего арифметического в два раза; максимальная чувствительность – больше среднего арифметического в три раза;

− «По числу существенных собеседников» – отмечает/не отмечает периоды с появлением большого количества НЕсущественных собеседников с установленной чувствительностью. Существенным считается собеседник, интенсивность связи с которым составляет процент, не меньше указанного в параметре «Существенные составляют % трафика». Параметр «Чувствительность» задается одним из трех значений, аналогичных указанных в параметре «По числу новых собеседников».

Результатом работы является таблица с указанной периодичностью с отмеченными аномалиями появления собеседников (Рисунок 78).



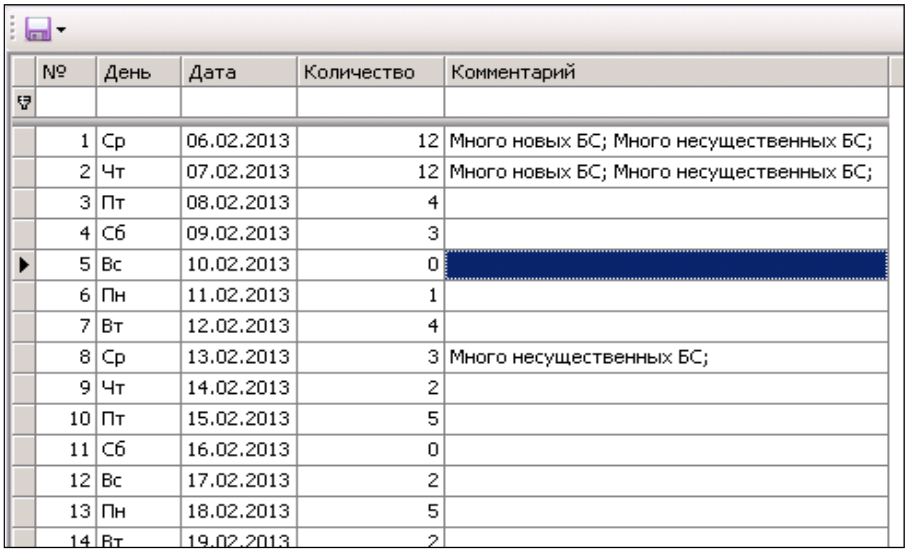
№	День	Дата	Количество	Комментарий
1	Ср	06.02.2013	19	Много новых собеседников; Много несущественных собеседников;
2	Чт	07.02.2013	11	Много новых собеседников; Много несущественных собеседников;
3	Пт	08.02.2013	3	Много новых собеседников;
4	Сб	09.02.2013	0	
5	Вс	10.02.2013	0	
6	Пн	11.02.2013	2	
7	Вт	12.02.2013	3	Много новых собеседников;
8	Ср	13.02.2013	5	Много новых собеседников; Много несущественных собеседников;
9	Чт	14.02.2013	6	Много новых собеседников;
10	Пт	15.02.2013	2	
11	Сб	16.02.2013	0	
12	Вс	17.02.2013	0	
13	Пн	18.02.2013	3	Много новых собеседников;
14	Вт	19.02.2013	1	

Рисунок 78 – Результат анализа поиска аномалий появления собеседников

По данному анализу можно сделать вывод, что 14.02.2013 имела место аномалия с большим количеством новых собеседников. Первые строки в качестве аномалии рассматривать не стоит, т.к. 06.02.2013 ВСЕ появившиеся собеседники в анализе в данные сутки являлись новыми.

«Поиск аномалий. Базовые станции» – отображает периоды с аномально большим количеством новых и несущественных базовых станций мобильных операторов. Входные параметры и настройки данного метода полностью идентичны указанным в методе «Поиск аномалий. Собеседники». Результатом анализа является таблица с отмеченными периодами с аномально большим появлением новых и несущественных базовых станций, по которым можно

сделать вывод о не характерном передвижении объекта в те или иные периоды (Рисунок 79).



№	День	Дата	Количество	Комментарий
1	Ср	06.02.2013	12	Много новых БС; Много несущественных БС;
2	Чт	07.02.2013	12	Много новых БС; Много несущественных БС;
3	Пт	08.02.2013	4	
4	Сб	09.02.2013	3	
5	Вс	10.02.2013	0	
6	Пн	11.02.2013	1	
7	Вт	12.02.2013	4	
8	Ср	13.02.2013	3	Много несущественных БС;
9	Чт	14.02.2013	2	
10	Пт	15.02.2013	5	
11	Сб	16.02.2013	0	
12	Вс	17.02.2013	2	
13	Пн	18.02.2013	5	
14	Вт	19.02.2013	2	

Рисунок 79 – Результат анализа поиска аномалий появления базовых станций

Так же, как и в случае с другими анализами аномалий, первые записи в таблице не стоит брать в основной расчет, т.к. все базовые станции в первый период будут новыми.

«Поиск аномалий. Сводная таблица» – представляет собой результат всех методов поиска аномалий в одной таблице. Задание входных параметров и настройки отображения представляют собой набор всех ранее описанных параметров для каждого из методов (Рисунок 80).

Рисунок 80 – Поле для ввода входных параметров сводной таблицы

Следует заметить, что представленный метод статистического анализа биллинговой информации позволяет эффективно расследовать различные виды преступлений.

1.6. Многомерные методы анализа биллинговой информации программного комплекса «Виток–3х»

Набор методов анализа «Многомерный» представляет собой анализ в табличном виде по выбранным параметрам с цветовой градацией в зависимости

от интенсивности с возможностью сортировки по выбранным пользователем критериям. Цветовая окраска результатов анализа обеспечивает эффективное визуальное восприятие результатов, не исследуя числовые значения анализа. Применяя последовательно тот или иной метод анализа, можно выявить закономерности в поведении абонента или наоборот, не характерные отступления от стандартных линий поведения.

Для всех методов анализа «Многомерный» предусмотрен одинаковый набор входных параметров и настроек (Рисунок 81).

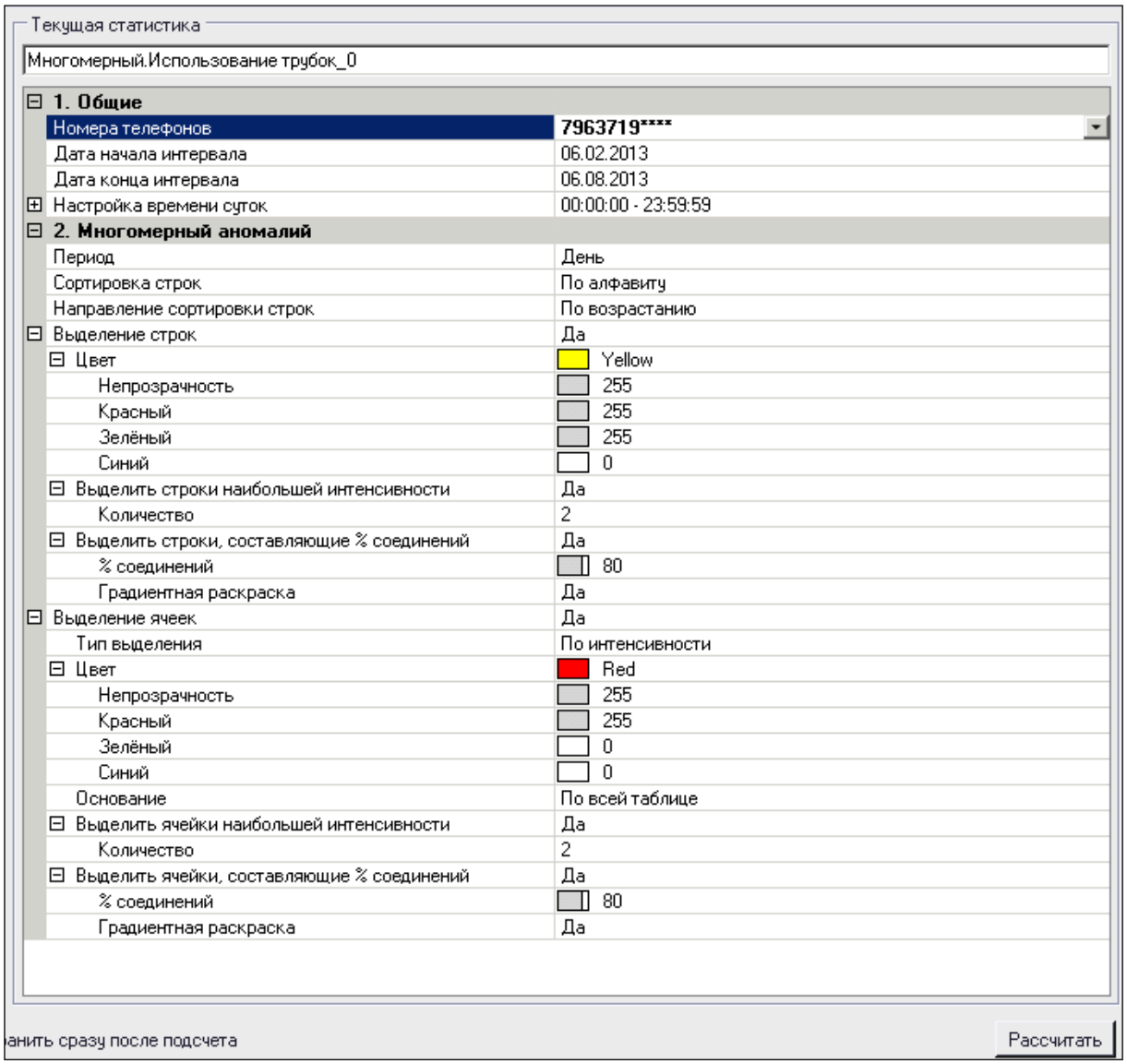


Рисунок 81 – Поле для ввода входных параметров и настроек отображения

В разделе «Текущая статистика» предусмотрены следующие поля для ввода данных:

- «Общие»-идентичны указанным в методах «Поиск аномалий»;
- «Период»-задает временные интервалы для анализа. С помощью данного параметра возможно исследование как дней, недель и месяцев, так и частей дня (в том числе и по часам и частям дня). Например, исследование только рабочего времени абонента или только ночной активности;
- «Сортировка строк» - отображает строки результирующей таблицы по алфавиту (в том числе по порядку цифр, начиная с первой), интенсивности заданного параметра и по первому соединению (дата и время). Данный параметр позволяет визуально оценить, например, самые активные базовые станции абонента или самых частых собеседников;
- «Направление сортировки строк» – задает отображение сортировки строк либо от минимальной интенсивности к максимальной, либо наоборот;
- «Выделение строк» – список параметров для цветового выделения строк результирующей таблицы анализа с цветовой градацией в зависимости от интенсивности. Возможна следующая настройка выделения строк таблицы:

1) «Цвет» – фоновая окраска строки по системе RGBA. Пользователю доступны все возможные оттенки с регулируемой степенью прозрачности (Рисунок 82);

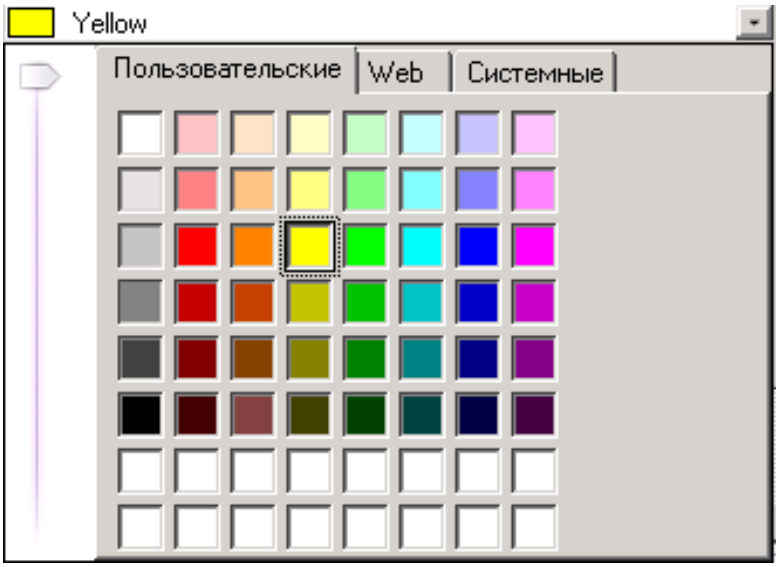


Рисунок 2 – Окно выбора цвета выделения строки

2) «Выделить строки наибольшей интенсивности» – включает фоновую окраску строк с наибольшей интенсивностью (строки- лидеры). Строк может быть несколько с одинаковой наибольшей интенсивностью. Параметр «Количество» указывает, сколько наибольших интенсивностей выделять, начиная с максимальной. Строки будут окрашены в одинаково насыщенный цвет, выбранный пользователем в параметре «Цвет» (см. выше). Данная опция помогает визуально быстро найти записи с наибольшей интенсивностью в больших результирующих таблицах;

3) «Выделить строки, составляющие % соединений» – отмечает строки, сумма интенсивностей которых составляет указанный процент трафика всех соединений. Строки будут отмечены менее насыщенным цветом, нежели строки-лидеры. Если включен параметр «Градиентная окраска», то насыщенность окраски будет возрастать от строк с меньшей интенсивностью к большей;

– «Выделение ячеек» - список параметров для выделения внутренних ячеек результирующей таблицы анализа с цветовой градацией в зависимости от интенсивности. Пользователю доступны два вида выделения:

«По интенсивности» - тип выделения, аналогичный при выделении строк. Пользователь выбирает цвет выделения, определяет, выделять ли ячейки наибольшей интенсивности (и их количество), и выделять ли ячейки с градацией цвета, составляющие указанный процент от общего трафика соединений. Параметр «Основание» определяет, осуществлять подсчет по всей таблице или отдельно по каждой строке. Если выбран тип «По всей таблице», то самым насыщенным цветом выделяются наиболее интенсивные ячейки во ВСЕЙ таблице, менее насыщенным ячейки с указанным процентом соединений от общего трафика (Рисунок 3).

07:00	24	13.03.2013 7:53:16	18.07.2013 7:53:41									
08:00	88	04.03.2013 8:01:00	31.07.2013 8:53:18									
09:00	344	12.02.2013 9:55:18	06.08.2013 9:45:24							4		
10:00	644	06.02.2013 10:34:54	05.08.2013 10:34:16	12	16	10			4	2	4	
11:00	800	06.02.2013 11:02:09	02.08.2013 11:26:33	18	12	10	2	4		4		
12:00	732	07.02.2013 12:04:42	05.08.2013 12:50:41		16	2		2	4	8	6	4
13:00	610	06.02.2013 13:04:31	06.08.2013 13:11:17	20		2			2	2	16	4
14:00	894	06.02.2013 14:09:11	06.08.2013 14:38:03	30	6			2	6	8	24	22
15:00	732	06.02.2013 15:05:48	06.08.2013 15:24:35	6	40	4	2	4		4	4	6
16:00	808	06.02.2013 16:12:11	05.08.2013 16:57:49	16	2	4	4		8	8	4	
17:00	672	06.02.2013 17:15:32	06.08.2013 17:59:39	2	2		2		4	2	2	
18:00	544	07.02.2013 18:05:16	06.08.2013 18:47:20		4				4	6	2	

Рисунок 83 – Выделение ячеек «По всей таблице»

Если выбран тип «По рядам», самым насыщенным цветом выделяются наиболее интенсивные ячейки в КАЖДОЙ строке, менее насыщенным - ячейки с указанным процентом интенсивности от общего трафика (Рисунок 84).

08:00	88	04.03.2013 8:01:00	31.07.2013 8:53:18									
09:00	344	12.02.2013 9:55:18	06.08.2013 9:45:24							4		
10:00	644	06.02.2013 10:34:54	05.08.2013 10:34:16	12	16	10			4	2	4	
11:00	800	06.02.2013 11:02:09	02.08.2013 11:26:33	18	12	10	2	4		4		
12:00	732	07.02.2013 12:04:42	05.08.2013 12:50:41		16	2		2	4	8	6	4
13:00	610	06.02.2013 13:04:31	06.08.2013 13:11:17	20		2			2	2	16	4
14:00	894	06.02.2013 14:09:11	06.08.2013 14:38:03	30	6			2	6	8	24	22
15:00	732	06.02.2013 15:05:48	06.08.2013 15:24:35	6	40	4	2	4		4	4	6
16:00	808	06.02.2013 16:12:11	05.08.2013 16:57:49	16	2	4	4		8	8	4	
17:00	672	06.02.2013 17:15:32	06.08.2013 17:59:39	2	2		2		4	2	2	
18:00	544	07.02.2013 18:05:16	06.08.2013 18:47:20		4				4	6	2	

Рисунок 84 – Выделение ячеек «По рядам»

Запись в таблице в 13:00 при выборе типа «По рядам» попадает в наиболее интенсивные (Рисунок 84).

«По интервалам» - тип выделения, при котором в КАЖДОЙ строке отмечен интервал между первой записью с ненулевой интенсивностью и последней. Данная опция значительно увеличивает визуальное восприятие результирующей таблицы (Рисунок 5).

Собеседник	Всего	Первое соединение	Последнее соединение	06.02.2013	07.02.2013	08.02.2013	09.02.2013	10.02.2013	11.02.2013	12.02.2013	13.02.2013
7905782	12	06.02.2013 16:18:42	07.02.2013 14:02:46	8	4						
7908750	2	13.02.2013 18:05:34	13.02.2013 18:05:34								2
7910234	8	07.02.2013 14:39:20	12.02.2013 14:45:21		4	2				2	
7910409	12	08.02.2013 16:22:27	10.02.2013 12:14:27			2	8	2			
7915043	2	13.02.2013 13:29:38	13.02.2013 13:29:38								2
7915055	8	06.02.2013 17:15:32	12.02.2013 19:12:07	2						6	
7915225	8	08.02.2013 20:27:30	10.02.2013 14:05:47			2		6			
7915302	2	06.02.2013 11:57:56	06.02.2013 11:57:56	2							
7916536	4	12.02.2013 12:01:16	13.02.2013 16:48:04							2	2
7916637	4	11.02.2013 20:26:36	11.02.2013 20:26:42						4		
7916828	26	06.02.2013 16:12:11	13.02.2013 19:10:21	2	4	4	4	2	6	2	2
7916899	10	08.02.2013 21:29:23	13.02.2013 12:16:12			2		2		4	2

Рисунок 85 – Тип выделения «По интервалам»

Из данного анализа (Рисунок 85) визуально просто можно сделать вывод, что целевой абонент начал общение с абонентом 7915225**** 08.02.2013 и закончил 10.02.2013. Ниже описаны используемые методы многомерного анализа:

«Многомерный. Использование трубок» - отображает использованные целевым абонентом IMEI номера мобильных телефонов за указанный временной интервал (Рисунок 86).

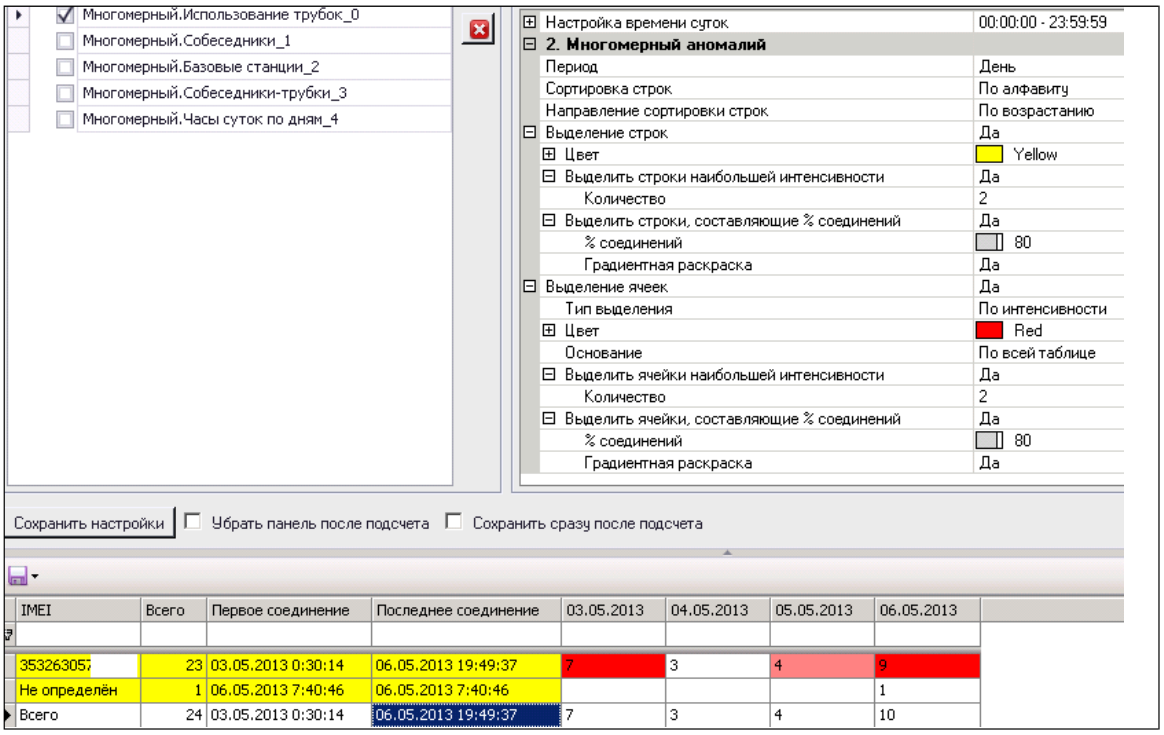


Рисунок 86 – Анализ использования трубок

Из данной результирующей таблицы можно сделать вывод, что целевой абонент использовал один номер IMEI за указанный период (запись в столбце «Не определен» говорит о некорректных данных от сотовых операторов). В данной таблице выделены строки и ячейки с наибольшей интенсивностью (количество «2») и градиентная раскраска менее интенсивных.

«Многомерный. Собеседники» - отображает интенсивность общения целевого абонента со всеми собеседниками за указанный интервал с выбранной

периодизацией (Рисунок 87).

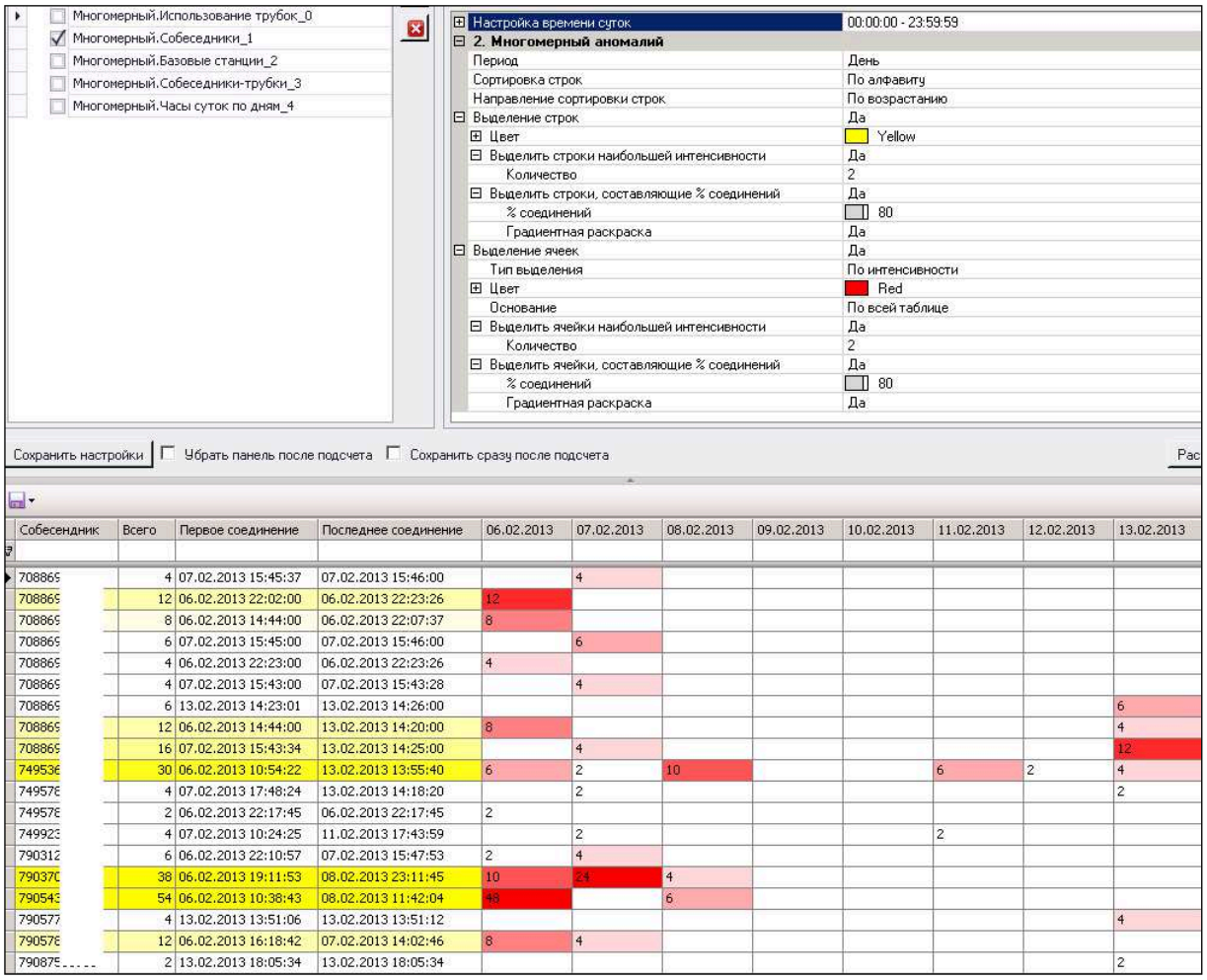


Рисунок 87 – Анализ интенсивности общения с абонентами

Из данного анализа можно сделать вывод об интенсивности общения с тем или иным собеседником, определить начало и конец общения и проследить всю историю общения.

Изменяя параметр «Период», можно оценить общение с собеседником в той или иной ситуации. А так результат выглядит после сортировки строк по суммарной интенсивности и убыванию (Рисунок 88).

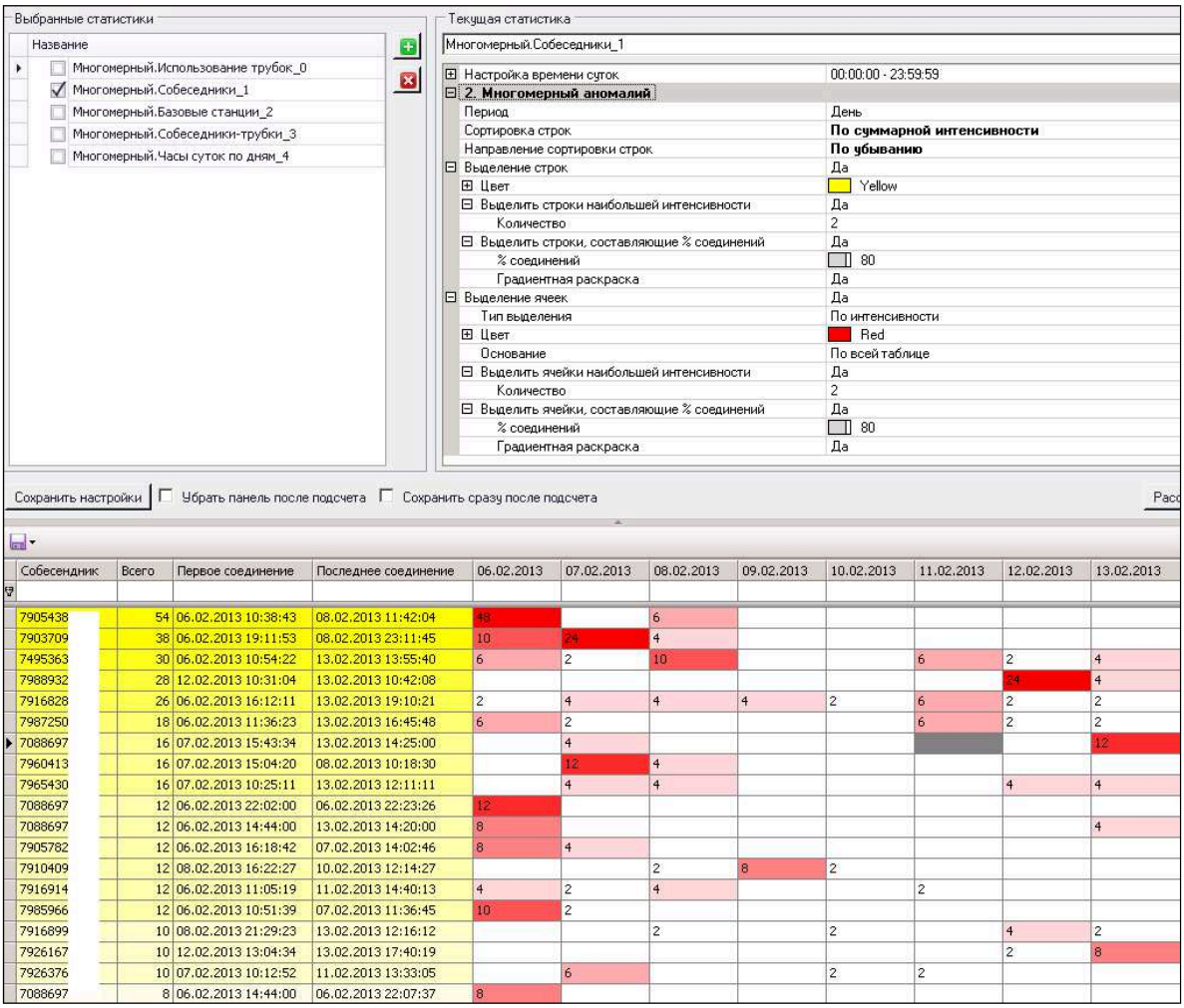


Рисунок 88 – Результат анализа собеседников

Выбрав период анализа «Дни недели», можно сделать вывод например, о необходимости общения целевого абонента с другими абонентами в выходные (будни). Из таблицы ниже видно, что с абонентом 7495593**** целевой абонент общается преимущественно в воскресенье, а с абонентом 7985444**** только в будни (Рисунок 9) (возможно, деловой партнер или человек, с которым проходят выходные). Для уточнения можно применить анализ базовых станций.

Собеседник	Всего	Первое соединение	Последнее соединение	Пн	Вт	Ср	Чт	Пт	Сб	Вс
798544	56	07.02.2013 10:26:43	28.06.2013 17:42:57	6	8		10	32		
792660	54	11.02.2013 10:04:00	18.07.2013 16:47:18	28	8		8	10		
708869	52	07.02.2013 15:45:37	05.08.2013 19:10:37	8			14	16	4	10
773689	52	01.05.2013 15:56:07	17.07.2013 21:10:57	2	6	20		12	12	
792620	50	28.02.2013 13:43:54	06.08.2013 17:07:30	26	8	6	8		2	
708869	48	06.02.2013 14:44:00	05.08.2013 16:45:00	10		34				4
790247	48	06.03.2013 20:01:48	06.08.2013 9:06:48	6	10	4	2	8	6	12
792616	48	12.02.2013 13:04:34	04.07.2013 19:06:20	16	6	16	4	6		
749559	46	03.03.2013 21:25:08	01.08.2013 17:51:01		4	2	6	4	8	22
791023	46	07.02.2013 14:39:20	06.08.2013 9:45:24	10	8	4	16	8		

Рисунок 89 – Анализ общения с собеседниками

«Многомерный. Базовые станции» - отображает интенсивность общения абонента на тех или иных базовых станциях. Зная географическое местоположение базовых станций операторов мобильной связи, можно сделать вывод о соединениях абонента в той или иной зоне в указанный период (Рисунок 90).

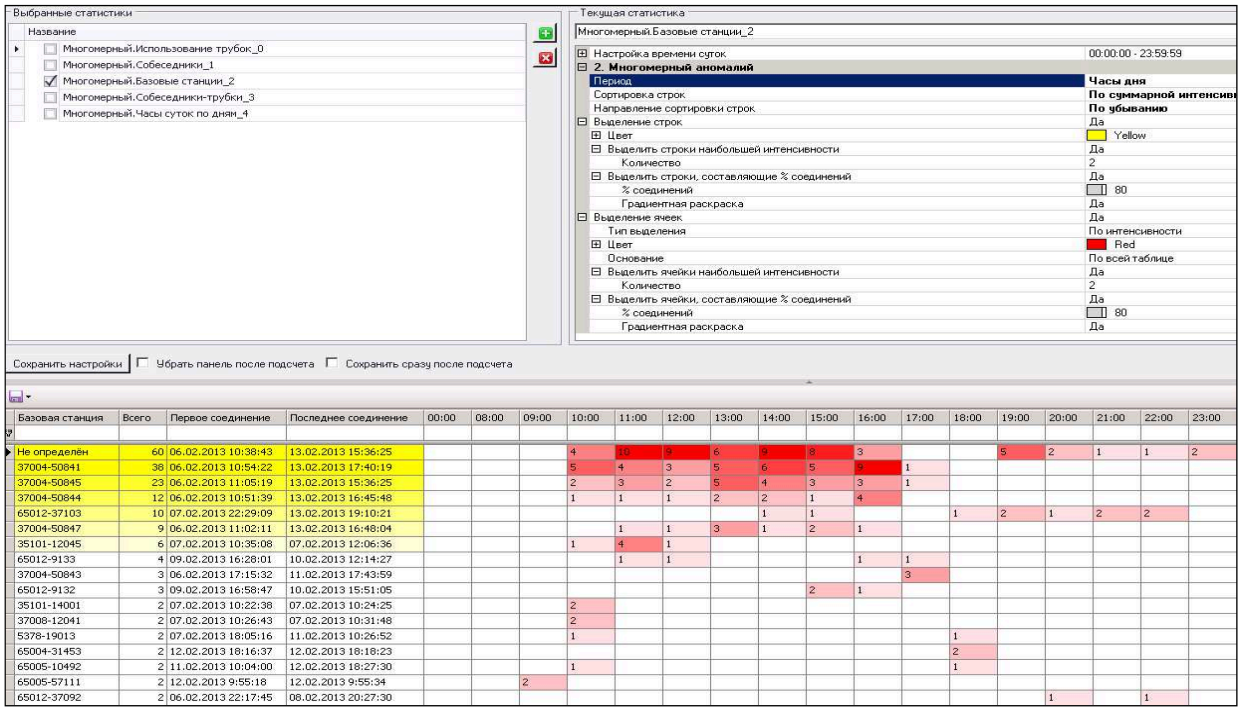


Рисунок 90 – Результат анализа базовых станций

Например, из данной таблицы (после сортировки по интенсивности и направлению и выбора периода «Часы дня») предположительно можно сделать вывод об интенсивности соединений в период с 10:00 до 16:00 в районе трех базовых станций. Это, скорее всего, свидетельствует о месте и времени работы абонента. Изменив параметр «Период» на «Дни недели» можно оценить активность абонента в выходные/будни в той или иной географической зоне.

«Многомерный. Собеседники трубки» - отображает информацию о том, с каких IMEI целевой абонент общался с другими собеседниками (Рисунок 91).

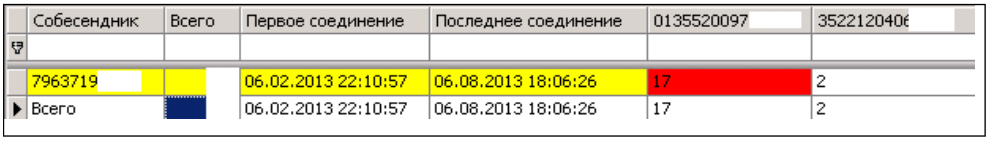


Рисунок 91 – Анализ IMEI собеседников

Из таблицы можно сделать вывод о том, что за указанный период целевой абонент дважды общался с собеседником 7963719**** с нехарактерного для него IMEI номера.

«Многомерный. Часы суток по дням» - позволяет оценить интенсивность общения целевого абонента в течение суток за указанный интервал времени. Характерной особенностью данного анализа является отсутствие параметра «Период». Из анализа можно сделать вывод о всплесках интенсивности в тот или иной период, либо, наоборот, о падении интенсивности общения (Рисунок 92).

Час суток	Всего	Первое соединение	Последнее соединение	06.02.2013	07.02.2013	08.02.2013	09.02.2013	10.02.2013	11.02.2013	12.02.2013	13.02.2013
00:00	0										
01:00	0										
02:00	0										
03:00	0										
04:00	0										
05:00	0										
06:00	0										
07:00	0										
08:00	0										
09:00	4	12.02.2013 9:55:18	12.02.2013 9:55:34							4	
10:00	48	06.02.2013 10:34:54	13.02.2013 10:42:08	12	16	10			4	2	4
11:00	50	06.02.2013 11:02:09	12.02.2013 11:56:40	18	12	10	2	4		4	
12:00	38	07.02.2013 12:04:42	13.02.2013 12:16:12		16	2		2	4	8	6
13:00	42	06.02.2013 13:04:31	13.02.2013 13:55:40	20		2			2	2	16
14:00	76	06.02.2013 14:09:11	13.02.2013 14:26:00	30	6			2	6	8	24
15:00	64	06.02.2013 15:05:48	13.02.2013 15:36:25	6	40	4	2	4		4	4
16:00	46	06.02.2013 16:12:11	13.02.2013 16:48:04	16	2	4	4		8	8	4
17:00	14	06.02.2013 17:15:32	13.02.2013 17:40:19	2	2		2		4	2	2
18:00	16	07.02.2013 18:05:16	13.02.2013 18:05:34		4				4	6	2
19:00	14	06.02.2013 19:11:53	13.02.2013 19:10:21	10						2	2
20:00	8	08.02.2013 20:27:30	11.02.2013 20:26:42			2		2	4		
21:00	6	08.02.2013 21:29:23	09.02.2013 21:57:16			4	2				
22:00	32	06.02.2013 22:02:00	08.02.2013 22:12:21	28	2	2					

Рисунок 92 – Анализ интенсивности общения по часам суток

Из данного анализа нетрудно сделать вывод об активности абонента в течение дня, его рабочем времени (с 10:00 до 16:00) и не характерном всплеске активности 06.02.2014 после 22:00, что может свидетельствовать о вынужденном изменении в поведении.

Оператору доступна настройка взаиморасположения рабочих окон. Для этого необходимо, удерживая левую клавишу мыши, перетащить закладку с названием окна на соседнее окно, при этом отобразится инструмент навигации между окнами (Рисунок 93).

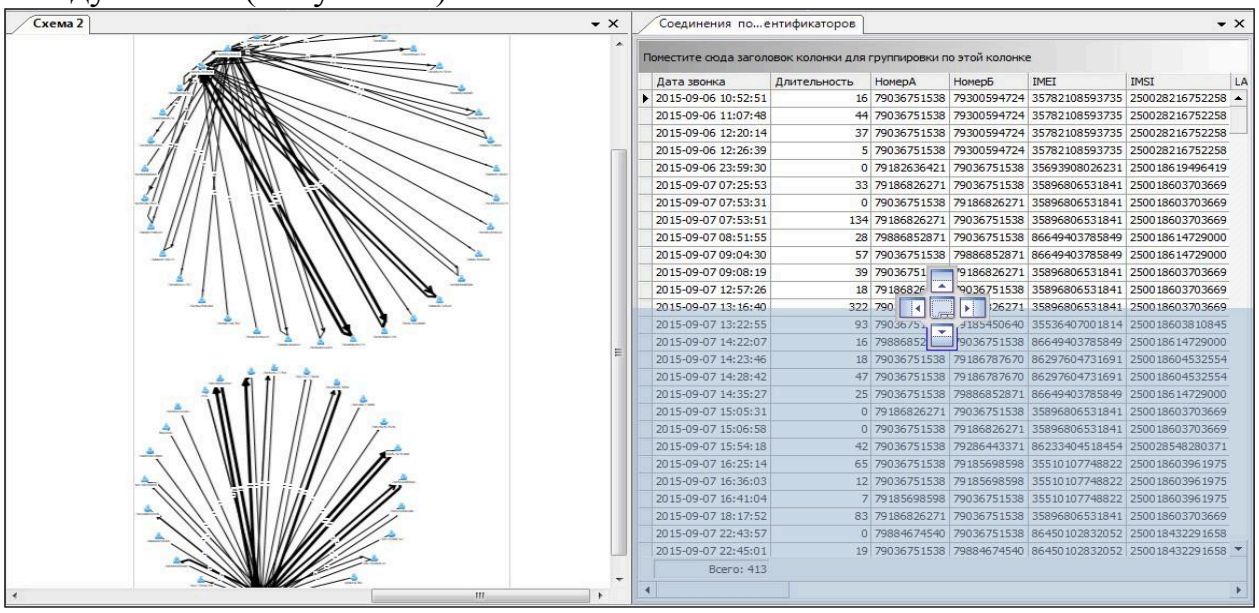


Рисунок 93 – Взаиморасположение окон

Для удобства работы с приложением во вкладке «Окна» имеется окно заметок (Рисунок 94).

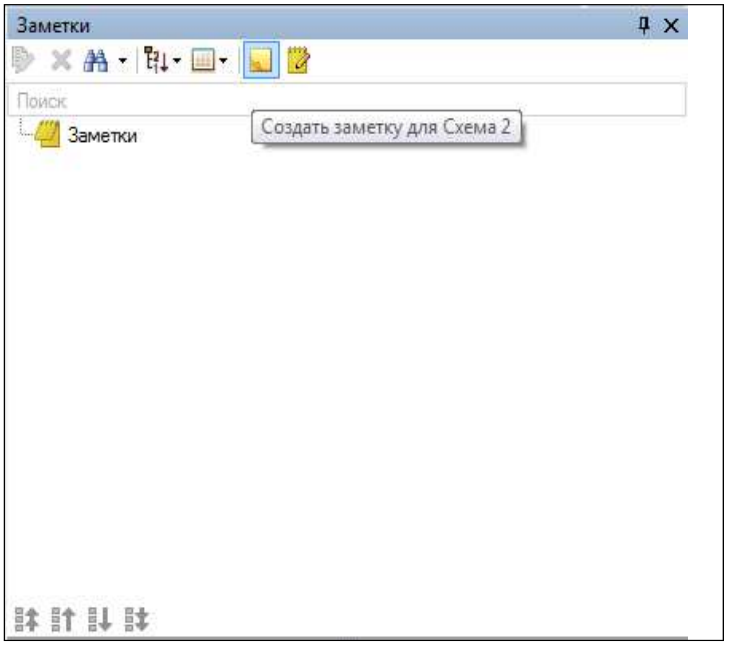


Рисунок 94 – Окно Заметки

Текст заметки формируется в нижней части окна (Рисунок 95).

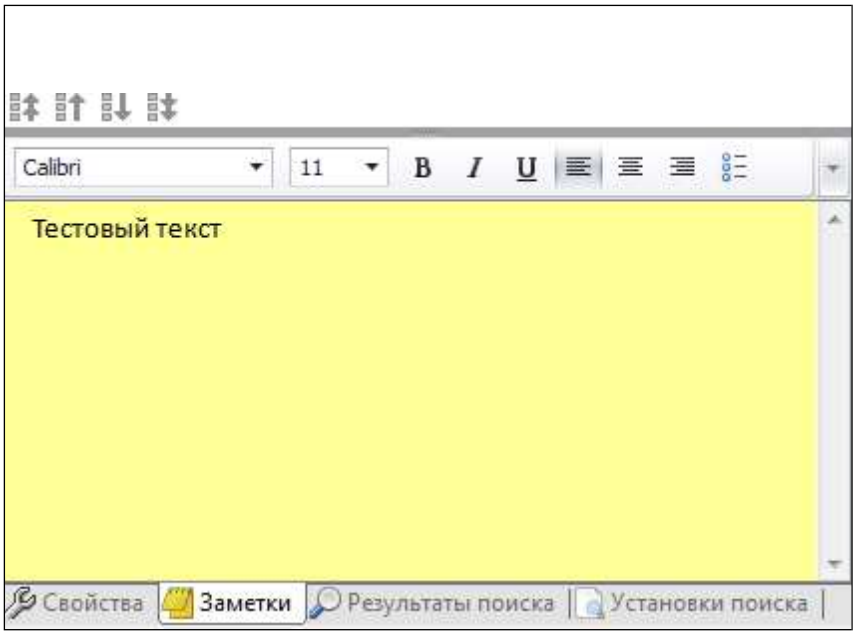


Рисунок 95 - Окно заметки

1.7. Построение, сохранение, вывод на печать отчетов по анализу биллинговой информации

После проведенного расследования анализа биллинговой информации в рассматриваемом программном комплексе существует возможность формирования, редактирования и сохранения отчета о проделанной работе. Для построения отчета необходимо выполнить действия, указанные на рисунке 96.

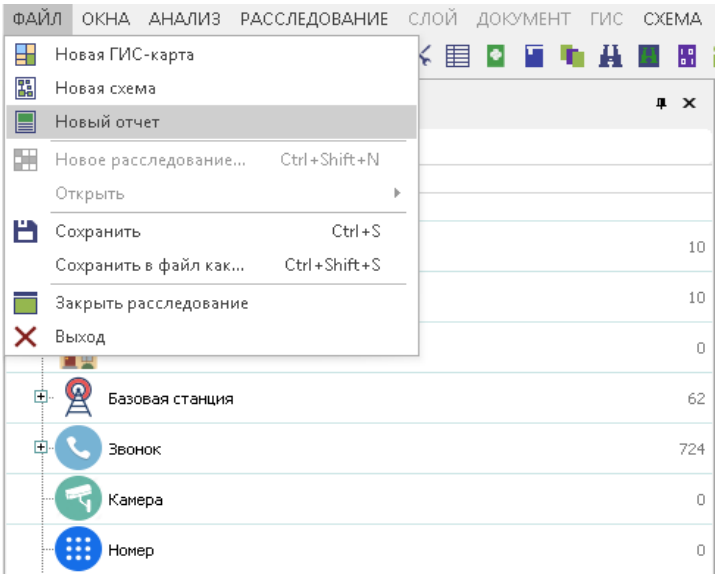


Рисунок 96 – Построение отчета

В меню «Файл» выбираем пункт «Новый отчет». Следует заметить, что отчет может быть пустым или же с объектами и связями (по результатам всех поисков), присутствующими в расследовании (Рисунок 97, 98).

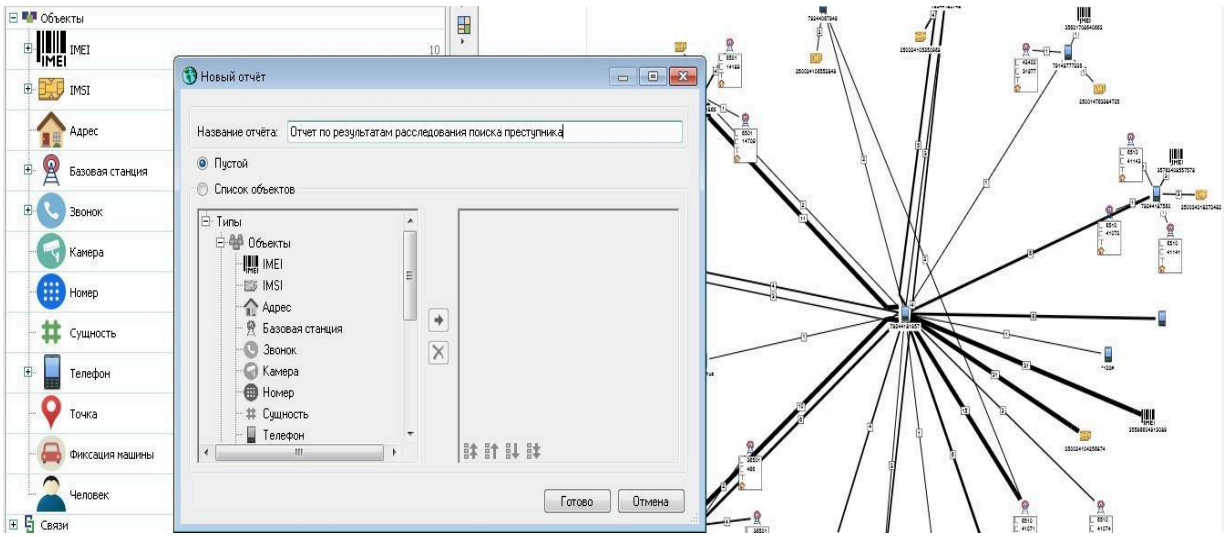


Рисунок 97– Пустой отчет

Для формирования отчета по проведенному расследованию необходимо выбрать пункт «Список объектов» (объекты в левом окне станут активными) и написать название данного отчета. Далее необходимо выбрать типы добавляемых в отчет объектов с помощью левой клавиши мыши и нажать на

кнопку со стрелочкой, расположенной между двумя окнами. После данного действия соответствующие объекты появятся в правом окне.

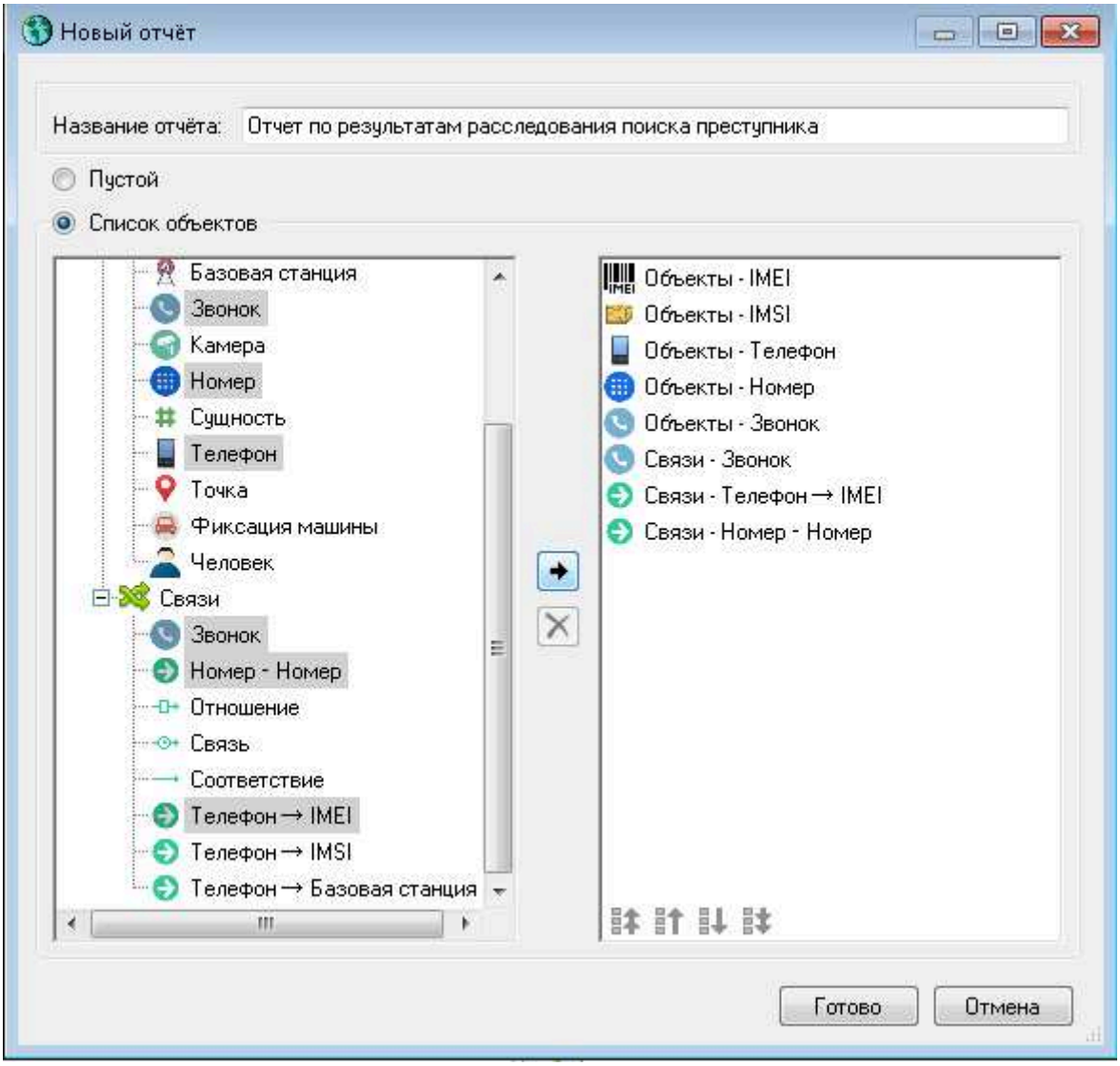


Рисунок 98 – Отчет с объектами и связями

Достаточно важно заметить, что объекты, представленные на приведенном выше рисунке можно выделять выборочно при нажатой клавише «Ctrl». Кроме того, случайно добавленные объекты в левом окне можно также выборочно удалять, предварительно их выделив, с помощью кнопки удаления, расположенной по центру окна.

После нажатия кнопки «Готово» появится отчет (Рисунок 99). При этом в отчет можно добавлять различные объекты, которые использовались в расследовании, проводить ряд операций, видоизменять текст, вносить схемы связей из расследования и т.д.

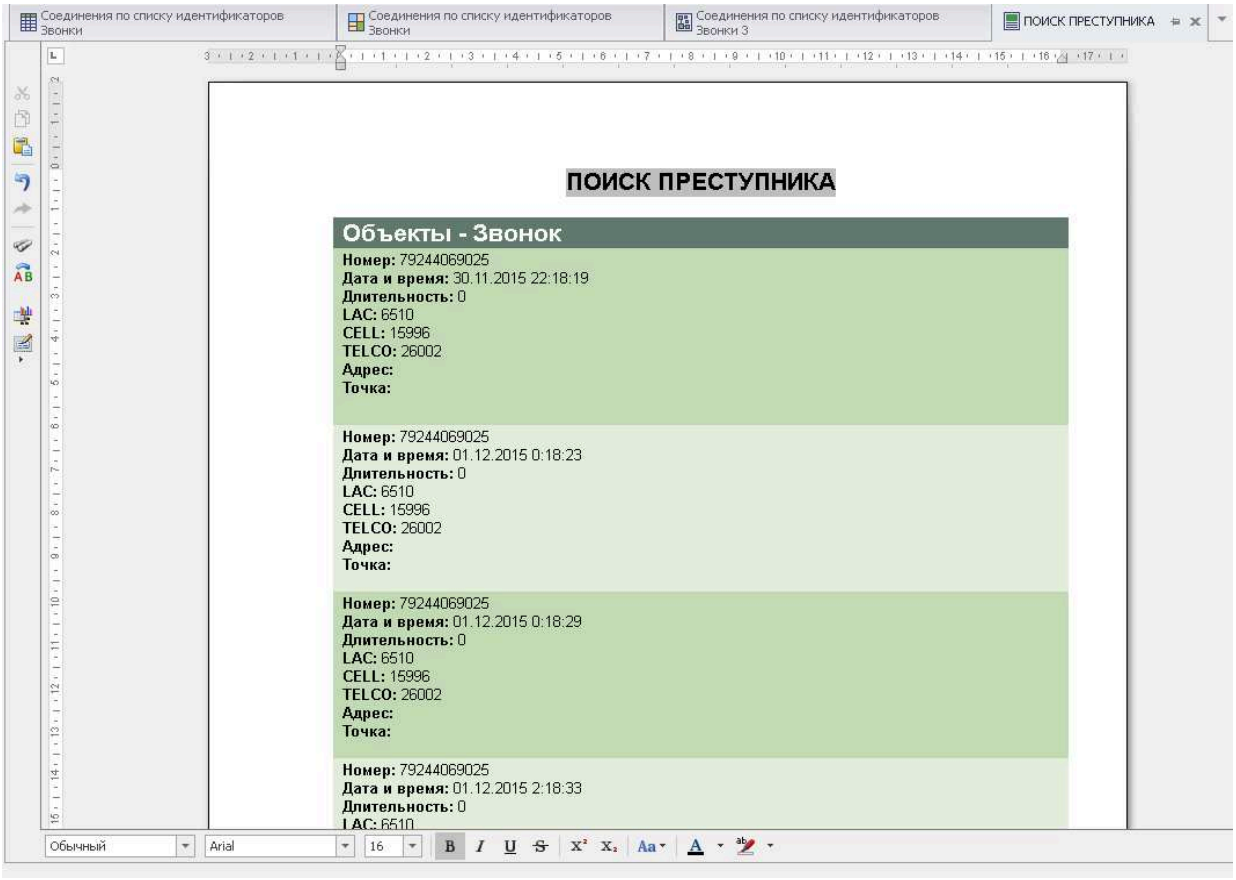


Рисунок 99 – Отчет после нажатия кнопки «Готово»

В открывшемся окне отчета слева расположена панель инструментов позволяющая его редактировать. При этом можно реализовать следующие операции:

- вырезать;
- копировать;
- вставить;
- отменить;
- вернуть;
- найти;
- заменить;
- вставить объекты…;
- вставить описательный атрибут.

Описательный атрибут позволяет вставить в формируемый отчет название расследования, название отчета, информацию о пользователе создавшем отчет, дату и время создания отчета.

Кроме того, в нижней части рассматриваемого окна расположена стандартная панель редактирования текста.

Основные компоненты, позволяющие редактировать отчет о проведенном расследовании, представлены на рисунке 100.

Рисунок 100 – Редактирование отчета

Для дополнения отчета данными из схем связей необходимо в панели инструментов выбрать кнопку «Вставить объекты…». Далее необходимо выбрать «Вид данных» и «Тип» для вставки в отчет и нажать кнопку «Вставить» (Рисунок 101).

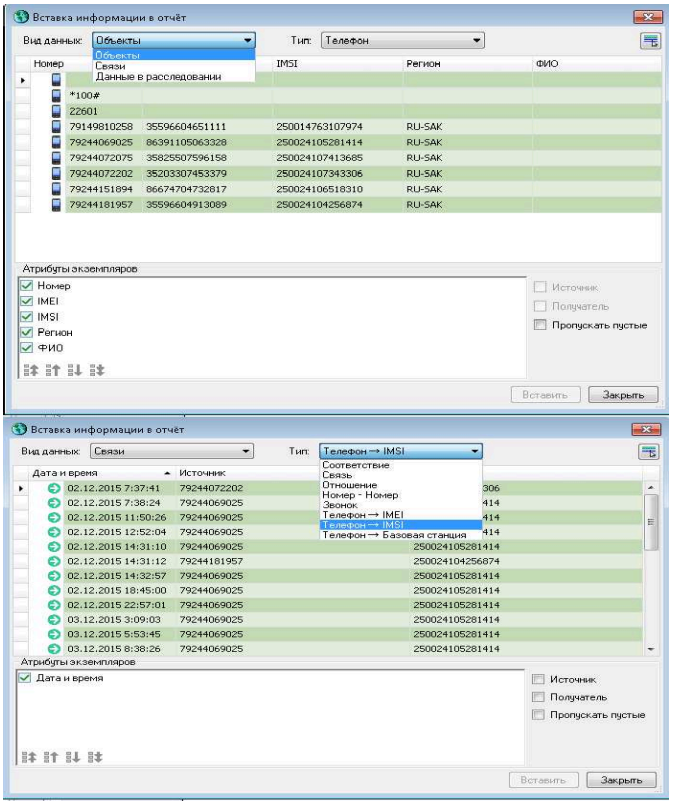
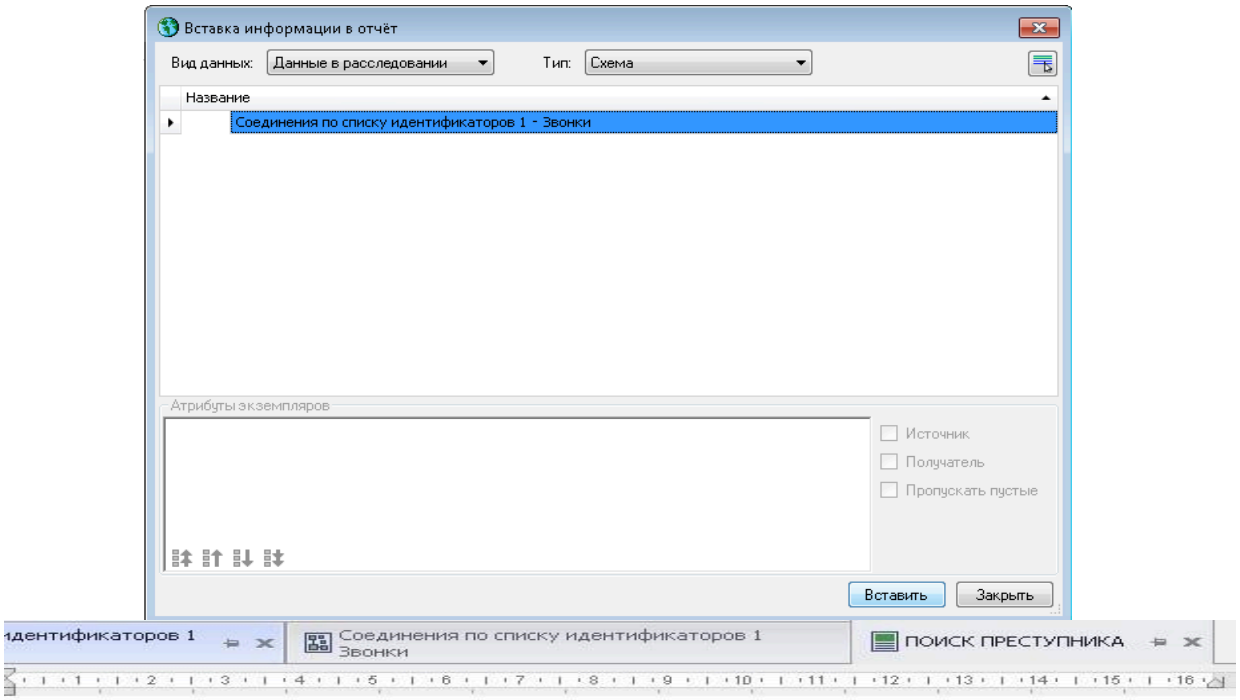


Рисунок 101 – Добавление данных в отчет

Представляется целесообразным рассмотреть порядок добавления в отчет схемы связей объектов, использовавшихся в расследовании, и ГИС – карты. Выбираем пиктограмму «Вставить объекты…». Указываем вид данных «Данные из расследования», а тип «Схема». Выделяем появившуюся строчку и нажимаем кнопку «Вставить». В результате в отчете появляется схема связей, представленная в виде графа (Рисунок 102).



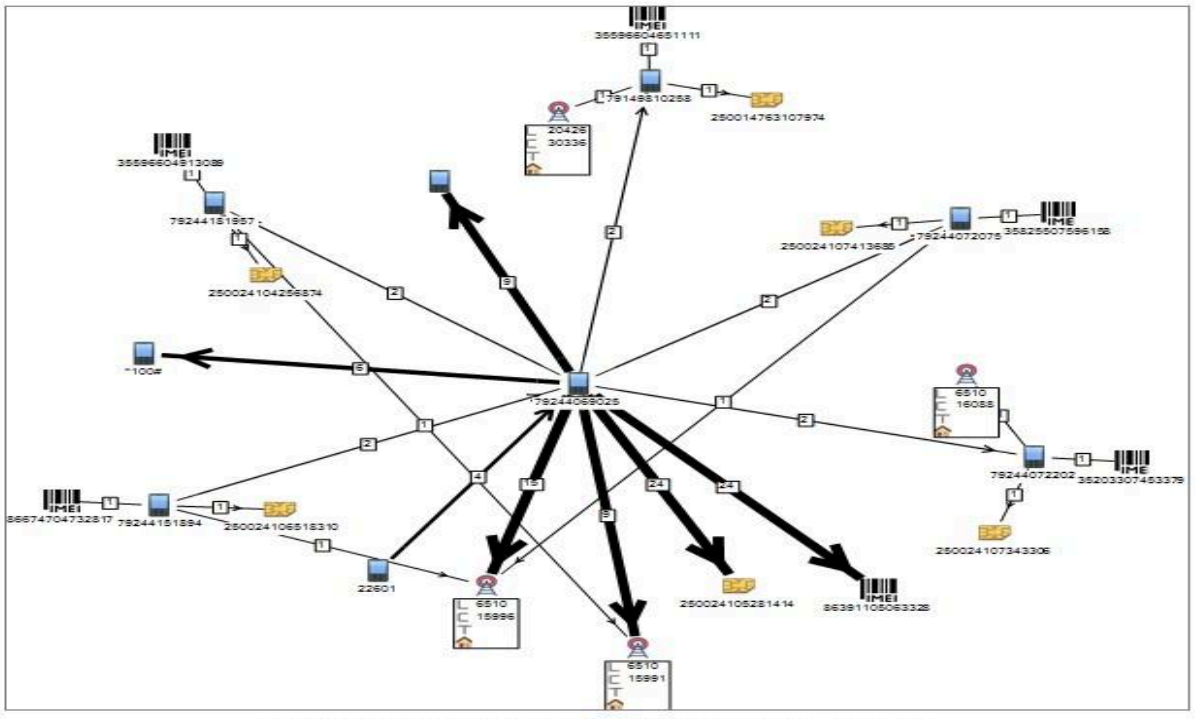


Рисунок 102 – Добавление схемы в отчет

Для добавления ГИС-карты в отчет проводятся действия, аналогичные действиям, представленным выше, лишь с той разницей, что при выборе параметра «Тип», следует указать «ГИС-карта». В результате в отчете должна появиться ГИС-карта с данными, использованными при расследовании (Рисунок 103).

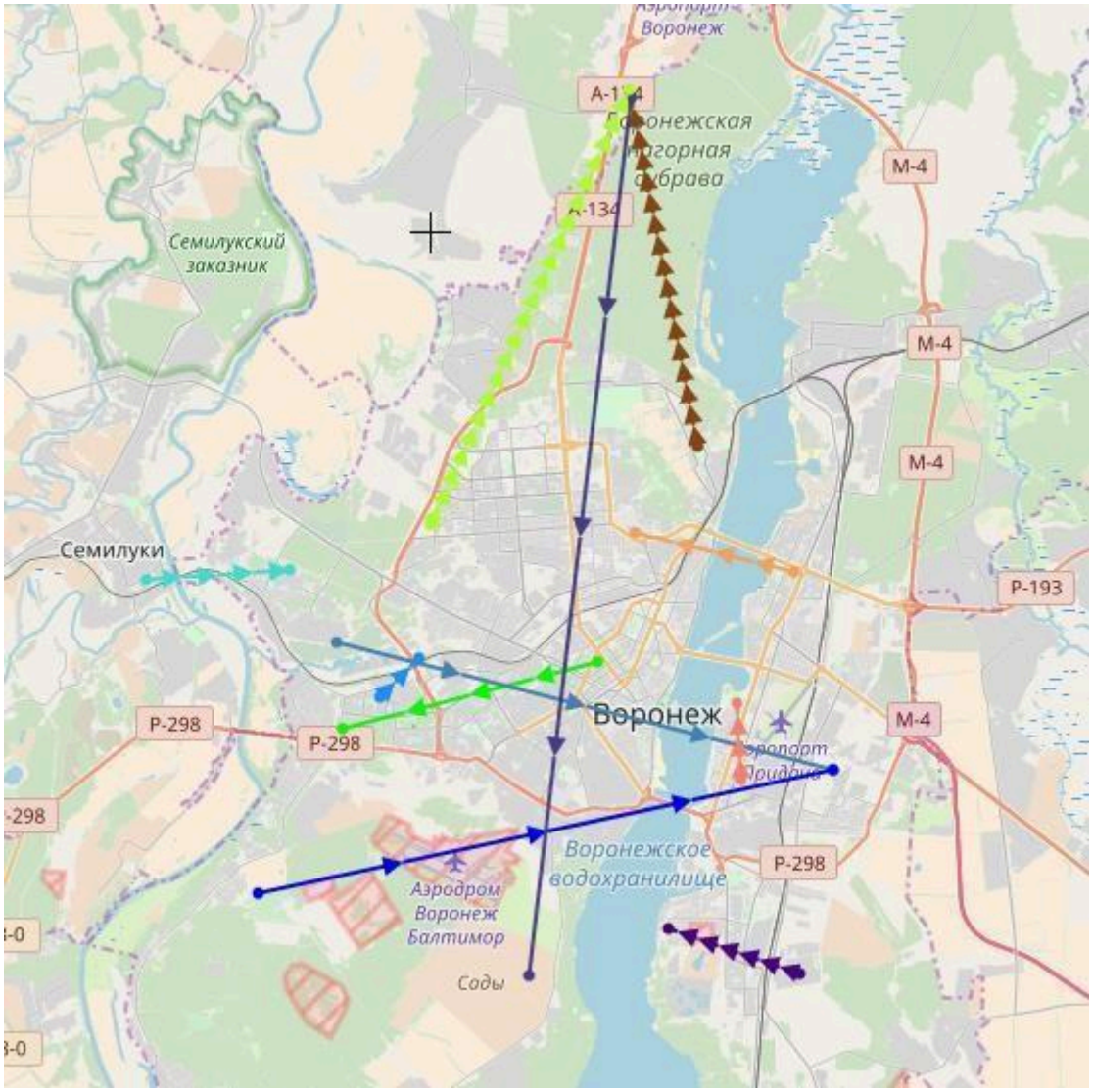


Рисунок 103 – Добавление ГИС-карты в отчет Для сохранения отчета необходимо:

- выбрать пункт меню «Отчет»;
- выбрать элемент меню «Сохранить как» или клавиша F12 (Рисунок 104).

После указанных действий откроется диалоговое окно, в котором необходимо указать путь сохранения файла, и формат, в котором необходимо сохранить отчет.

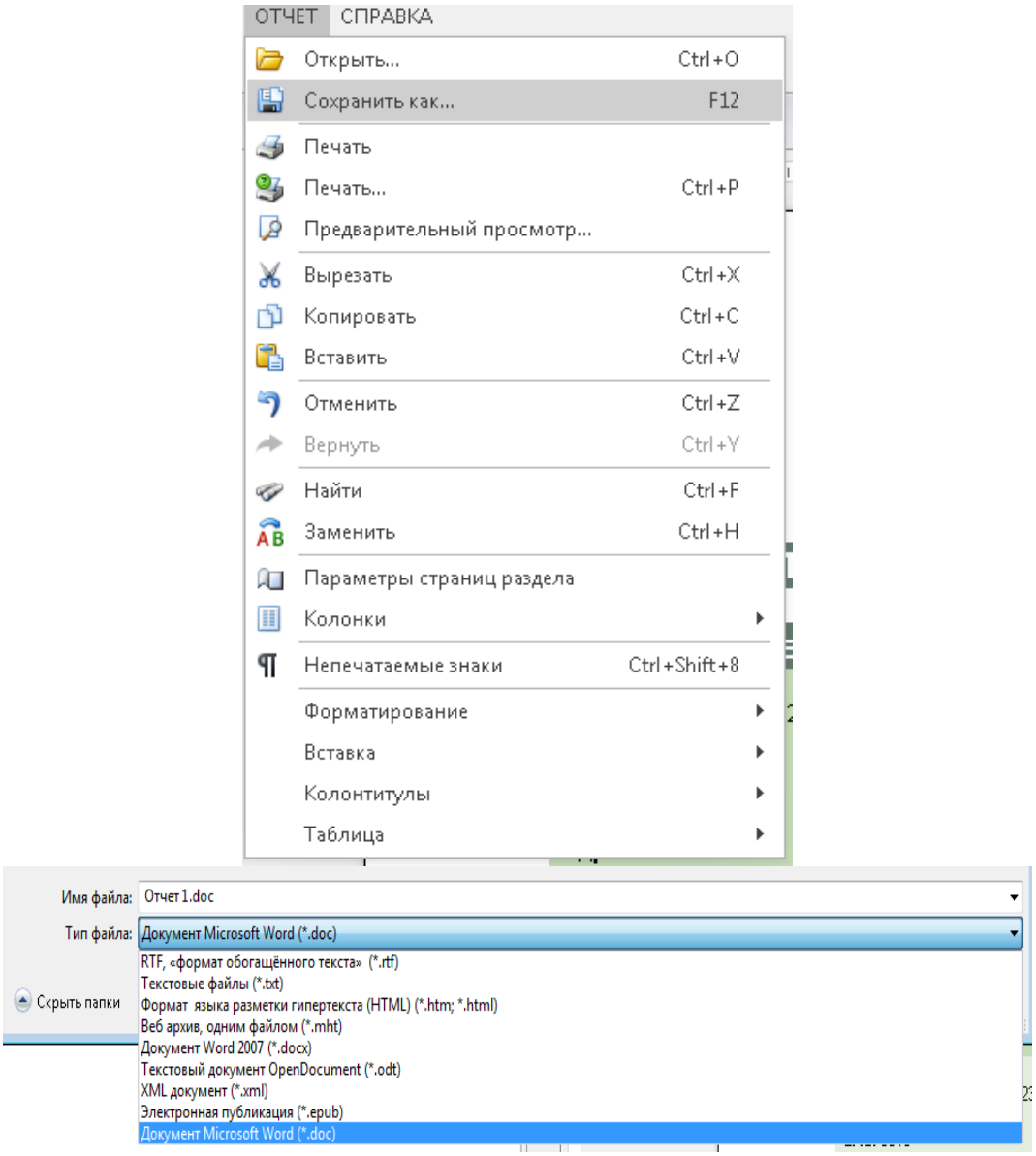


Рисунок 104 – Сохранение отчета

Следует заметить, что все операции, проводимые с отчетом, представлены в пункте основного меню «Отчет». Для печати отчета необходимо в панели инструментов нажать на кнопку «Печать». Если необходимо убедиться в правильности и безошибочности сформированного отчета, можно выбрать пункт «Предварительный просмотр» (Рисунок 105).

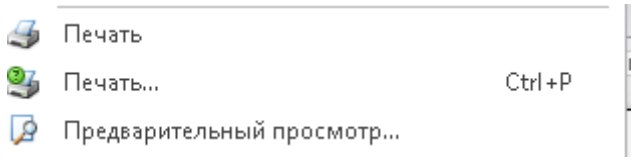


Рисунок 105 – Предварительный просмотр

Интерфейс программного обеспечения при предварительном просмотре, представлен на рисунке 106.

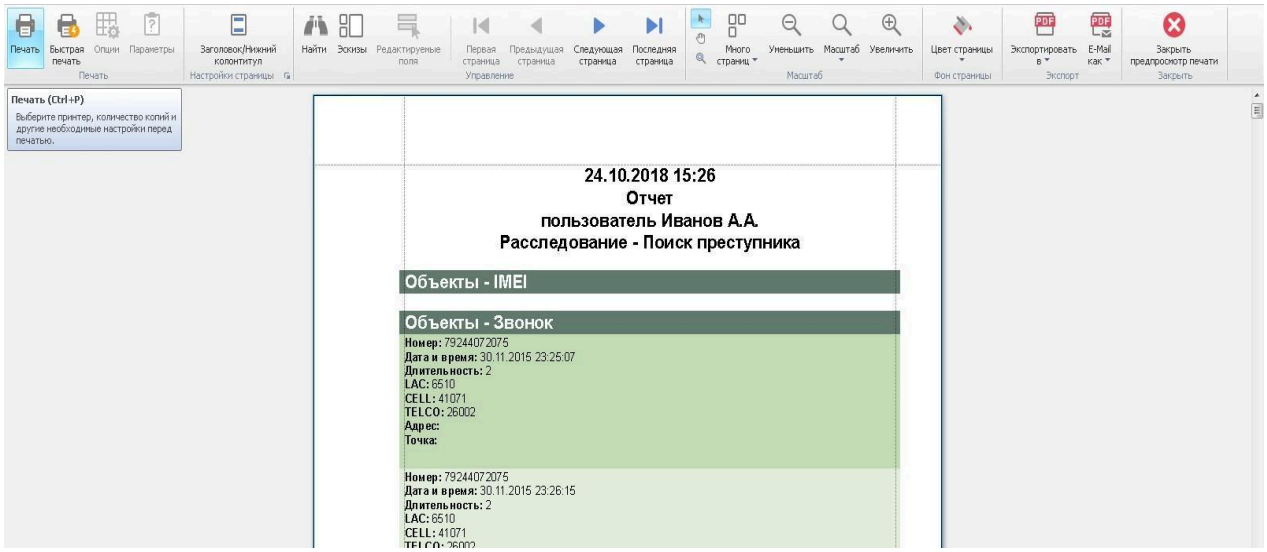


Рисунок 106 – Интерфейс программного обеспечения при предварительном просмотре

Таким образом, если все действия выполнены верно, то сформированный отчет отправится на печать.

2. СТРУКТУРА И ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПРОГРАММНОГО СРЕДСТВА «OCTOPUS»

2.1. Основные компоненты и структура программного средства «Octopus»

Программное средство «Octopus» является инструментом для анализа социальных сетей и больших массивов информации. «Octopus» включает в себя ряд режимов и инструментов для осуществления поставленных задач. Основными режимами программного продукта «Octopus» являются:

«Граф», «Досье» и «Задачи». Режим «Граф», в свою очередь, состоит из документа и рабочей области [4].

Режим «Досье» – инструментарий системы «Octopus», позволяющий работать с базой данных посредством досье объекта [5]. Режим «Граф» позволяет работать с базой данных посредством создания и просмотра выборок из базы данных – документов. Документ раздела «Граф» - инструмент, позволяющий создавать выборку из базы данных проекта – подграф объектов.

Проект – информационный массив, организованный и обособленный в отдельной базе данных. На каждый проект создается своя единственная, независимая и не связная с другими проектами база данных. При работе с системой «Octopus» пользователь всегда работает в контексте того или иного выбранного проекта (т.е. с базой банных этого проекта). В некотором смысле можно принять отождествление понятий проекта и базы данных проекта.

База данных проекта (БД) – совокупность информационных элементов - объектов базы данных [6]. БД представляет собой совокупность информации, взятой из различных источников, представленную в объектной форме и имеющую вид системы (графа).

Объект базы данных – запись, элемент БД, отражающий некоторую информацию об объекте реального мира (предметной области) или об их отношении. Записи в классической табличной базе данных хранятся в виде строк в таблице. В графовой БД объекты могут быть представлены двумя способами: в виде узла либо в виде связи узлов. В таблице каждая строка состоит из набора ячеек, в каждой из которых хранится одно из свойств (атрибутов) объекта. Аналогичным образом, каждый узел или связь так же обладает набором свойств. Кроме того, объект-узел всегда обладает классом узла (или несколькими классами), а объект-связь обладает типом связи. Перечень доступных классов узлов, возможные для них типы связей, а также соответствующие им наборы свойств описываются при помощи модели данных. Таким образом, объект (как узел, так и связь) также можно определить, как типизированный контейнер свойств.

К основным функциям режима «Досье» можно отнести создание/изменение/удаление объекта, добавление объекта в список, а также работу с модулями [30].

Режим «Задачи» обладает следующими возможностями: запуск задач, просмотр шагов завершенных ранее задач, история, обработка файлов Excel, а

также загрузка файлов. Запуск зада возможен вручную или по расписанию. Наряду с режимами существуют инструменты, с помощью которых происходит реализация функций программного средства «Octopus». Существуют следующие основные инструменты: поиск, создать/посмотреть/изменить/удалить, раскрыть/схлопнуть, скрыть, досье, найти путь, выделить, списки, экспорт CSV, зафиксировать, построение, фильтр (стиль), временной фильтр (плеер), снимок.

Структурная схема программного средства «Octopus» представлена на рисунке 107.

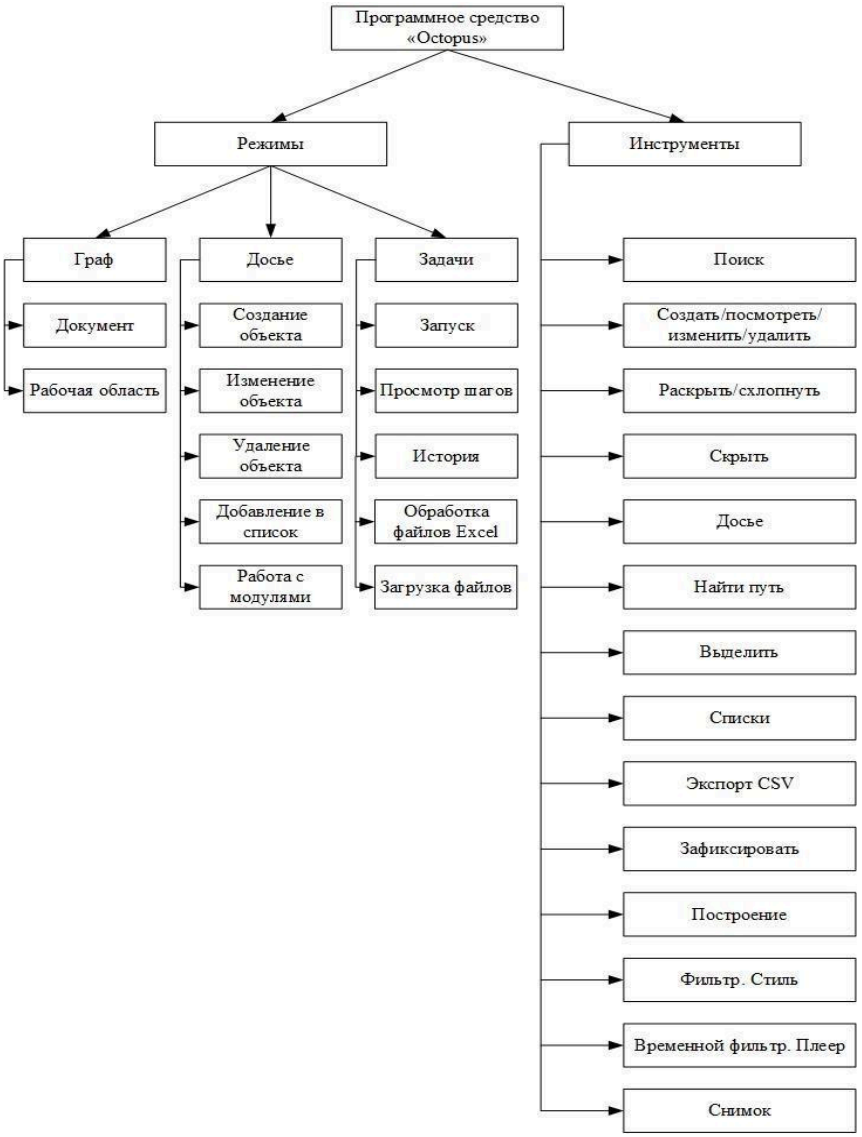


Рисунок 107 – Структурная схема программного средства «Octopus»

2.2. Рекомендации по работе с программным средством «Octopus»

Чтобы начать работу в «Octopus» следует запустить любой из веб-браузеров, затем перейти на адрес веб-сервера (например, 192.168.1.123:8080/Octopus). В открывшейся вкладке необходимо ввести логин и пароль (Рисунок 108), при введении корректных учетных данных, выполнится вход в программу.

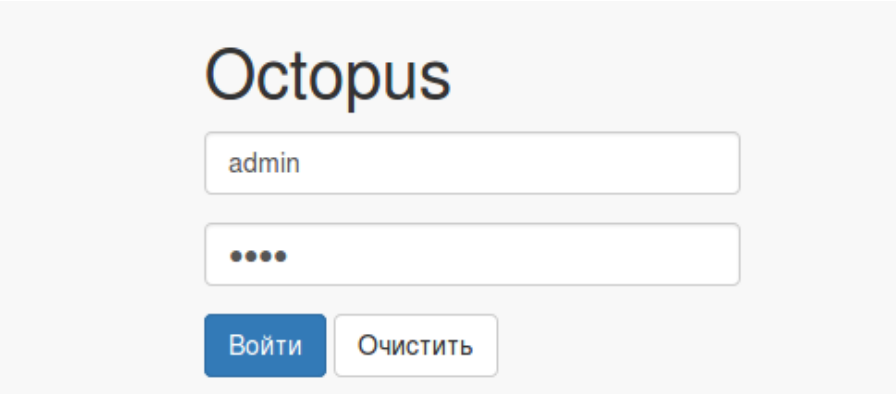


Рисунок 108 – Окно ввода логина и пароля

Далее необходимо выбрать проект из ранее созданных или создать свой (Рисунок 109).

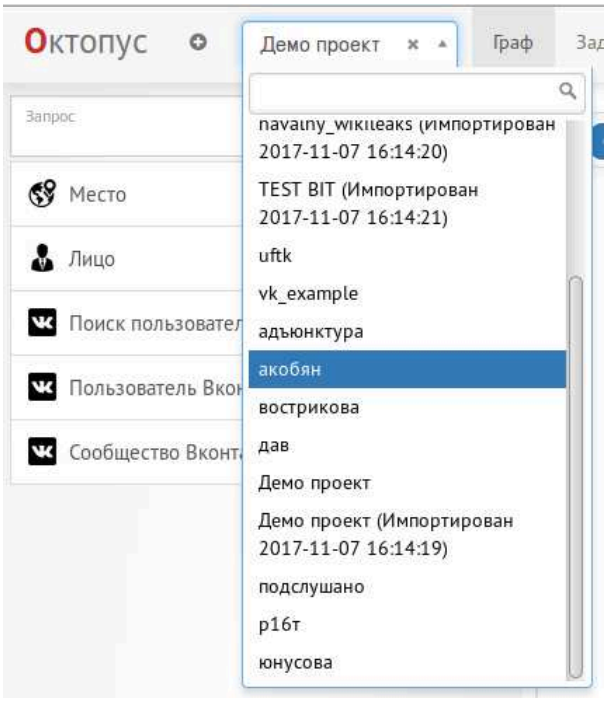


Рисунок 109 – Окно выбора проекта

В рамках каждого проекта есть инструмент «Документ», который предназначен для формирования выборки объектов базы данных проекта, для дальнейшей работы над графом объектов, а также для сохранения результатов.

Работая с документом, пользователь создает некую «проекцию» базы данных проекта, которая включает в себя сведения только о ключевых объектах текущей подзадачи. Добавление новых элементов в документ осуществляется как вручную, при помощи инструментов создания, так и автоматически при выполнении запросов в базу данных проекта посредством инструментов полнотекстового поиска, раскрытия связей и поиска путей[4].

При первом открытии интерфейса «Граф» автоматически создается новый несохраненный документ.

Для создания нового документа необходимо нажать на кнопку «Новый документ» (Рисунок 109), затем на кнопку «Сохранить как», указать имя нового документа (Рисунок 110) и нажать «Создать».

Рисунок 109 – Создание нового документа

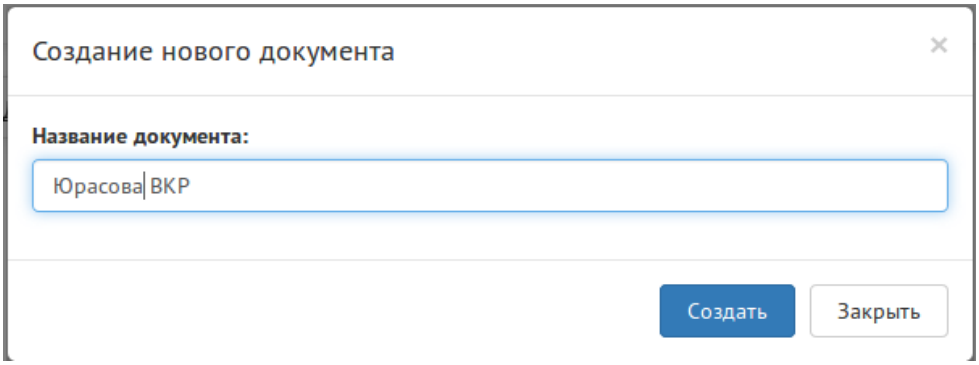


Рисунок 110 – Окно ввода имени нового документа

Для сохранения документа следует нажать на кнопку «Новый документ», затем на кнопку «Сохранить» (если документ новый, программа потребует ввода его имени), нажать «Создать» (Рисунок 110).

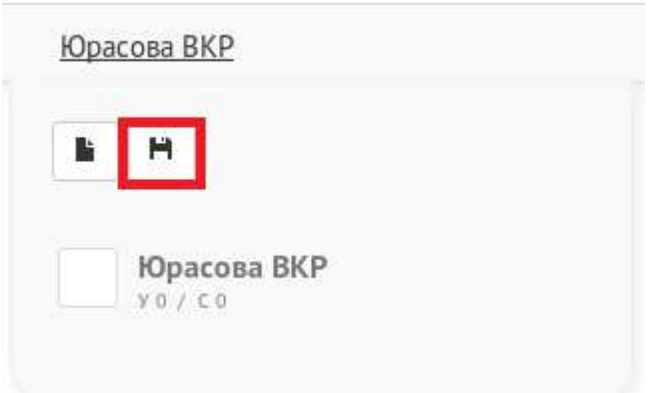


Рисунок 111 – Сохранение документа

Для выбора ранее созданного документа необходимо нажать на кнопку «Новый документ», а затем выбрать требуемый документ из предложенного списка (Рисунок 111).

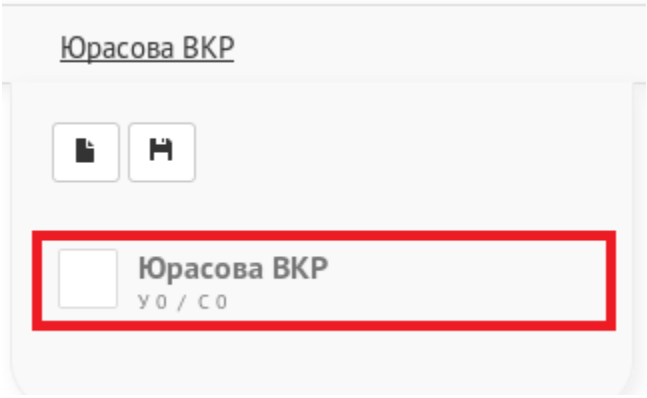


Рисунок 112. – Выбор существующего документа

Для того, чтобы удалить документ, необходимо нажать на кнопку «Новый документ», навести курсор на интересующий документ и нажать кнопку «Удалить» напротив названия элемента (Рисунок 112).

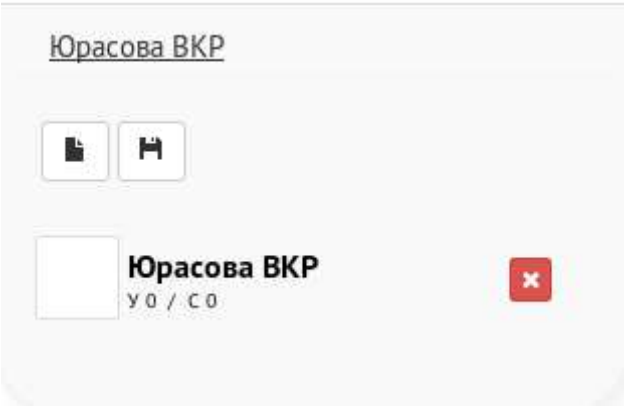


Рисунок 113. – Удаление документа

Каждый документ имеет свою рабочую область, которая представляет собой визуальное пространство, на котором размещаются прорабатываемые объекты. Данная область условно не имеет границы, поэтому позволяет располагать большое количество элементов, а также выполнять масштабирование и панорамирование. Размещение элементов в пространстве рабочей области происходит как вручную пользователем, так и автоматически при помощи инструментов построения.

Интерфейс рабочей области документа также включает в себя графические элементы управления различными инструментами раздела «Граф» (Рисунок 114).

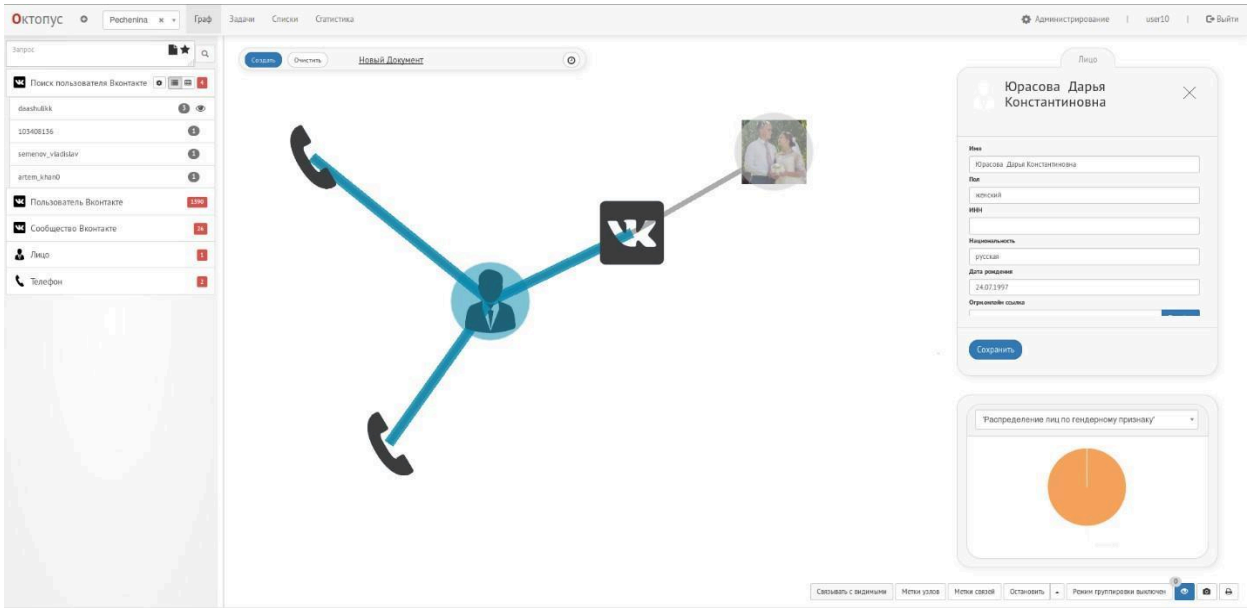


Рисунок 114. – Рабочая область

Для управления масштабированием рабочей области используются повороты колеса мышки: от себя — приближение, к себе — отдаление. Для того, чтобы панорамировать рабочую область, необходимо зажать левую кнопку мыши таким образом, чтобы под курсором не оказалось узла или связи [8].

В программе также реализован инструмент полнотекстового поиска по атрибутам объектов в базе данных проекта, а также визуальное выделение найденных элементов в рабочей области документа.

Поиск по заданному ключевому слову или фразе происходит по всем атрибутам указанного класса, в том числе по текстам файловых вложений. Найденные объекты могут быть добавлены пользователем в рабочую область документа.

Результаты поиска возвращаются сгруппированными по классу, с указанием количества найденных элементов. Также, в панели поиска для каждого объекта отображается количество связей в базе данных проекта.

Для осуществления поиска необходимо нажать на инструмент «Поиск», затем в поле ввода указать текст запроса, после чего в поле отобразится результат поиска, сгруппированный по классу объекта (Рисунок 115). Раскрыть необходимую группу объектов можно нажатием левой кнопкой мыши на группу, а для раскрытия карточки интересуемого объекта

- нажатием левой кнопкой мыши на названии объекта.

Для добавления объекта в рабочую область документа необходимо в списке найденных объектов выбрать необходимый объект левой кнопкой мыши, а для выбора нескольких объектов – нажать и удерживать левый Ctrl, после чего перетащить объекты курсором в рабочую область (Рисунок 116).

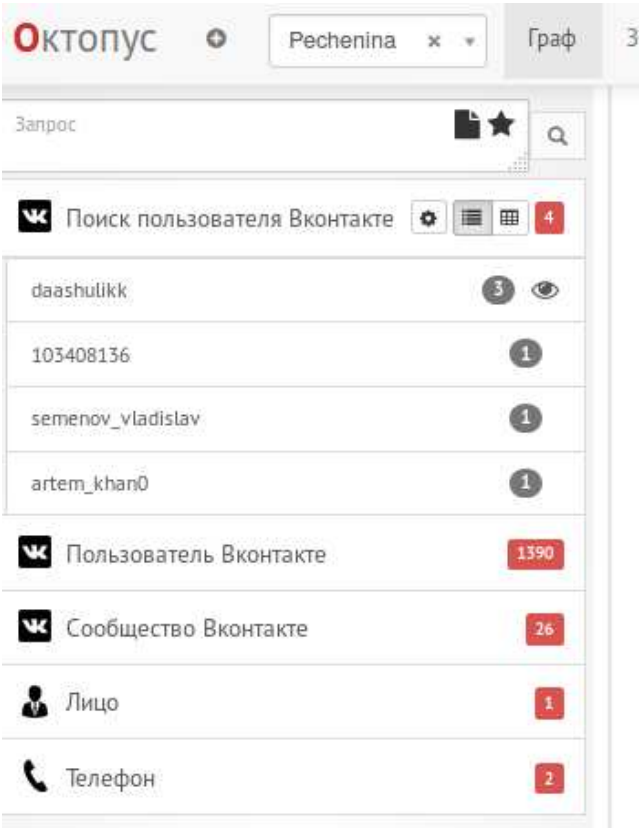


Рисунок 115. – Поиск

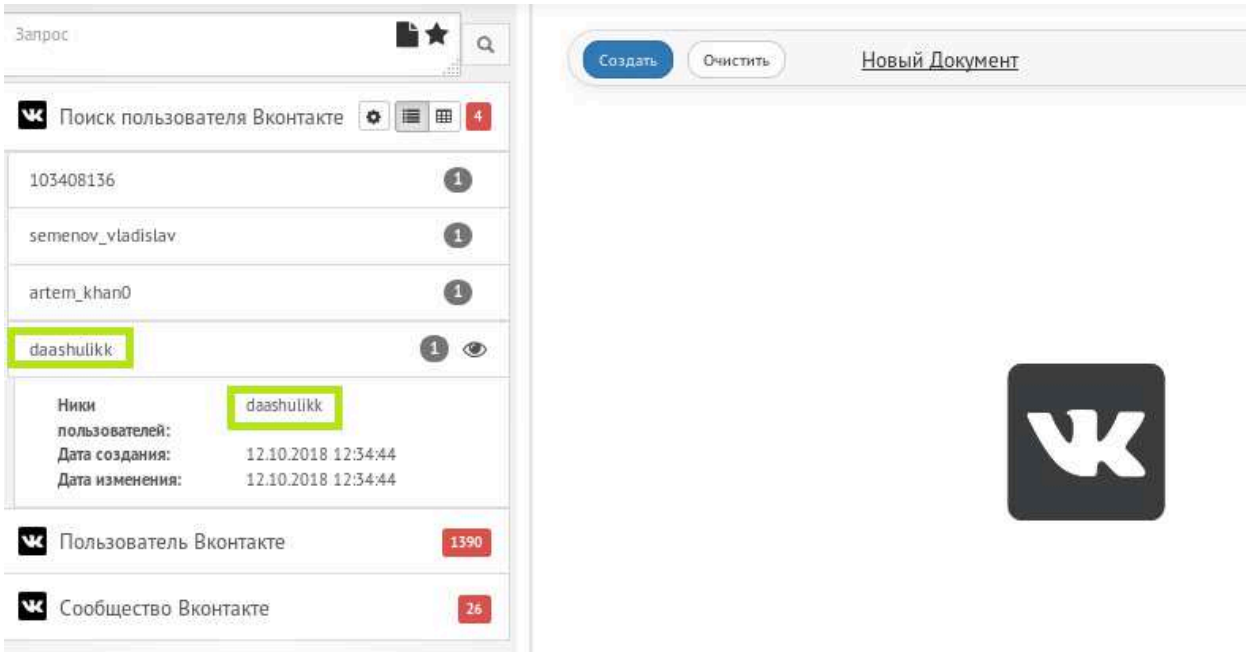


Рисунок 116. – Просмотр результатов поиска и перенос в рабочую область

Для сортировки в группе найденных объектов необходимо нажать на «Настроить», затем выбрать тип сортировки (по убыванию, по умолчанию, без сортировки) и указать атрибут сортировки (Рисунок 117).

Созданные объекты, а также изменения атрибутов объектов, внесенные в текущем документе, сохраняются в базу данных проекта и отражаются во всех прочих документах и досье, в которых присутствует измененный объект.

При изменении или добавлении атрибута, который в схеме данных имеет ограничение на значения «уникальное», не допускается ввод значения, которое уже присутствует в другом объекте этого же классаПредставляется целесообразным

рассмотреть следующие инструменты [31]:

1) создания новых объектов в рабочей области текущего документа;
2) просмотра и внесения изменений в атрибуты существующих объектов;
3) сохранения изменений в базу данных проекта;
4) добавления к узлу изображения и файлового вложения;
5) удаления объектов из базы данных.

Не следует путать удаление узла из базы данных с сокрытием его из рабочей области текущего документа. В первом случае, узел и все его связи будут стерты из базы данных и соответственно из всех документов и досье. Во втором случае, он и его связи перестанут отражаться только в текущем документе, так же, он все еще будет доступен через поиск.

После создания узла не допускается изменение его класса, аналогично, изменение типа связи так же невозможно.

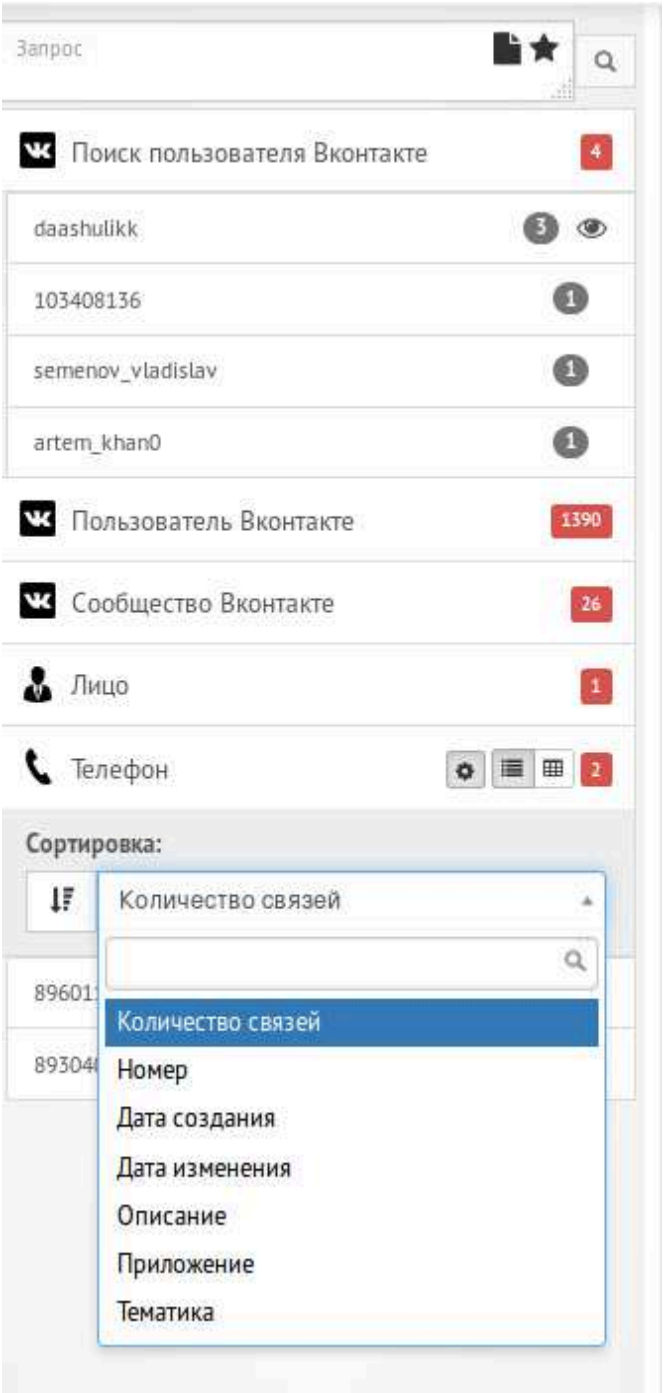


Рисунок 117. – Настройки сортировки результатов поиска

.Для создания узла необходимо вызвать контекстное меню в рабочей области документы нажатием правой кнопки мыши, затем из выпадающего списка выбрать пункт «Создать узел» (Рисунок 118), далее в открывшейся форме произвести редактирование атрибутов.

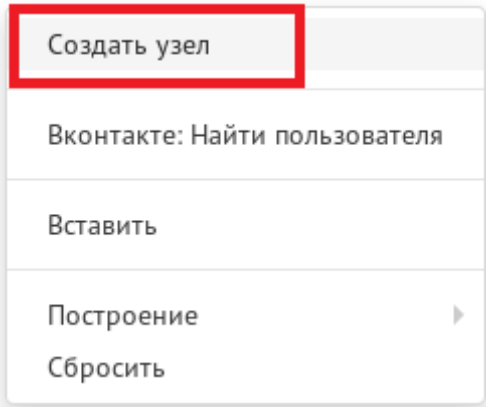


Рисунок 118. – Создание нового узла

Для изменения созданного ранее узла необходимо выбрать узел, вызвать его контекстное меню нажатием правой кнопкой мыши, выбрать пункт «Посмотреть» (Рисунок 119), после чего в открывшемся окне осуществить редактирование атрибутов.

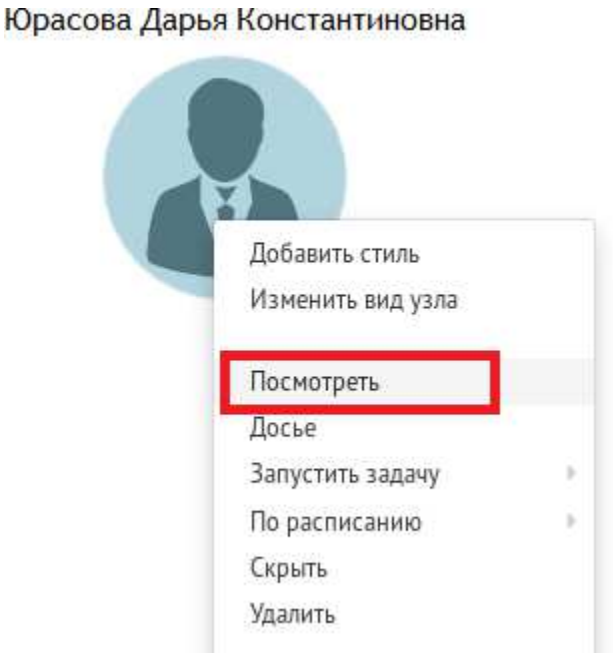


Рисунок 119 – Просмотр контекстного меню узла

Для редактирования атрибутов узла в поле выбора класса узла необходимо указать класс узла (только при создании), затем в поле выбора подклассов указать подклассы узла (необязательно), в списке атрибутов узла указать необходимые значения, добавить иконку (необязательно), добавить файл-вложение (необязательно), нажать на кнопку «Сохранить» (Рисунок 120).

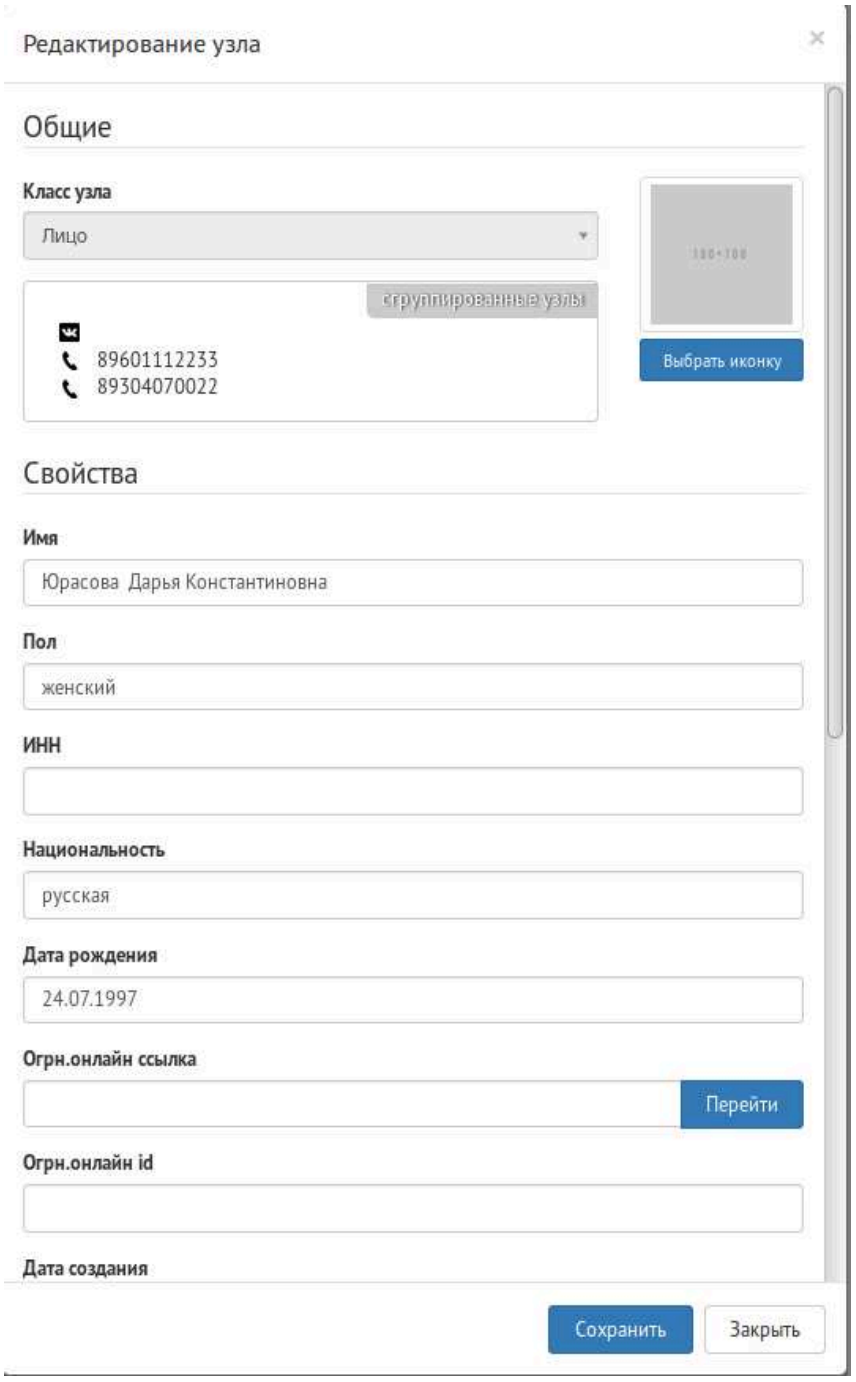


Рисунок 120 – Редактирование узла

Для добавления файла – вложения необходимо открыть карточку объекта, в соответствующем атрибуте нажать на «Выбрать», выбрать файл в файловой системе, нажать на «Сохранить» [8].

Для удаления узла необходимо выбрать узел, вызвав его контекстное меню правой кнопкой мыши, выбрать пункт «Удалить», после чего подтвердить удаление.

Для создания связи между узлами необходимо выбрать первый узел, вызвав его контекстное меню правой кнопкой мыши, выбрать пункт «Построить связь отсюда» (Рисунок 121), затем выбрать второй узел, вызвав его контекстное меню правой кнопкой мыши, после чего выбрать пункт «Построить связь сюда» (Рисунок 16), далее откроется окно создания связи, в

котором необходимо нажать на поле «Выберите тип связи» (Рисунок 122), в открывшемся списке доступных типов связей ввести название типа связи (необязательно для поиска), выбрать необходимый тип связи из списка, нажать на кнопку «Сохранить».

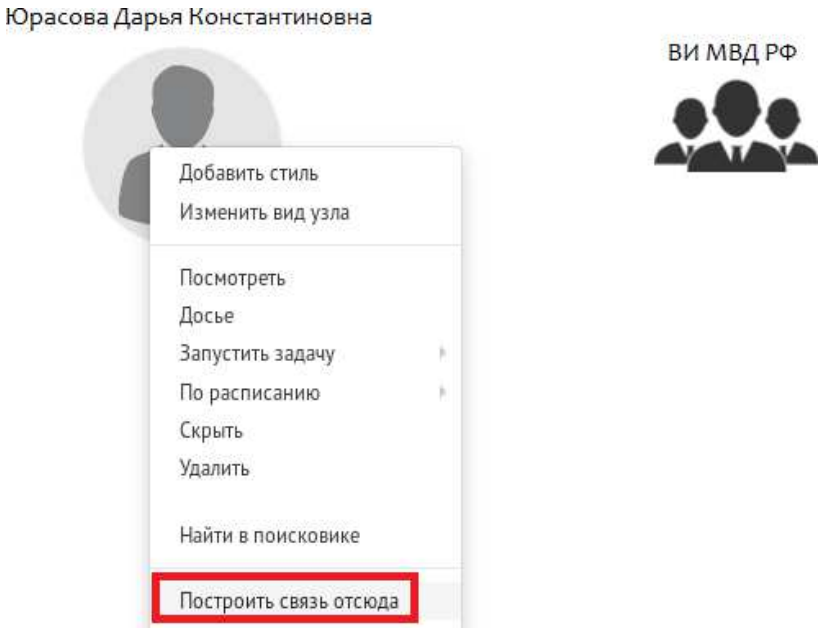


Рисунок 121 – Начальный узел построения связи

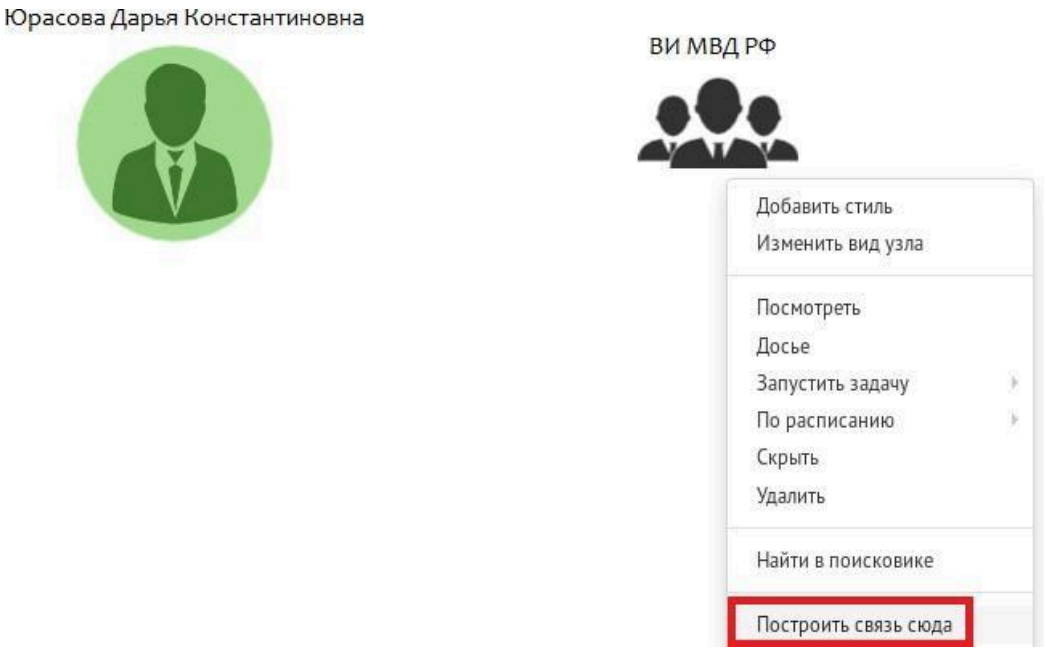


Рисунок 122 – Конечный узел построения связи

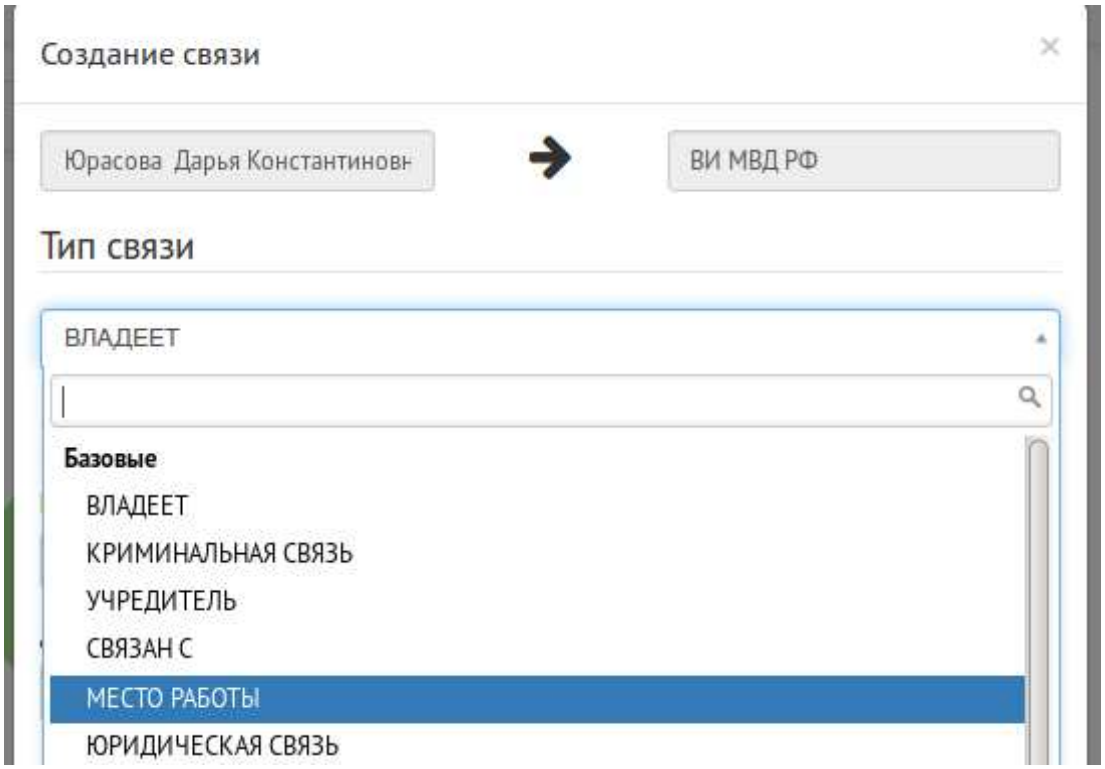


Рисунок 123 – Выбор типа связи

Для просмотра/удаления связей между узлами необходимо выбрать связь, вызвав ее контекстное меню правой кнопкой мыши, выбрать пункт

«Посмотреть» (Рисунок 124), после чего откроется окно просмотра связей между узлами (Рисунок 125), далее если необходимо удалить связь - нажать на «Удалить», нажать на «Закрыть».

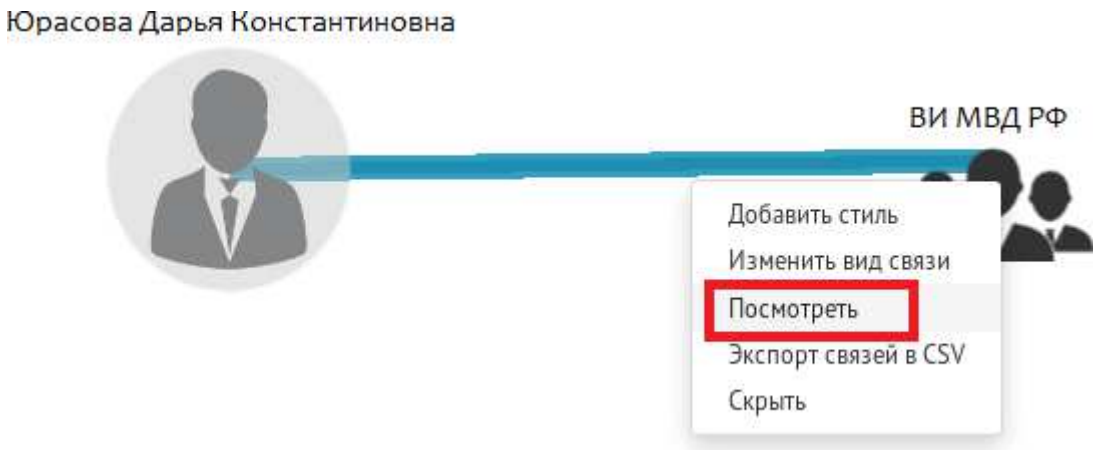


Рисунок 124 – Просмотр контекстного меню связи

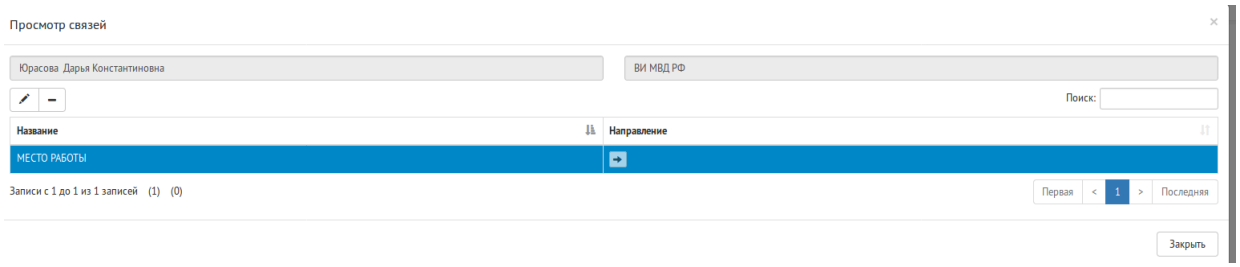


Рисунок 125 – Просмотр связи

Изменения типа существующей связи невозможно, поэтому в случае такой необходимости следует удалить старую связь, а затем создать новую с необходимым типом.

Для просмотра атрибутов узла необходимо навести указатель мыши на узел и дождаться появления информации об атрибутах узла. Данную функцию можно отключить (включить), для этого необходимо перейти в раздел Администрирование, выбрать подраздел Настройки, отключить (либо включить) функцию предпросмотра.

Для осуществления выборки связей для указанных узлов из базы данных проекта существует инструмент «раскрыть/схлопнуть». При раскрытии выбранных элементов осуществляется запрос в базу данных проекта для получения всех связей и соответствующих связных узлов. После выполнения запроса найденные элементы добавляются в текущий документ, а также выполняется их построение в рабочей области согласно выбранному принципу построения. При схлопывании узла происходит скрытие тех связей и связных узлов, которые не имеют дополнительных связей с другими узлами (так называемые листовые узлы). При этом соответствующие связные узлы также скрываются. Скрываемые объекты не удаляются из базы данных проекта и не скрываются из прочих документов [8].

Нераскрытые узлы помечаются при помощи серого полупрозрачного круга.

Для раскрытия узла необходимо выбрать узел, вызвав контекстное меню (ПКМ), выбрать пункт «Раскрыть». Для раскрытия нескольких узлов следует выбрать узлы при помощи инструмента выделения, вызвать контекстное меню (ПКМ) и выбрать пункт «Раскрыть». Для схлопывания узла – выбрать узел, вызвав контекстное меню (ПКМ), выбрать пункт «Схлопнуть».

Для скрытия выбранных узлов и их связей из текущего документа существует инструмент «скрыть». В отличие от схлопывания узла, при скрытии он удаляется из рабочей области текущего документа, а также скрываются все его связи, но не связные узлы, при этом скрываемые элементы не удаляется из базы данных проекта и не скрываются из прочих документов.

Также не следует путать удаление узла из базы данных с сокрытием его из текущего документа. В первом случае узел и все его связи будут стерты из базы данных и соответственно из всех документов и досье. Во втором случае,

он и его связи перестанут отражаться только в текущем документе, так же, он все еще будет доступен через поиск.

Чтобы скрыть узел следует выбрать узел, вызвав контекстное меню (ПКМ), выбрать пункт меню «Удалить» или (альтернативно) нажать на клавиатуре клавишу «Del».

Для поиска в базе данных проекта последовательностей связей между указанными узлами в соответствии с заданными параметрами поиска существует инструмент «найти путь».

Путь представляет собой цепочку из связей узлов заданной длины или диапазона длин. Результатом расчета является подграф, включающий узлы и связи из найденных путей. Найденные узлы и связи добавляются в рабочую область, а также подсвечиваются.

Шаблон поиска позволяет задавать параметры длины пути, а также типов и направления связей. Также опционально, указывается количество возвращаемых результатов.

Для поиска путей между двумя узлами необходимо выполнить следующие действия:

1) выбрать первый узел, вызвав контекстное меню (ПКМ);
2) выбрать пункт «Найти путь отсюда»;
3) выбрать второй узел, вызвав контекстное меню (ПКМ);
4) выбрать пункт «Найти путь сюда»;
5) появится окно задания параметров поиска;
6) указать дополнительные параметры поиска (опционально);
7) нажать на кнопку «Найти».

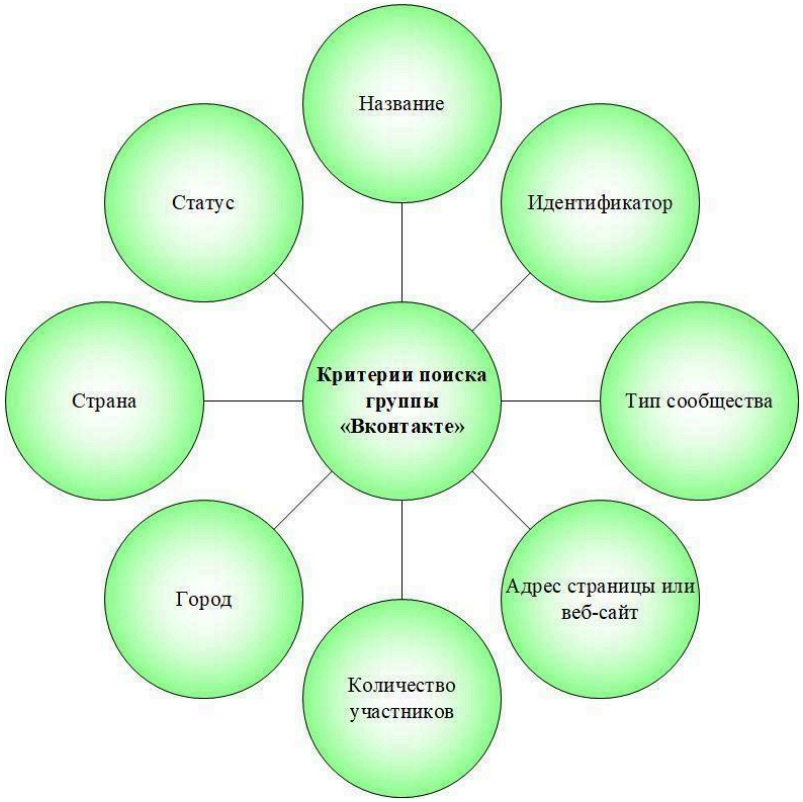
Также в представленной работе разработан алгоритм поиска сообщества в «Вконтакте», приведенный на рисунке 126.

Рисунок 126 – Алгоритм поиска сообщества «ВКонтакте»

Для поиска какого-либо сообщества «ВКонтакте» необходимо в рабочей области документа щелкнуть ПКМ, из предложенного списка выбрать пункт «Создать узел», далее в поле «Класс узла» указать

«Сообщество Вконтакте». В открывшейся форме следует ввести критерии для поиска группы (Рисунок 127). Такими критериями могут быть:

1) название;
2) системный идентификатор;
3) пользовательский идентификатор;
4) тип сообщества;
5) адрес страницы;
6) веб сайт;
7) количество участников;
8) город;



9) страна
10) статус.

Рисунок 127 – Критерии поиска группы «ВКонтакте»

2.3. Анализ данных из социальной сети в режиме «Граф»

Раздел «Граф» веб интерфейса системы представляет собой набор инструментов для решения задач, выявления прямых и косвенных связей между сущностями базы данных проекта. Работа в данном разделе осуществляется посредством формирования и анализа выборки из базы данных проекта, представляемой в виде диаграммы связей объектов - графа объектов.

Целесообразным представляется рассмотреть основные определения, таковыми являются граф, узел и связь.

Граф (объектный граф) – структура, представляющая собой совокупность Узлов и Связей, соединяющих эти Узлы. Таким образом, Объекты базы данных, хранящиеся в подобной структуре, могут быть либо Узлами, либо Связями. Сетевая структура в виде графа является эволюцией классической табличной структуры. В отличие от таблиц графы лучше приспособлены для хранения сильно связных и структурированных данных, т.е. информации такого характера, который подразумевает наличие большого количества отношений (связей) между объектами.

Узел (вершина) – элемент базы данных (объект), основной способ хранения и представления сведений об объекте реального мира в графовой базе данных. В рамках одного проекта каждый узел имеет уникальный идентификатор, выдаваемый системой автоматически при создании узла. Узел в БД всегда обладает Классом (или несколькими классами), а также набором Свойств, соответствующих этому Классу. Пара узлов может быть связанна посредством объекта-Связи. Узлы могут быть связанны друг с другом несколькими различными связями. Связи могут быть исходящими и входящими по отношению к данному узлу. В свою очередь, узлы, хранящиеся в разных проектах, не могут быть связанны.

Связь (ребро) – элемент базы данных (объект), основной инструмент для организации и представления информации об отношениях и взаимосвязях между объектами реального мира. Связь в базе данных всегда строится для двух связываемых узлов той же базы. Связь может обладать Направлением, в этом случае один из двух связываемых узлов будет начальным, а другой конечным по отношению к данной связи. Соответственно, для начального узла данная связь будет исходящей, а для конечного входящей. Связь всегда обладает типом связи и, аналогично узлу, может содержать набор дополнительных свойств. Каждая связь, так же обладает уникальным (в рамках проекта) системным идентификатором. Последовательные цепочки связей образуют пути между узлами.

Процесс работы с графами включает в себя следующие позиции [8] :

1. Поиск информации в базе данных.
2. Получение связей объектов или цепочек связей между парой объектов.
3. Ручное и автоматическое построение диаграмм связей.
4. Стилизация и фильтрация элементов.
5. Выполнение визуального и статистического анализа.
6. Экспорт отчетных данных в файлы текстовых и графических форматов.
7. Создание и пополнение списков объектов для работы в разделе «Задачи».
8. Сохранение и организация результатов при помощи документов в проекте.

Интерфейс раздела «Граф» представлен на рисунке 128.

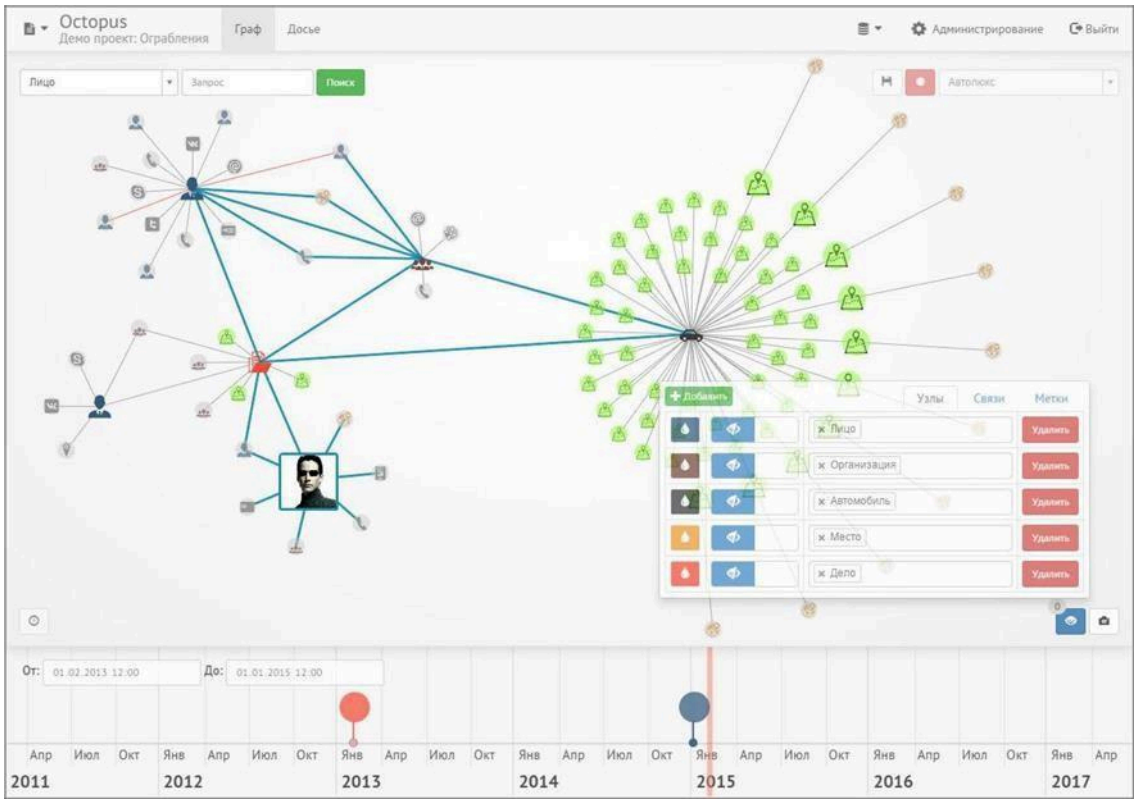


Рисунок 128 – Интерфейс раздела «Граф»

2.4. Аналитическая работа программного средства «Octopus» в режиме «Досье»

Раздел «Досье» (Рисунок 129) веб интерфейса системы представляет собой набор инструментов для автоматического построения модульного досье на тот или иной объект базы данных. Досье объекта включает в себя карточку с его атрибутами, а также набор информационных модулей - т.н. виджетов. Каждый такой модуль содержит результат того или иного запроса в базу данных [8].

Совокупность результатов подобных запросов формирует отчет, включающий информацию, находящуюся в базе данных, и имеющую отношение к текущему объекту. При этом каждый такой запрос в БД может решать некоторую аналитическую задачу, связанную с текущим объектом, такую как подсчет каких-либо статистических показателей или же выводить таблицу, содержащую связанные с ним объекты. Данные, полученные посредством запроса, могут быть представлены как в классическом табличном режиме, так и при помощи графиков или карт.

Работая в режиме «Досье», пользователь может выполнять полнотекстовый поиск объектов, создавать новые объекты, изменять атрибуты, удалять, добавлять к объектам файл-вложение, а также создать связи с другими объектами. Кроме того, каждый виджет табличного вида позволяет осуществлять сортировку данных по каждому из столбцов, выполнять переход в досье других объектов, а также выполнять экспорт содержимого в CSV файл.

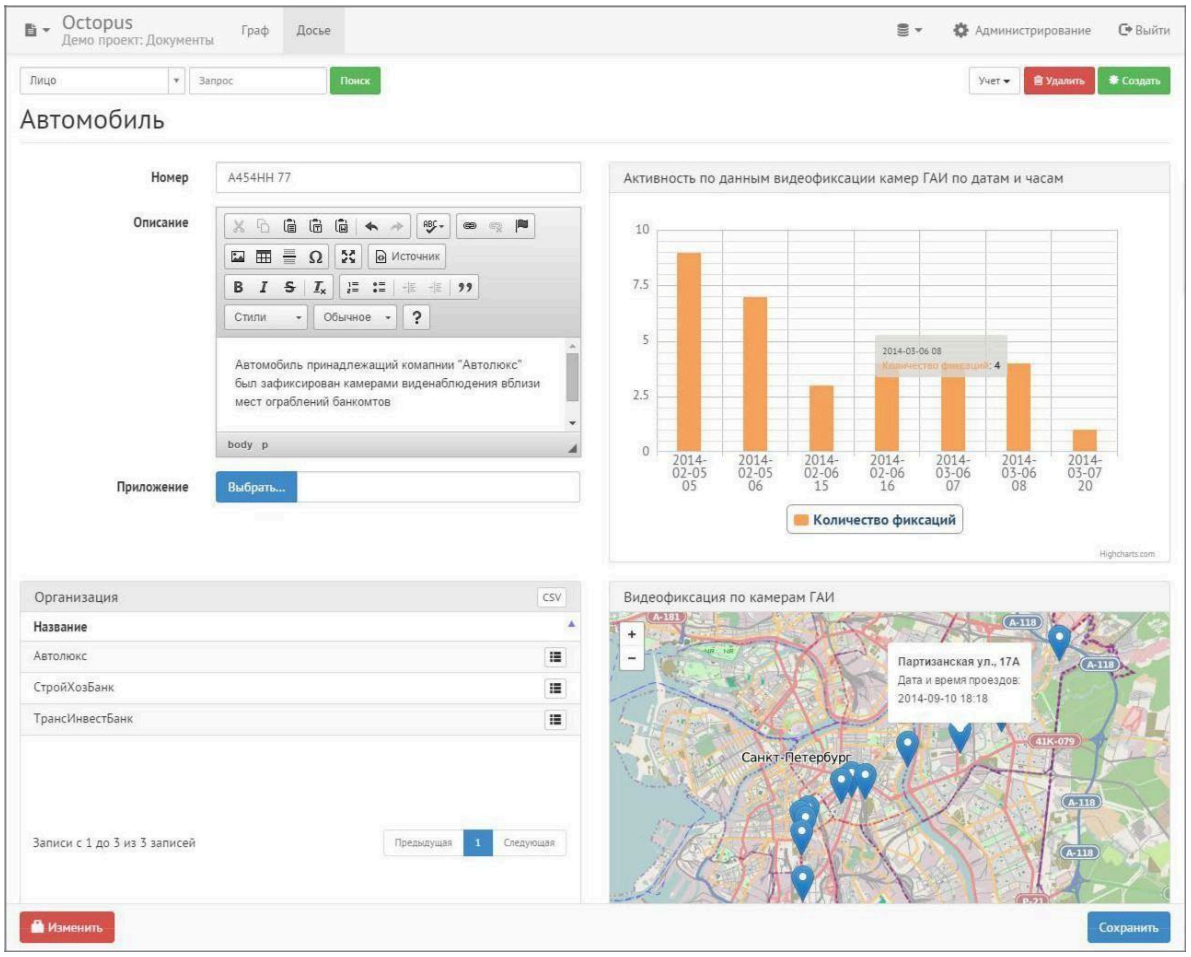


Рисунок 129 – Раздел «Досье»

В рамках режима «Досье» возможно создание, изменение и удаление объектов. Создание новых объектов происходит посредством занесения информации в форму ввода, изменение атрибутов может выражаться в добавлении к узлу изображения и файлового вложения.

Созданные объекты, а также изменения атрибутов объектов, сохраняются в базу данных проекта и будут отражены во всех документах и досье, в которых присутствует измененный объект.

При изменении или добавлении атрибута, который в схеме данных имеет ограничение на значения «уникальное», не допускается ввод значения, которое уже присутствует в другом объекте этого же класса. После создания узла не допускается изменение его класса.

Также в рамках режима «Досье» существует возможность добавления объекта в список для дальнейшего выполнения аналитической задачи над ним, либо синхронизации с внешними ресурсами [8].

Помимо списков существует возможность построения модульного отчета по тому или иному объекту базы данных.

Досье объекта, помимо карточки с его атрибутами, также может включать в себя перечень виджетов. Каждый виджет содержит результат того или иного запроса в базу данных, связанный с текущим объектом. Примером такого

запроса может быть получение всех сотрудников, работающих в данной организации – в этом случае в досье той или иной организации, подобный виджет будет содержать список объектов – лиц, которые работают в данной организации. Другим примером может служить запрос, который высчитывает статистику по году рождения друзей пользователя социальных сетей – таким образом, виджет, отображающий результат данного запроса, будет содержать таблицу, в которой будет представлено статистическое распределение по годам рождения друзей данного пользователя соцсетей.

Виджеты могут быть нескольких типов:

1) табличные – содержат таблицу с результатом запроса;

2) картографические – отображают объекты на картографической подложке;

3) графические – включают графики тех или иных показателей. Простые табличные виджеты, содержащие список связных узлов,

4) могут быть отредактированы, в этом случае у пользователя есть возможность внести изменения в таблицу виджета, т.е. добавить или удалить связь с другим объектом.

Табличный виджет может отобразить не более 10 (значение может быть изменено) записей - строк. В том случае если таблица содержит большее количество записей, то они разбиваются на страницы.

Картографические виджеты предназначены для отображения объектов базы данных на картографической подложке. Каждый объект на карте может так же содержать набор свойств.

Возможные следующие способы отображения объектов: маркер, линия, полигон[4].

Графические виджеты предназначены для отображения информации в виде столбиковой диаграммы. График этой диаграммы располагается в двух измерениях. Каждое из измерений может иметь тот или иной смысл. Например, по оси X может быть дата (или день), а по оси Y кол-во сообщений в этот день.

Один виджет может содержать несколько графиков, в этом случае все они содержат информацию из тех же измерений. При этом каждый из графиков будет отображен своим цветом.

2.5. Реализация функциональных возможностей программного средства «Octopus» в режиме «Задача»

Средство Octopus позволяет загружать сведения из различных информационных ресурсов, в том числе из реляционных и nosql баз данных, rest сервисов, файлов, а также из открытых источников сети Интернет, таких как социальные сетей или поисковые сервисы.

Работа с этими сведениями подразумевает их загрузку в базу данных проекта Octopus для последующего хранения, обработки и анализа. Таким образом, загруженная информация остается в базе данных системы даже после ее удаления из внешнего ресурса. Система также позволяет выполнять

синхронизацию данных по расписанию для осуществления непрерывного мониторинга и автоматической загрузки новых сведений.

Загрузка сведений осуществляется посредством задач. Задача представляет собой последовательность шагов. На каждом шаге производится получение и преобразование в граф некоторой порции данных (см. пункт «Описание задач»).

Все аналитические и поисковые инструменты Octopus оперируют только над загруженными в базу данных сведениями. Таким образом, результаты тех или иных вычислений или поисковых запросов в систему Octopus не опираются на незагруженные в систему данные [4].

Также, принимая во внимание возможные объемы данных в тех или иных источниках, а также ограниченность временных и вычислительных ресурсов, следует иметь в виду, что загрузка всех сведений единовременно иногда не представляется возможной, а зачастую и не имеет смысла. (например, грузить данные обо всех пользователях социальной сети, если производится анализ только над определенными пользователями и их друзьями)

Поэтому основной принцип работы с большими источниками данных посредством задач Octopus предполагает итеративное (пошаговое) накопление и анализ.

Данный принцип заключается в следующем: каждая итерация - процесс загрузки данных производится сначала для некоторого заданного набора ключевых объектов из проекта. Пользователь формирует данные объекты в список для последующей обработки. В дальнейшем, если круг ключевых объектов изменился, итерация повторяется.

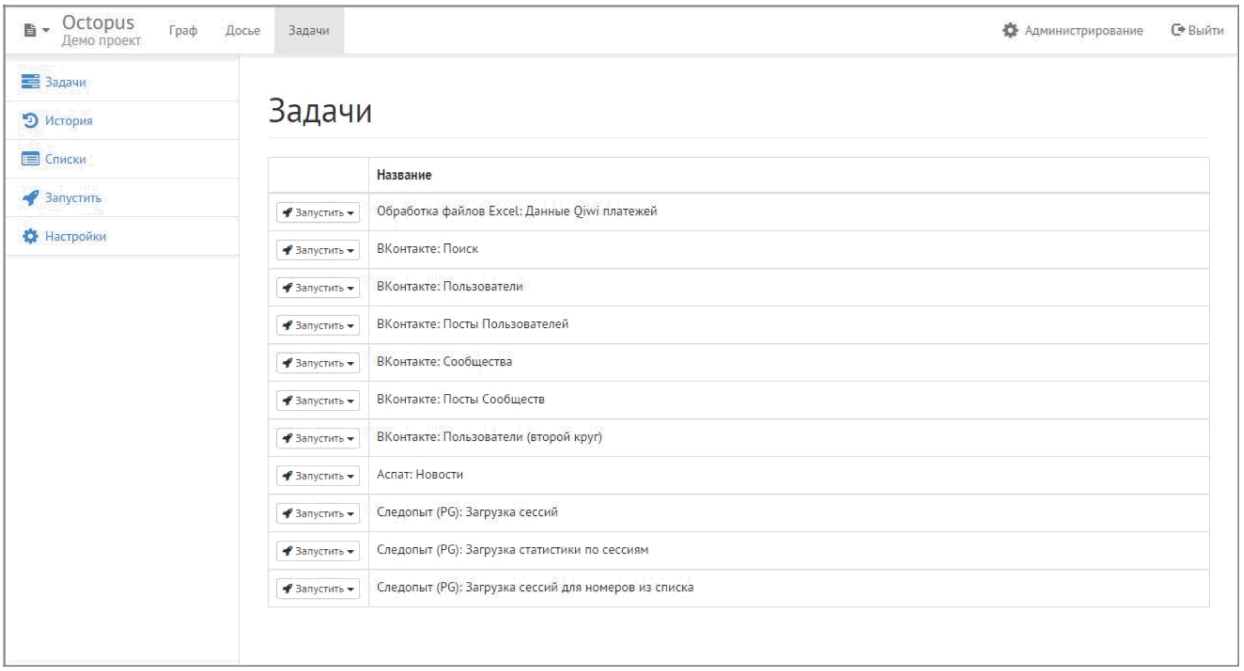


Рисунок 130 – Режим «Задачи»

В рамках режима «Задачи» (Рисунок 130) существует инструмент «Запуск». Для запуска задачи необходимо выбрать задачу из списка, затем

выбрать список обработки (опционально, в случае если задача выполняется над списком), указать дополнительные параметры запуска (опционально), после чего появится интерфейс просмотра шагов.

Интерфейс просмотра шагов позволяет просматривать детальный ход задачи и содержит следующие сведения: название, дата начала, последнее обновление, количество обработанных записей, статус («STARTING» - шаг запускается, «STARTED» - шаг запустился и работает, «COMPLETED» - выполнение шага завершилось успешно, «FAILED» - выполнение шага завершилось с ошибкой).

При этом количество обработанных записей может отличаться от реального кол-ва созданных объектов узлов и связей и отражает лишь количество элементов, которые были получены системой во время выполнения данного шага. Т.е. одна полученная из внешнего источника обрабатываемая запись может содержать в себе несколько узлов и связей. Поэтому данный показатель является условным [8].

Инструмент история служит для просмотра истории выполнения задач. В таблице представлена следующая информация о задачах: название задачи, статус («STARTING» - задача запускается, «STARTED» - задача запустилась и работает, «COMPLETED» - выполнение задачи завершилось успешно, «FAILED» - выполнение задачи завершилось с ошибкой), дата создания, дата начала и дата окончания.

Для анализа социальной сети «ВКонтакте» существуют следующие задачи (Рисунок 131):

1) Поиск пользователей и сообществ;
2) ВКонтакте: Поиск постов;
3) Профили пользователей, друзья и сообщества;
4) Посты пользователей;
5) Профили сообществ, участники;
6) Посты сообществ.

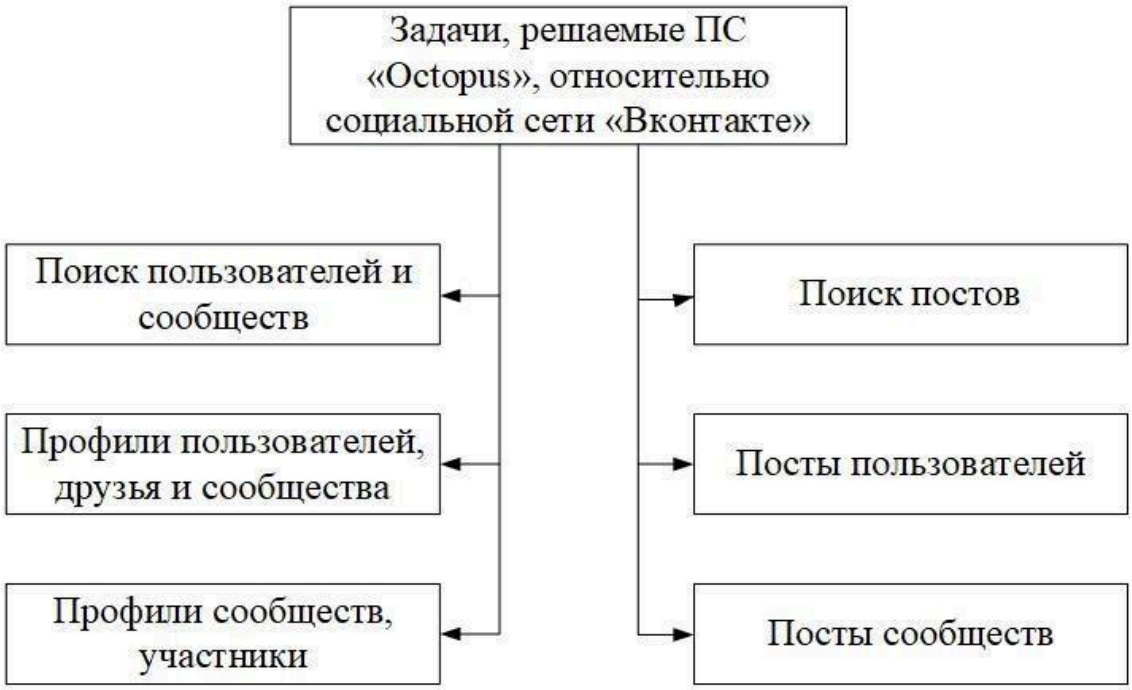


Рисунок 131 – Задачи для анализа социальной сети «ВКонтакте»

Поиск по пользователям и сообществам социальной сети «ВКонтакте» осуществляется по атрибутам заданных ключевых объектов:

«Текст» объекта «Ключевое слово», а также номерам телефонов, именам лиц и названиям организаций.

Далее происходит построение графа связей между ключевыми объектами поиска и найденными объектами «Пользователь ВКонтакте» и

«Сообщество ВКонтакте». Поиск пользователей и сообществ осуществляется по информации указанной в профиле [8].

Также будет создана связь типа «СВЯЗАН С» с соответствующим ключевым объектом поиска.

Поиск ВКонтакте позволяет получать до 2000 результатов (1000 пользователей + 1000 сообществ) для каждого из ключевых объектов поиска.

Поиск постов (комментариев к постам) в социальной сети

«ВКонтакте» осуществляется по атрибутам заданных ключевых объектов - по тексту объекта «Ключевое слово», а также по номерам телефонов, имен лиц и организаций. После чего происходит построение графа связей между ключевыми объектами поиска и найденными сообщениями. При этом происходит Создание в проекте найденных объектов типа «Пост ВКонтакте» с занесением следующих свойств: дата, текст, ссылка, количество одобрений, количество репостов и количество комментариев.

Для каждого поста, в свою очередь, будут созданы следующие связи:

1) «СВЯЗАН С» с ключевым объектом поиска, для которого был найден данный пост;

2) «ОПУБЛИКОВАЛ» с объектом - автором данного сообщения («Пользователь ВКонтакте» или «Сообщество Вконтакте»);

3) «НА СТРАНИЦЕ» с объектом, на стене которого был опубликован пост («Пользователь ВКонтакте» или «Сообщество Вконтакте»);

4) в случае если найденное сообщение является комментарием к посту, так же будет создана связь «КОМЕНТАРИЙ К» с оригинальным постом.

Поиск ВКонтакте позволяет получать до 1000 постов для каждого из ключевых объектов поиска.

Загрузка профиля пользователя ВКонтакте включает в себя следующую информацию: профиль страницы, связи с друзьями, а также связи с сообществами, в которых он состоит. Также сохраняются профили друзей и сообществ. Для каждого объекта «Пользователь ВКонтакте» из списка будет загружена информация о его профиле с занесением следующих свойств: системный и пользовательский идентификатор, адрес страницы, указанное имя, пол, год рождения, город, страна, школа, год окончания школы, университет, год окончания университета, веб-сайт, интересы.

Так же будут созданы следующие связи: «ДРУЖИТ С» с объектами – друзьями пользователя; «СОСТОИТ В» с объектами – сообществами, в которых состоит пользователь.

В рамках задачи по поиску постов происходит загрузка информации о постах, опубликованных на странице заданного пользователя ВКонтакте, так же загрузка информации об авторах постов, комментариях, одобрениях и репостах, в том числе построение графа связей по постам между пользователями с указанием времени публикации.

Для каждого объекта «Пользователь ВКонтакте» из списка будут созданы связи типа «НА СТРАНИЦЕ» с соответствующими постами, опубликованными на его странице. Для загруженных постов, в свою очередь, будут созданы следующие связи: «ОПУБЛИКОВАЛ» с объектом - автором данного сообщения («Пользователь ВКонтакте» или «Сообщество Вконтакте»); «РЕПОСТ К» с постами – репостами данной записи;

«КОММЕНТАРИЙ К» с комментариями к данной записи; «ОДОБРИЛ» с пользователями, которые поставили данному посту отметку «Мне нравится».

Дополнительно будет построен однородный граф связей типа «ОПУБЛИКОВАЛ СООБЩЕНИЕ НА СТРАНИЦЕ» между объектами – пользователями, с занесением даты публикации.

В результате выполнения задачи «ВКонтакте: Профили сообществ, участник» осуществляется загрузка информации о сообществе ВКонтакте, с занесением профиля страницы, а также связей с вступившими в сообщество пользователями.

Для каждого объекта «Сообщество ВКонтакте» из указанного списка будет загружена информация о его профиле с занесением следующих свойств: системный и пользовательский идентификатор, название, адрес страницы, город, страна, статус, описание сообщества, веб-сайт, тип сообщества.

Также будут созданы связи типа «ДРУЖИТ С» с объектами – пользователями, которые состоят в данном сообществе.

Задача «ВКонтакте: Посты сообществ» состоит в загрузке информации о постах, опубликованных на странице заданного сообщества ВКонтакте, а также загрузке информации об авторах постов, комментариях, одобрениях и репостах.

Для каждого объекта «Сообщество ВКонтакте» из списка будут созданы связи типа «НА СТРАНИЦЕ» с соответствующими постами, опубликованными на странице сообщества [7].

Для загруженных постов, в свою очередь, будут созданы связи по аналогии с задачей «ВКонтакте: Посты пользователей».

ЗАКЛЮЧЕНИЕ

Методические рекомендации носят ярко выраженный проблемно-ориентированный характер. Большая часть работы описывает решение практических вопросов по отработке поисково-аналитических методик в программных комплексах.

методических рекомендациях основные принципы и реализации программного комплекса для анализа данных из разнородных источников Виток-3х. А также проведен анализ функциональных возможностей программного средства «Octopus», их преимуществ и недостатков, подробно представлена структура и основные функциональные возможности позволяющие проводить качественный анализ данных.

Программный комплекс «Виток-3Х» (Lampyre RC 1.0) предназначен для сбора и обработки информации, полученной в ходе специальных, поисковых и проверочных мероприятий. В частности, данный программный комплекс позволяет автоматизировать процессы загрузки в хранилище данных (ХД) информации, поступающей от внешних источников, с обеспечением ее последующей оперативной обработки и анализа.

Программное средство «Octopus» является инструментом для анализа социальных сетей и больших массивов информации. Поэтому основной принцип работы с большими источниками данных посредством задач Octopus предполагает итеративное (пошаговое) накопление и анализ. «Octopus» включает в себя ряд режимов и инструментов для осуществления поставленных задач в интересах ОВД.

Рассмотрены основные аспекты особенности эксплуатации программных продуктов, представлены особенности использования современных информационных технологий при раскрытии и расследовании преступлений (как тяжких, так и особо тяжких).

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Гольдштейн Б.С. и др. Интерфейсы СОРМ. Справочник. – Санкт-Петербург : БХВ-Петербург, 2014. – 160 с.

2. Васильев А. Н. Python на примерах. Практический курс ·по программированию / А. Н. Васильев. – Санкт-Петербург : Наука и Техника, 2016. – 432 с.

3. Эксплуатация автоматизированных систем специального назначения: учебно-методическое пособие / С. Г. Мачтаков, В. В. Конобеевских, С. А. Мальцев. – Воронеж : Воронежский институт МВД России, 2016. – 182 с.

4. Основные возможности использования программного средства «Octopus» для анализа информации из открытых источников / В. В Конобеевских, Д. К. Печенина // Сборник материалов всероссийской научно-практической конференции Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем. – 2018. – С. 317 – 318.

5. Дьюсон Р. MicrosoftSQLServer 2008 для начинающих разработчиков. – Санкт-Петербург: БХВ-Петербург, 2010. – 704 с.

6. Кириллов В. В. Введение в реляционные базы данных / В. В. Кириллов, Г. Ю. Громов. – Санкт-Петербург : БХВ-Петербург, 2012. – 464 с.

7. Программное средство «Octopus». Компания ООО «БалтИнфоКом» [Электронный ресурс] : офиц. сайт. Санкт-Петербург, 2019. URL : http://baltinfocom.ru/BigData (дата обращения: 25.06.2020).

8. Программное средство «Octopus». Руководство пользователя : Компания ООО «БалтИнфоКом». Санкт-Петербург, 2017 – 82 с.