СОРМ 3

Системы СОРМ 3 обеспечивают длительное хранение и оперативный доступ к данным об абонентах и оказанных им услугах — звонках, смс, доступе к сайтам, электронной почте, VoIP-звонках и т. д.

Без контента

Система хранит только мета-данные, например, для электронной почты, будет сохранена тема, от кого и кому отправлено письмо, но не само письмо, для смс — дата отправки, номера абонентов, но не само сообщение.

Длительное хранение

Данные хранятся в системе годами это позволяет решать аналитические задачи статистическими методами.

Критерии поиска

- IP-адрес сервера, абонента
- Логин, IMSI, IMEI, MAC-адрес
- Адрес сайта
- Логин FTP-пользователя
- Адрес электронной почты
- Местоположение абонента
- Ник в чате и т. д.

Описание

Поиск по дате с 00:00 по 00:00

Идентификатор абонента

Login | Можно задать значение, список или перетащить текстовый файл в поле

IP источника

IP получателя

☐ Ресурсы и сервисы

☐ HTTP example.org/some/*

☐ FTP login

☐ E-mail petya@google.com ⇄ vasya@mail.ru

☐ IM nickname ⇄ nickname2

☐ VoIP nickname ⇄ nickname2

☐ Сессии абонентов

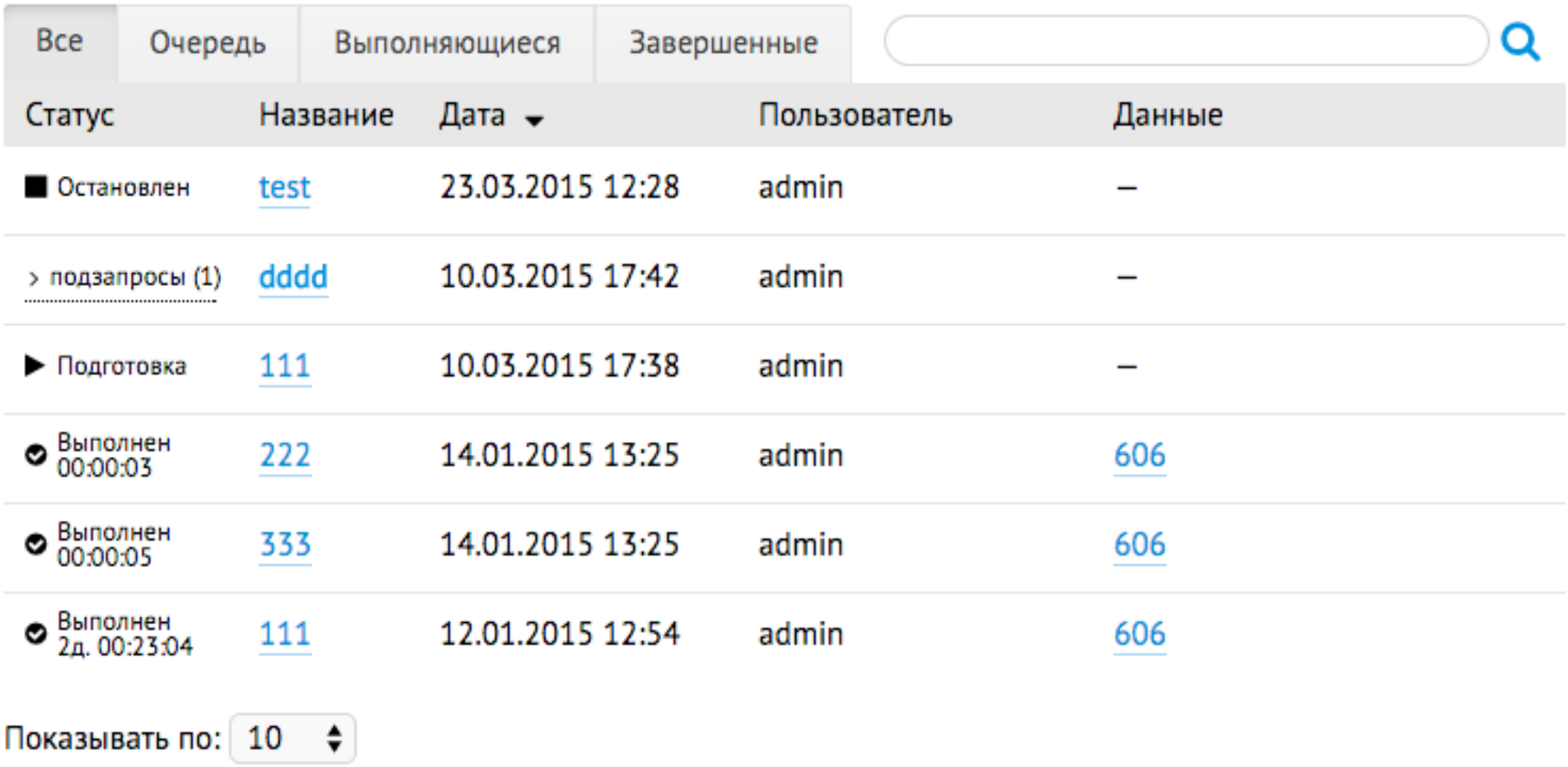
☐ Потоки

Полезные мелочи

Возможна работа со сторонними пультами
по протоколу ASN.1.

Поисковые поля поддерживают ввод списков значений и загрузку списков из файлов.

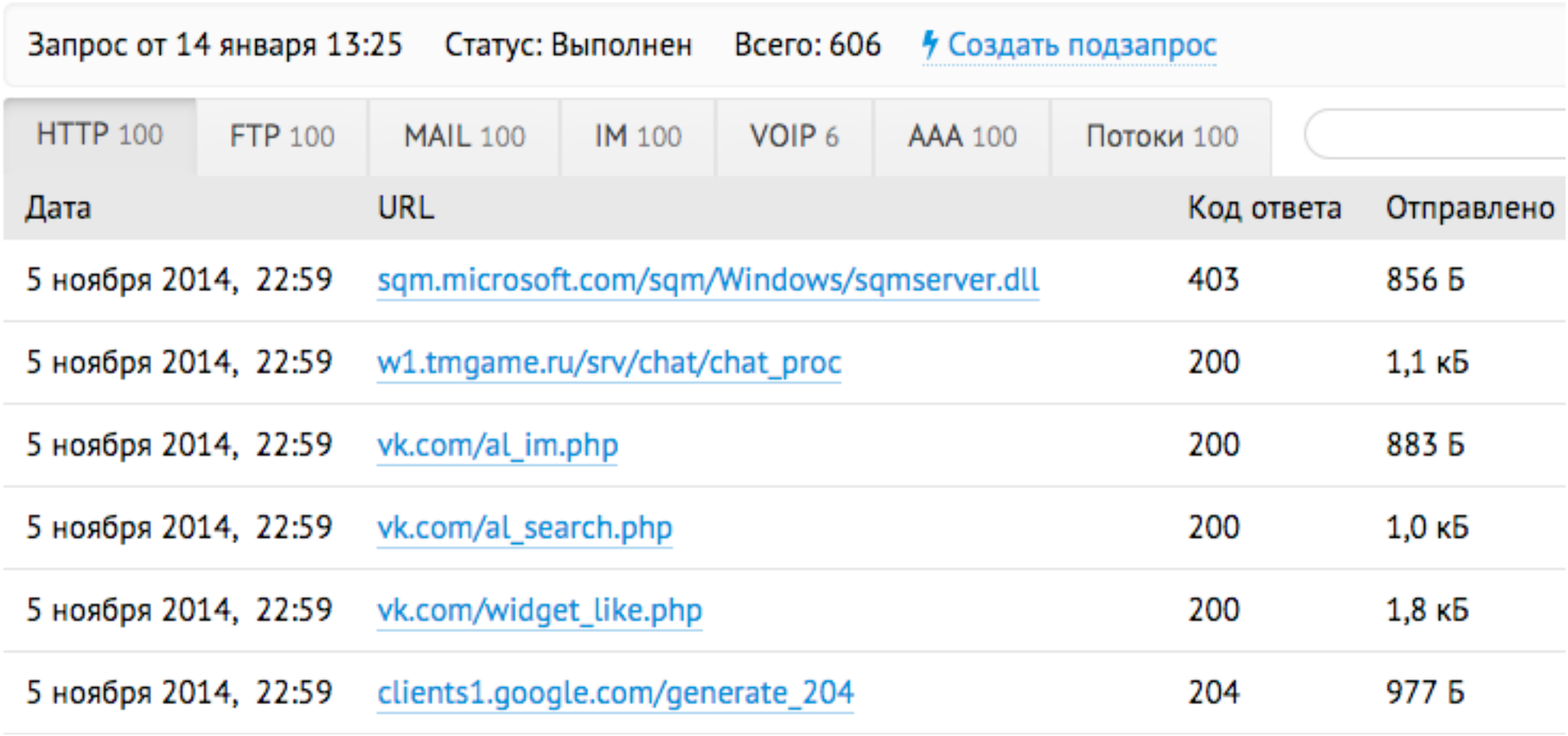
Поиск по прикладным протоколам (E-mail, IM, VoIP) может содержать пары идентификаторов и указывать направление, например, можно поискать только исходящую переписку с one@qip.ru на two@gmail.com.



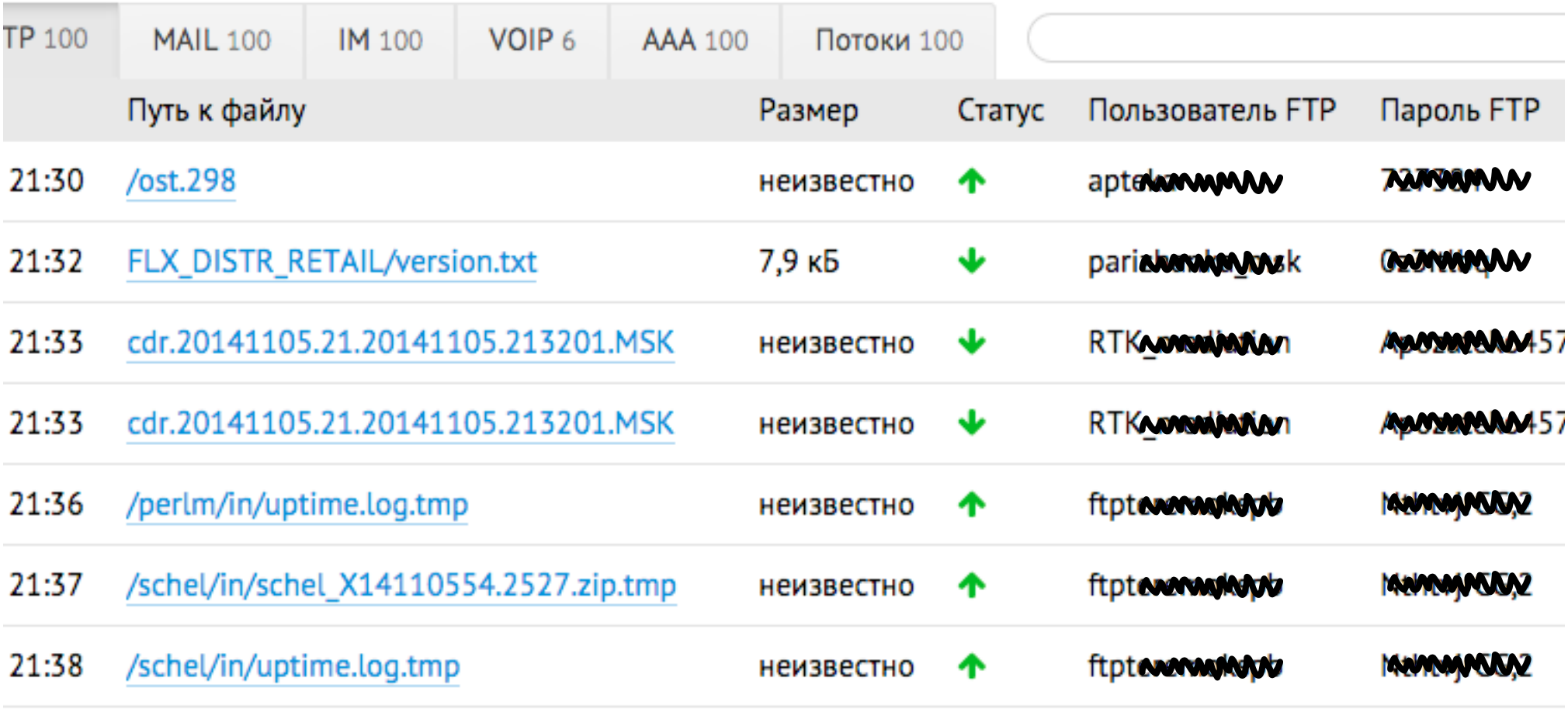
На больших объемах запросы могут долго работать, поэтому используется механизм фонового выполнения запросов.

Данные

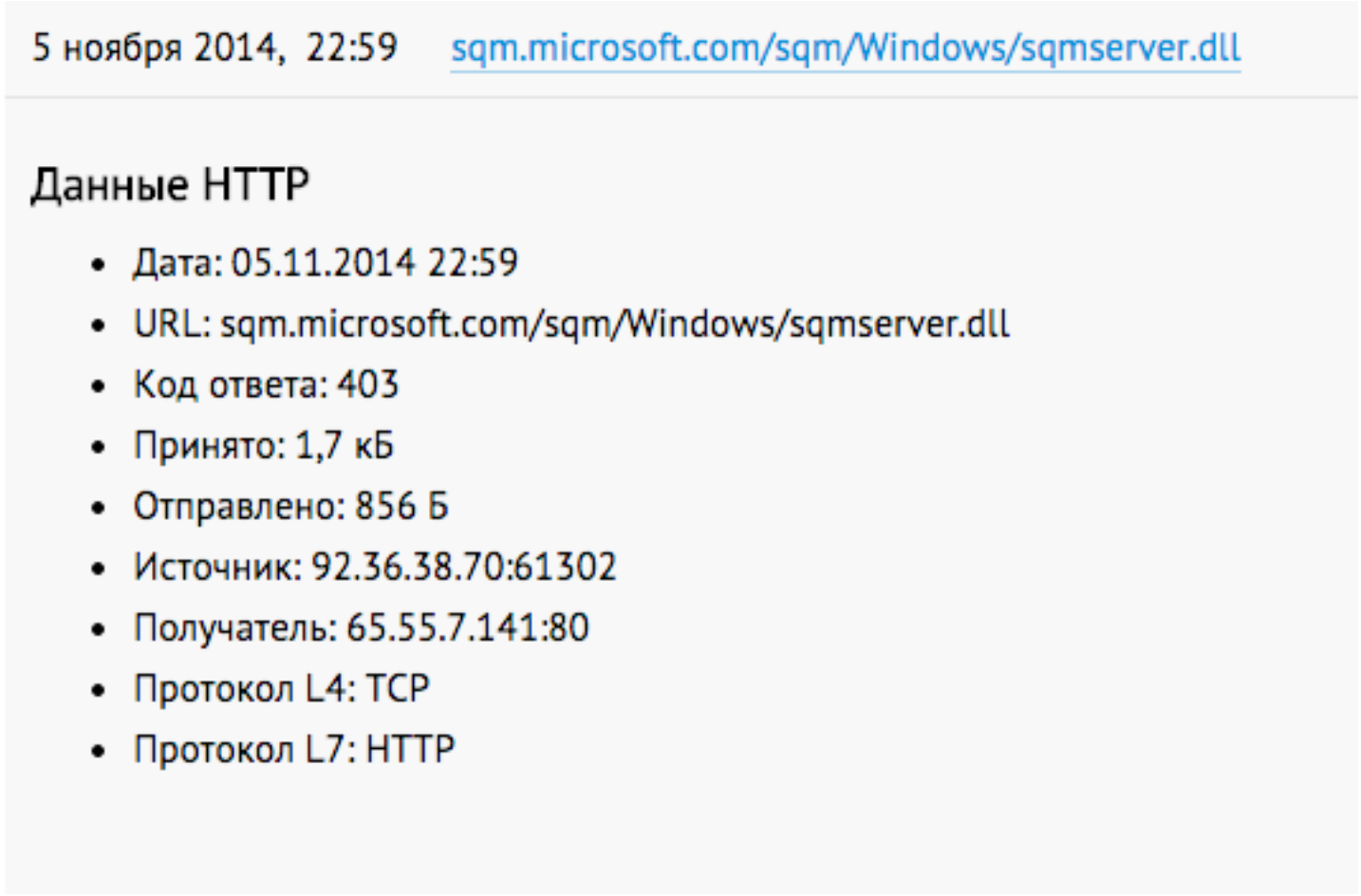
Результаты запросов автоматически разделяются по типу HTTP, FTP и т. д. Таблица результатов может быть отсортирована по любому полю. Умный фильтр показывает только то, что нужно пользователю.



Основные параметры по каждому типу протоколов представлены в табличном виде.



В результатах FTP сохраняется логин и пароль пользователя, размер, путь к файлу и т. д.



Для каждого типа протоколов доступен полный список полей.

12:43	TCP	AMAZON	1,8 кБ	4,9 кБ	00:00:03	1082779	–
12:43	UDP	BITTORRENT	1,5 кБ	1,0 кБ	00:00:03	5043023	–
12:43	UDP	BITTORRENT	1,2 кБ	929 Б	00:00:03	–	–
12:43	TCP	WHATSAPP	70,1 кБ	7,2 кБ	00:00:03	–	–
12:43	TCP	SKYPE	2,6 кБ	2,3 кБ	00:00:03	–	–
12:43	UDP	BITTORRENT	1,8 кБ	1,2 кБ	00:00:03	7185297	–

Уникальная особенность – все данные классифицируются по типу приложения (L7). Более 180 распознаваемых типов приложений.

Справочники

Справочники абонентов и базовых станций выгружаются оператором и позволяют определить принадлежность номера физическому или юридическому лицу, показать события на карте.

ФИО	MSISDN	IMSI	ICC
[redacted] ★ в Избранное	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

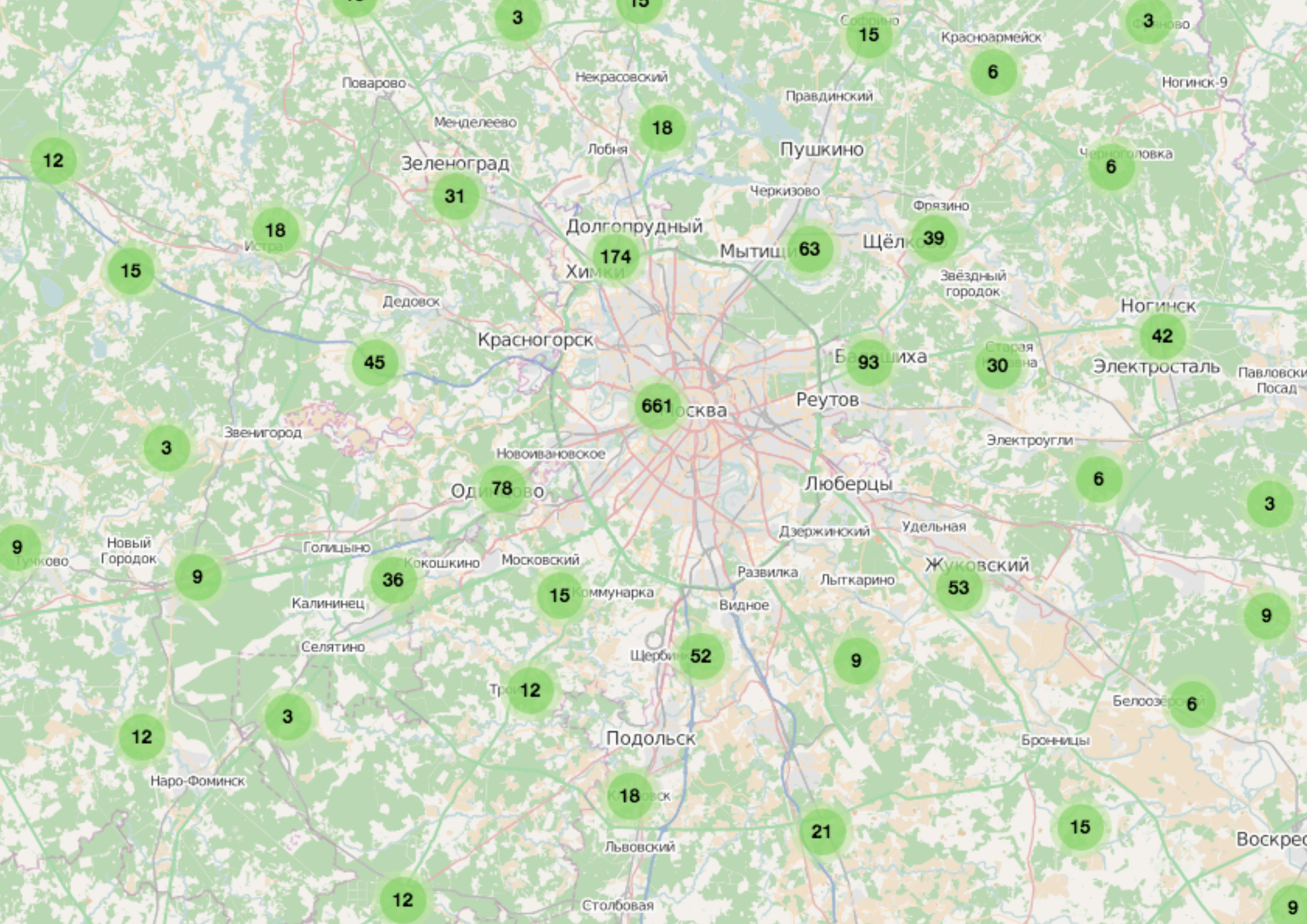
Данные из справочника автоматически привязываются к результатам запросов. Возможен поиск по данным из справочника абонентов.

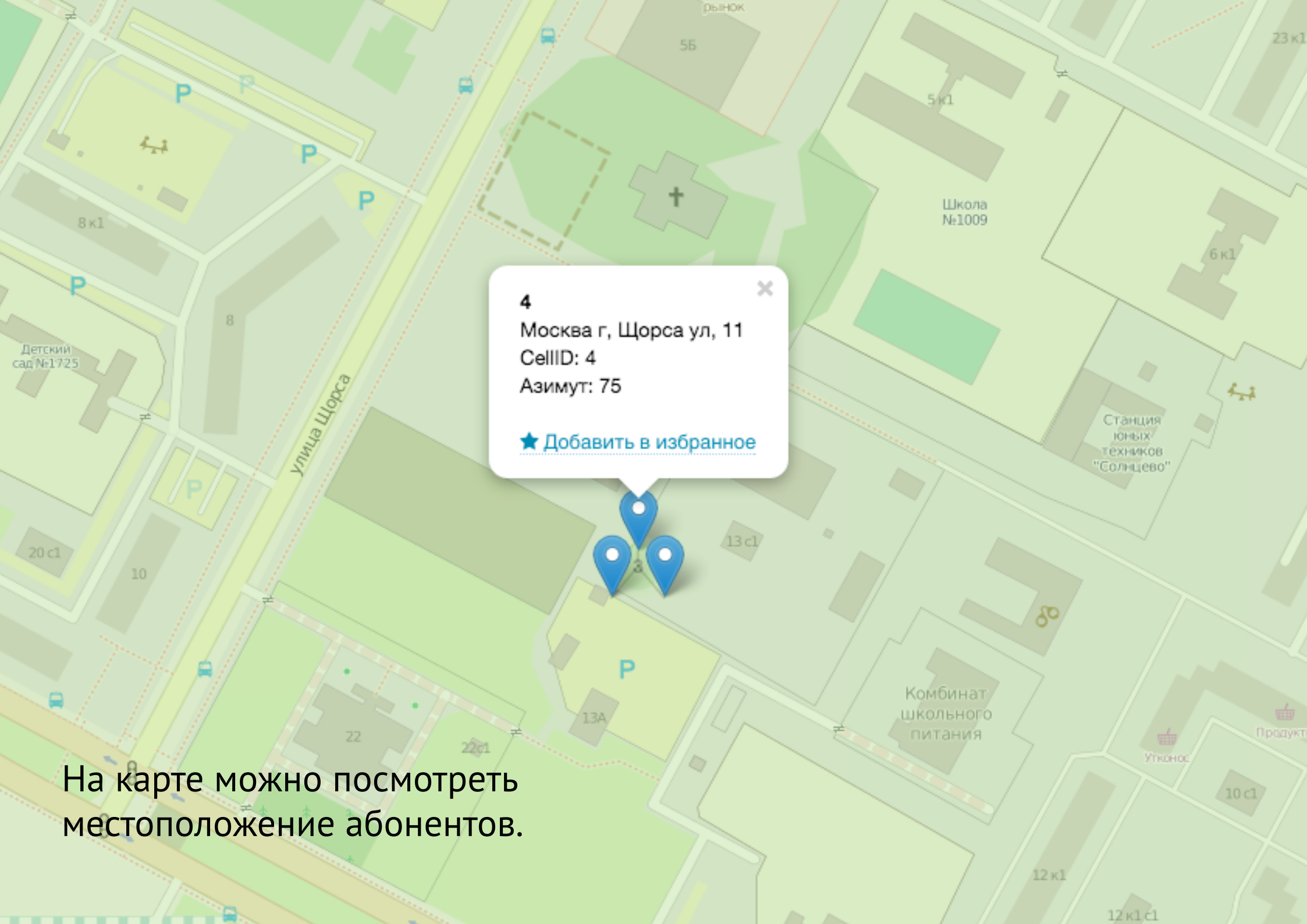
Адрес	Оператор	LAC	CELL	Широта	Долгота	Азимут	Высо
Московская обл, Химки г, Ленинградская ул, 29	[redacted]	0	2	55.903	37.420	30	41.6
Московская обл, Химки г, Ленинградская ул, 29	[redacted]	0	2	55.903	37.420	150	41.6
Московская обл, Химки г, Ленинградская ул, 29	[redacted]	0	2	55.903	37.420	270	41.6
Москва г, Зубовская пл, 3	[redacted]	0	5	55.738	37.586	50	27.5
Москва г, Зубовская пл, 3	[redacted]	0	5	55.738	37.586	130	28

Данные из справочника автоматически привязываются к результатам запросов. Возможен поиск по данным из справочника базовых станций.

Местоположение

Информация о местоположении абонента визуализируется на карте.


3
15
Красноармейск
3
6
Ногинск-9
Поварово
Некрасовский
Правдинский
Менделеево
18
Лобня
Пушкино
12
Зеленоград
6
Черноголовка
31
Черкизово
Фрязино
18
Долгопрудный
39
Щёлк
15
174
Химки
Мытищи
63
Звёздный городок
Дедовок
Ногинск
42
Красногорск
45
93
30
Электросталь
Павловски Посад
661
Реутов
Звенигород
3
Электроугли
Новоивановское
6
78
Люберцы
3
9
Новый Городок
Дзержинский
Удельная
Голицыно
Кокошкино
Московский
Развилка
Лыткарино
Жуковский
9
36
15
53
Калининец
Коммунарка
Видное
9
Селятино
52
9
12
6
3
12
Подольск
Бронницы
Наро-Фоминск
18
21
15
Львовский
12
Столбовая
9



На карте можно посмотреть местоположение абонентов.

Пользователи и система прав

Многоступенчатая система прав обеспечивает гибкие настройки разграничения зоны ответственности пользователей.

- Базовая
  - admin
  - new user
- группа 1
  - 12
  - 123

Логин: admin

Группа: Базовая

Фамилия И. О.: admin

Статус: Включен

Права пользователя:

В системе

Администрирование
- База данных
- Устройства
- Журналы
- Пользователи

Данные
- Экспорт
- Пометки
- Просмотр

Запросы
- Выполнение
- Просмотр
- Управление

В своей группе

Администрирование
- Пользователи

Данные
- Экспорт
- Пометки
- Просмотр

Запросы
- Выполнение
- Просмотр
- Управление

Журналы

Все действия пользователей в системе логируются и сохраняются в журнал, это позволяет проводить проверки в случае возникновения утечек данных и прочих неправомерный действий.

Действия пользователей

За всё время | Все события

Дата	Событие
29.12.2014 18:01	Пользователь admin вошел в систему с IP-адреса 10.0.2.2
29.12.2014 18:01	Пользователь admin вышел из системы
12.01.2015 12:53	Пользователь admin вошел в систему с IP-адреса [redacted].210
12.01.2015 12:53	Пользователь admin вышел из системы
12.01.2015 12:54	Пользователь admin вошел в систему с IP-адреса [redacted]
12.01.2015 12:54	Новый IPDR запрос 111
12.01.2015 12:54	Пользователь admin вошел в систему с IP-адреса [redacted].210
14.01.2015 13:11	Пользователь admin вошел в систему с IP-адреса [redacted].210
14.01.2015 13:25	Новый IPDR запрос 222
14.01.2015 13:25	Новый IPDR запрос 333

Мониторинг

В режиме онлайн производится мониторинг параметров серверов и прочего оборудования, входящего в состав комплекса это позволяет своевременно реагировать на возможные отказы аппаратуры.

0 %

диск: 35,4 ГБ, занято: 52 %

18,30

Всего: 23,5 ГБ, занято: 78 %

Вход 8,91

Выход 8,91

Загрузка процессора | Температура процессора | Загрузка памяти | Использование HDD | Сеть | Потери