

# Система параллельной обработки трафика оператора мобильной связи

А.С. Трофимов, М.К. Чобану

Национальный исследовательский университет «МЭИ» (НИУ «МЭИ»), molochmail@gmail.com

**Аннотация** — В статье рассмотрен вопрос построения массивно-параллельной масштабируемой системы анализа трафика абонентов оператора мобильной связи.

**Ключевые слова** — СОРМ, эффективный захват трафика, параллельная обработка данных, резервирование.

## I. ВВЕДЕНИЕ

Обработка информации в части анализа трафика является важным аспектом цифровой обработки сигналов. В 2013 году приняты поправки к закону о связи [1], касающиеся мониторинга активности абонентов сетей мобильной связи для функционирования системы технических средств обеспечения функций оперативно-розыскных мероприятий (СОРМ), в частности, в области взаимодействия через сеть Интернет. В рамках данных поправок регламентируется обязательный захват,

анализ и хранение всего исходящего и входящего трафика абонентов сети оператора мобильной связи.

В статье изложены результаты проекта по исследованию и разработке массивно-параллельной масштабируемой системы анализа трафика, приведено описание архитектура проекта с точки зрения эффективного параллельного выполнения, а также проведено сравнение по параметрам результатов проекта с существующими аналогами.

Целью проекта является создание масштабируемой системы по потоковой обработке сетевого трафика оператора для исполнения требований закона. Для решения задачи использованы методы экспериментального анализа и прототипирования.

На рис. 1 приведена общая схема включения системы СОРМ в инфраструктуру оператора мобильной связи.

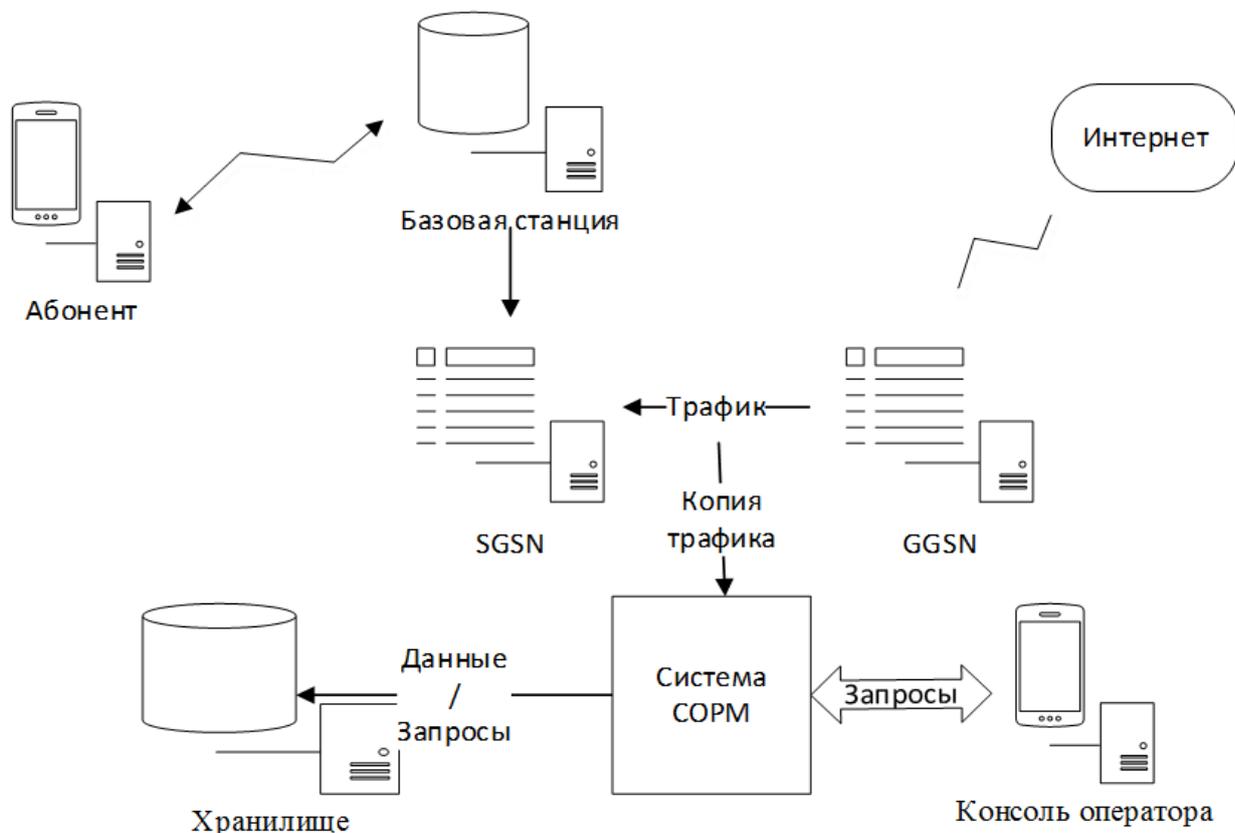


Рис. 1. Схема включения СОРМ в инфраструктуру оператора мобильной связи

Рассмотрим подробнее компоненты схемы. Абонент – это телефон или какое-либо другое устройство, оборудованное модулем GSM [2] (Group Special Mobile) / GPRS (General Packet Radio Service) связи. Базовая станция – это точка подключения абонентского устройства к инфраструктуре оператора мобильной связи. SGSN (Serving GPRS Support Node) это один из ключевых компонентов сети мобильной связи, отвечающий за передачу пакетов данных, пришедших от абонентского устройства, в сеть оператора мобильной связи. GGSN (Gateway GPRS Support Node) – это узел сети GPRS, отвечающий за маршрутизацию пакета данных из внутренней сети оператора мобильной связи во внешнюю сеть Интернет.

## II. СУЩЕСТВУЮЩИЕ СИСТЕМЫ COPM

**Система Яхонт** [3]. Данная система представляет собой набор аппаратно-программных средств для анализа трафика различных операторов связи. Она поддерживает взаимодействие со следующими сервисами операторов связи: выделенный и модемный доступ в Интернет, связь на базе IP транспорта передачи данных, подвижная связь через GPRS/EDGE/UMTS/WiFi/WiMAX, связь через VoIP, веб хостинг и виртуальные выделенные серверы.

**Достоинства:** система обладает возможностью обработки до 160 Гбит/с при каскадном включении звеньев, обеспечивает до 1.16 Гбит/с (до 4 Тб/час) записи индексированных данных в хранилище, объём хранимой информации до нескольких петабайт, позволяет работать с несколькими источниками данных (не только трафик сети), имеется возможность строить запросы к хранилищу параллельно с записью потока данных, возможность работы с несколькими интерфейсами 10G, возможность строить сложные запросы, включая многокритериальные запросы, тонкий клиент-интерфейс оператора.

**Недостатки системы:** существует ограничение по масштабируемости обрабатываемого потока (максимальный входящий трафик при каскадном включении до 160 Гбит/с), низкая скорость сохранения данных до 1.16 Гбит/с.

**Система Январь** [4]. Данная система состоит из программно-аппаратного комплекса и предназначена для долгосрочного хранения и оперативного доступа к данным абонента, и оказанным услугам связи. Данная система представляет собой комплексное решение, позволяющее сохранять данные о совершённых голосовых вызовах абонента, отправленных и принятых SMS, и MMS, стоит отметить также фиксацию положения абонента в текущий момент времени, что позволяет упростить поиск потенциально-опасного абонента.

**Достоинства:** достаточно высокая производительность, возможность работы с другими системами оператора (биллинг и т.д.).

**Недостатки системы:** ограничение по масштабируемости и по объёму встроенного хранилища (10 Тб).

## III. АРХИТЕКТУРА МАССИВНО ПАРАЛЛЕЛЬНОЙ МАСШТАБИРУЕМОЙ СИСТЕМЫ COPM

Разработка массивно параллельной масштабируемой системы COPM является инновационной задачей и ранее была мало освещена в публичных источниках.

В основу проекта положены следующие формализованные требования, отвечающие требованиям закона о связи:

- 1) Система должна быть линейно-масштабируемой в любом направлении.
- 2) Захват и обработка трафика должны быть максимально производительными.
- 3) Система должна позволять использовать гетерогенное оборудование (что позволяет диверсифицировать заказ аппаратного обеспечения центров обработки данных).
- 4) Система должна обеспечивать избыточность, саморезервирование и отказоустойчивость даже в случае полного выхода из строя части серверов.

В рамках исследовательской работы был проведён анализ существующих подходов к реализации подобных систем, проведены эксперименты, разработан ряд прототипов, итеративно улучшающих эффективность работы проектируемой системы. В результате исследования и прототипирования была сформирована модель массивно параллельная масштабируемая архитектура системы. На рис. 2 схематично представлена данная архитектура.

Рассмотрим компоненты разработанной системы.

В целом модель системы представляет собой многоуровневый конвейер обработки данных, формально разделённый на слои по функциональному назначению.

*Первым слоем* системы является слой модулей системы захвата трафика, которые удовлетворяют всем четырём требованиям, формализованным ранее.

Во-первых, при добавлении новых сетевых интерфейсов в сервер системы захвата трафика получается линейный прирост производительности захвата трафика, также прирост возможен при добавлении новых модулей (или процессоров) в существующую конфигурацию, кроме того данный слой отвечает за первичную балансировку трафика, гарантируя эффективную загрузку последующих слоёв.

Во-вторых, за счёт механизма быстрого захвата пакетов уровня ядра операционной системы обеспечена максимальная производительность данного слоя.

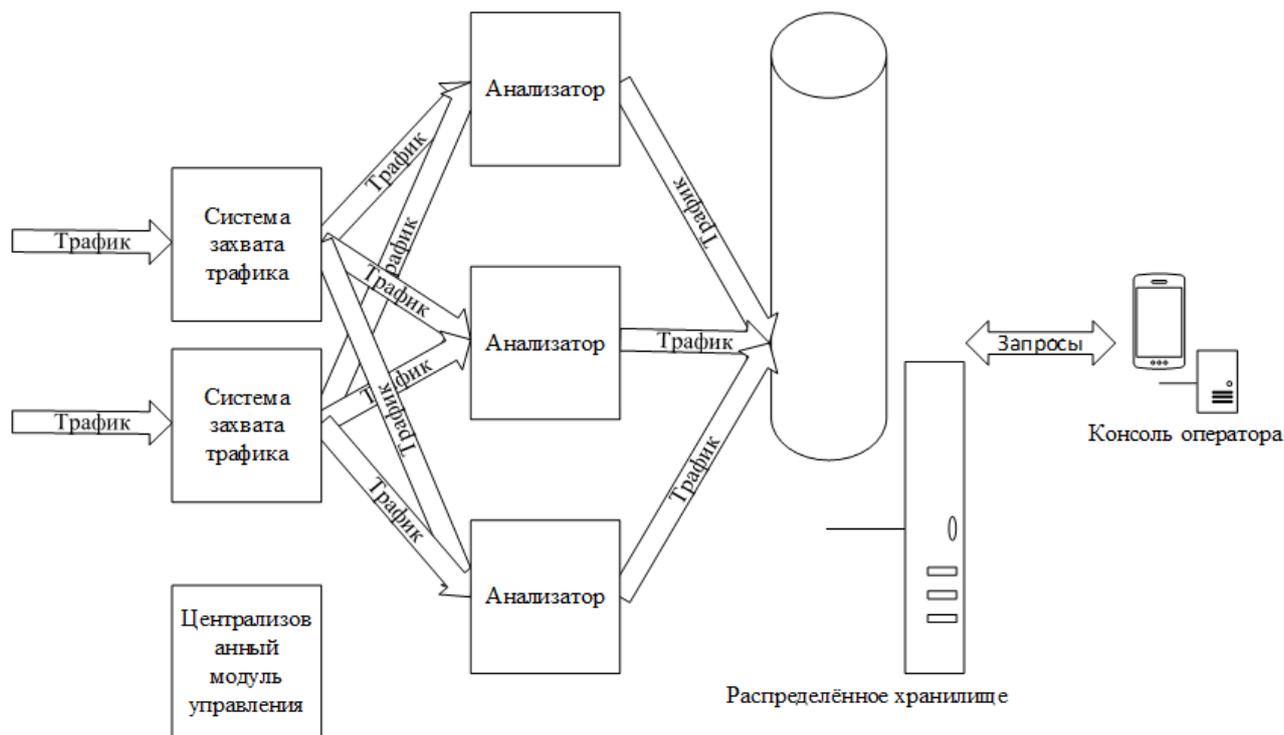


Рис. 2. Архитектура массивно параллельной масштабируемой системы СОРМ

В-третьих, в качестве базового аппаратного обеспечения для моделирования использовалась и может быть использована любая бездисковая 64-битная система с достаточным объёмом памяти (порядка 16 Гб на один сетевой интерфейс 10G) и достаточным числом процессоров (порядка 8 на один сетевой интерфейс 10G).

В-четвёртых, в зависимости от требований к конкретной конфигурации обеспечения отказоустойчивости, можно обеспечить полное или частичное двойное и тройное резервирование.

Первый слой является наиболее критичным для обеспечения полной обработки трафика оператора без потерь.

Вторым слоем системы является слой модулей анализа трафика, он так же, как и первый слой, удовлетворяет всем формальным требованиям к системе.

Во-первых, при добавлении новых серверов обеспечивается линейный рост производительности слоя за счёт механизмов балансировки первого слоя и автоматической балансировки загрузки второго слоя.

Во-вторых, данный слой обеспечивает эффективную параллельную обработку и фактически независим по данным, что снижает до минимума необходимость взаимодействия между модулями слоя.

В-третьих, в качестве базового оборудования использовались сервера ранее приобретённые оператором связи для общих нужд центра обработки

данных, точнее может быть использованы как новые, так и несколько устаревшие вычислительные системы.

В-четвёртых, данный слой в зависимости от требований может обеспечивать как неполное (+1 - +N), так и двойное, и тройное резервирование, в зависимости от требований к отказоустойчивости оператора мобильной связи.

Данный слой является ключевым звеном системы, формирующим множество фактически хранимых данных. Исключая нерелевантную информацию из захваченного потока данных и формируя карту социальных связей абонентов.

Третий слой состоит из децентрализованного хранилища данных, так же как и предыдущие, удовлетворяющего всем формальным требованиям к системе.

Во-первых, при добавлении новых серверов обеспечивается линейный рост производительности и практически линейный рост дискового пространства.

Во-вторых, данные хранятся параллельно на множестве серверов и на множестве носителей.

В-третьих, базовая платформа достаточно нетребовательна к аппаратному обеспечению, впрочем, чем выше производительность дисковой подсистемы, тем выше результирующая производительность.

В-четвёртых, данный слой архитектурно-саморезервированный, так как данные хранятся всегда

в виде 2-3 копий на разных носителях и на разных серверах хранилища.

Данный слой является так же очень важным для полноценного функционирования системы и обеспечения оперативного доступа к собранным данным.

Детально рассмотрим централизованный модуль управления и консоль оператора. Централизованный модуль управления представляет собой кроссплатформенный сервис, управляющий и контролирующей работу всех без исключения подсистем системы СОРМ, позволяющий оперативно обнаруживать наличие сбоев и автоматически исправлять их. Кроме сбора информации о состоянии всех слоёв системы модуль управления отвечает за доставку и применение новых параметров конфигурации модулей системы, заданных администратором.

Интерфейс оператора системы СОРМ предоставляет доступ к различным формам вывода результатов работы системы. Например, консоль позволяет формировать общую отчётность по функционированию сети оператора, формировать общую отчётность по маркерам, сигнализирующим возможную незаконную деятельность абонентов, формировать детальную отчётность по конкретному абоненту и связанными с ним людьми.

Стоит отметить, что наиболее важным аспектом архитектуры системы является то, что каждый слой является независимым и может быть расширен или урезан в зависимости от настроек сети, свойств поступающего трафика и изменения абонентской базы, что теоретически не ограничивает сверху возможность увеличения поступающего трафика.

Результат исследования и разработки позволяет решить проблемы масштабируемости существующих систем и в значительной степени улучшить параллельность функционирования.

#### IV. АППАРАТНО-ПРОГРАММНАЯ РЕАЛИЗАЦИЯ

Прототип системы был построен на базе серверной платформы компании IBM, включающей в себя двух-юнитовые сервера со следующей аппаратной конфигурацией:

- 1) Четыре процессора семейства x86 производства компании Intel модель Xeon E5540.
- 2) Оперативная память DDR3-1066 объёмом 32Гбайт.
- 3) Два сетевых адаптера 10Гбит производства компании Broadcom модели BCM57710 (для непосредственного захвата трафика и последующей передачи одного анализирующему слою).
- 4) Сетевой адаптер 1Гбит производства компании Intel, для обеспечения задач управления и мониторинга системы.
- 5) Жёсткий диск объёмом 500ГБ (для начальной загрузки системы).

Данная конфигурация аппаратной платформы была использована как базовая для всех вычислительных узлов системы анализа трафика.

На модулях, обеспечивающих первичный захват трафика было использовано ядро ОС Linux с минимальным программным обеспечением пользовательского пространства. Как было сказано ранее функция захвата пакетов и первичной обработки была реализована на уровне ядра операционной системы.

На модулях анализа трафика использовались как ОС семейства Linux, так и ОС семейства Windows, что стало возможно в виду кроссплатформенной реализации вычислительного ядра системы. Стоит отметить, что слой анализа обладал дополнительным набором жёстких дисков для обеспечения отказоустойчивости и возможности сохранения живых сессий локально.

На модулях хранения использовалось внешнее отказоустойчивое хранилище, а также был значительно расширен объём оперативной памяти (до 128Гбайт).

#### V. РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

Система была внедрена и практически апробирована на базе оператора мобильной связи Московского региона, что позволило достичь следующих результатов:

- 1) Макет системы был построен на базе двух модулей захвата трафика, трёх модулей анализа и одного модуля хранилища, схема представлена на рисунке 3.
- 2) Система обеспечила покрытие юго-восточного сегмента сети.
- 3) Система обеспечила бесперебойное функционирование в режиме 24/7.
- 4) Объём хранилища для обработанных данных и полных сессий составил 100 Тбайт.
- 5) Скорость обрабатываемого трафика (средняя и пиковая) 4Гбит / 18Гбит.
- 6) Скорость выборки результатов обеспечена на уровне не более 10 минут при комплексных запросах на интервале 1 месяц.

На рисунке 4 приведён график интегрального уровня загрузки вычислительных блоков в зависимости от скорости входящего трафика.

Стоит ещё раз отметить, что для эффективности реализации системы были использованы компоненты доступные на рынке аппаратных компонент, кроме того не использовалась специальная адаптация программного обеспечения для аппаратной платформы ввиду требований изначально поставленной задачи по возможности неограниченного расширения системы как горизонтально, так и вертикально.



Рис. 3. Схема экспериментального стенда

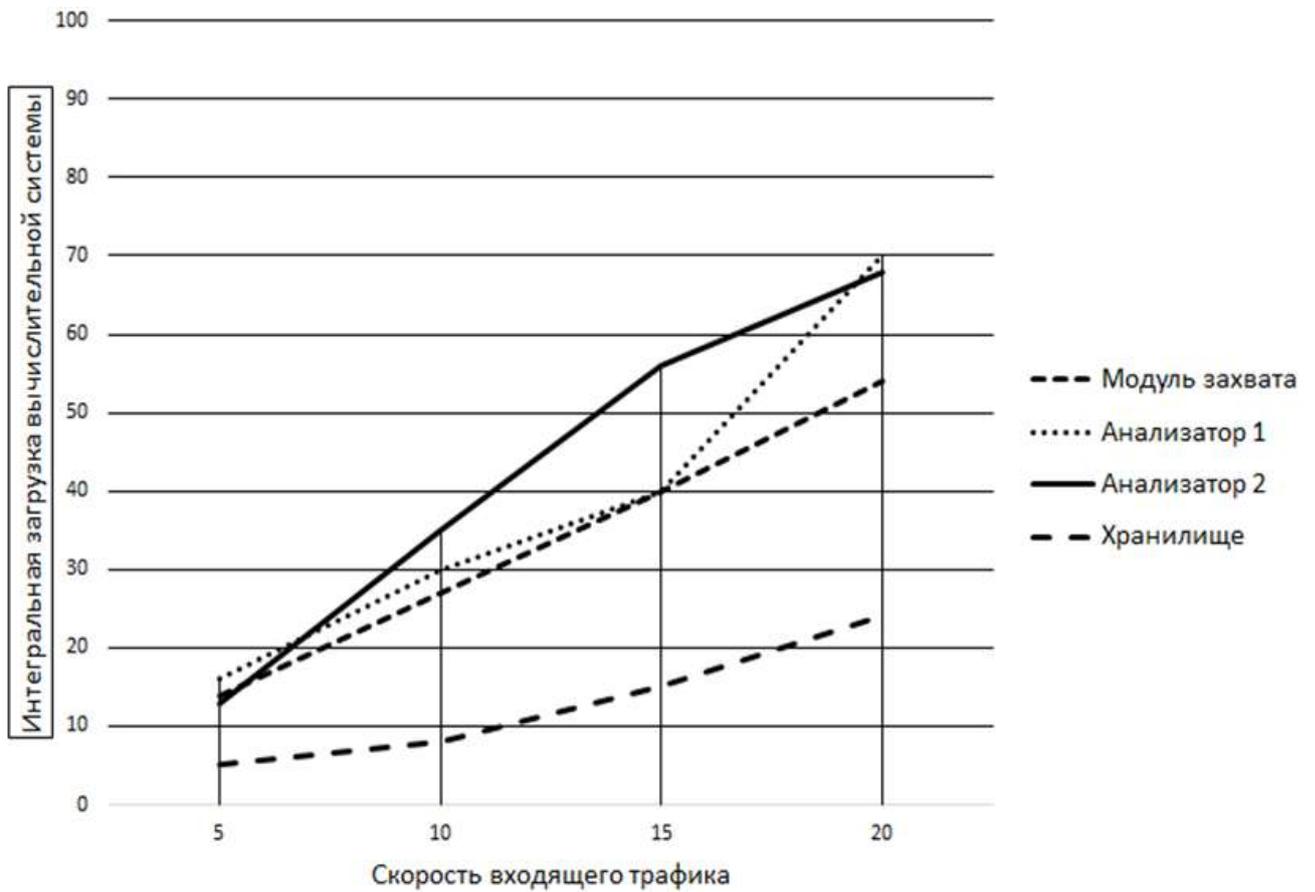


Рис. 4. График загрузки вычислительных блоков

В отличие от существующих систем разработанное решение позволяет обеспечить обработку растущих объёмов потоков данных, при этом не ограничивая эффективность работы системы сверху ввиду архитектурных особенностей.

В ходе экспериментов были выявлены значительные недостатки операционной системы семейства Windows, а именно:

7) Ограничение производительности POSIX совместимого интерфейса сокетов.

8) Невозможность эффективно работать с более чем 10000 открытых файловых дескрипторов.

В особенности эти ограничения касаются версий операционной системы ранее Windows 2008 R2.

Вследствие данных проблем было принято решение не использовать Windows в качестве базовой платформы для модулей анализа.

#### VI. ОЦЕНОЧНАЯ МОДЕЛЬ ТРЕБОВАНИЙ К СИСТЕМЕ

Для упрощения оценки требований по прогнозированию производительности была проведена оценка загрузки системы в зависимости от уровня входящего трафика. В результате данной оценки были сформированы оценочные формулы для вычисления параметров оборудования для обеспечения заданной производительности системы. Предположим, что конфигурация серверов одинакова для всех звеньев системы. Тогда:

$$N = R \left( \frac{S}{10 \cdot 3.75} \right) + 1, \quad (1)$$

где  $N$  – количество узлов модулей захвата,  $R$  – функция округления к большему целому,  $S$  – скорость трафика,  $+1$  – избыточность для обеспечения резервирования.

$$A = R \left( \frac{S}{10 \cdot 3} \right) + 1, \quad (2)$$

где  $A$  – количество узлов анализаторов,  $R$  – функция округления к большему целому,  $S$  – скорость трафика,  $+1$  – избыточность для обеспечения резервирования.

$$B = R \left( \frac{S}{10 \cdot 9} \right) + 1, \quad (3)$$

где  $B$  – количество узлов распределённого хранилища,  $R$  – функция округления к большему целому,  $S$  – скорость трафика,  $+1$  – избыточность для обеспечения резервирования

Для сравнения приведём параметры системы необходимые для того чтобы достичь и превзойти производительность системы Яхонт:  $N=6$ ,  $A=7$ ,  $B=2$ .

#### ЛИТЕРАТУРА

- [1] Федеральный закон «О связи» №126-ФЗ.
- [2] Timo Halonen, Javier Romero, Juan Melero GSM, GPRS and EDGE Performance. John Wiley & Sons USA, 2003 654 с.
- [3] Описание системы Яхонт <http://www.norsitrans.ru/pdetail/yahont-sorm3>, 04.03.2014
- [4] Описание системы Январь <http://www.mfisoft.ru/products/sorm/sorm3/yanvar>, 04.03.2014