*УДК ?*

Андресюк Богдан

Бойкив Тарас

Паламарчук Валерий

Щербина Александр

Национальный технический университет Украины «КПИ», Киев, Украина

**Заглавие?**

**Аннотация.** Предложено улучшение алгоритма планирования А\* для использования в Private Cloud системах реального времени. Алгоритм в связке с алгоритмом разделения секрета Shamir позволяет обеспечить статическое планирование с учетом уровня безопасности и требуемого времени отклика для задач. Обеспечивается безопасность доставки задач в Cloud систему и результатов обратно к пользователю.

**Анотація.** Запропоновано покращення алгоритму планування А\* для використання в Private Cloud системах реального часу. Алгоритм у парі з алгоритмом розподілу даних Shamir дозволяє забезпечити статичне планування з урахуванням рівня безпеки і вимагаємого часу відгуку системи для задач. Забезпечується безпека доставки задач до Cloud системи і результатів назад до користувача.

**Annotation.** Proposed improvement of the scheduling algorithm A \* for use in the Private Cloud real-time systems. Algorithm in composition with the Shamir secret sharing algorithm gives: static task scheduling, high level security and the required response times for the tasks. Ensures safe delivery tasks in Cloud system and the results back to the user.

**Ключевые слова**. Private Cloud, система реального времени, планирование распределения задач.

**Ключові слова**. Private Cloud, система реального часу, планування розподілу задач.

**Keywords.** Private Cloud, real time system, task scheduling.

**Постановка проблемы.** Запуск задач с требованиями реального времени в Cloud системе, накладывает определенный набор требований к уровню обслуживания задач в Cloud системе. Использование стандартных алгоритмов планирования и обеспечения безопасности в Cloud системе не позволяет удовлетворять эти требования.

**Анализ последних исследований и публикаций.** Согласно последним данным NIST (Национальный институт стандартов и технологий США) "Cloud Computing Synopis and Recommendations"[1] частное облако – облачная инфраструктура, которая эксплуатируется исключительно организацией, может находиться под управлением организации или третьей стороны, и быть собственностью организации или третьей стороны.

**Периметр безопасности**

**Периметр безопасности**

\*\*\*

Клиент

Клиент

\*\*\*

Клиент

Клиент

А

В

Рис. 1 А- Собственное частное облако, В - стороннее частное облако

При использовании собственного частного облака нет необходимости полагаться на внешние сети, а также легче обеспечить внутреннюю безопасность. Но для создания и поддержки этой инфраструктуры потребуются значительно большие средства, чем при использовании сторонних сервисов. Кроме того, доступно меньшее количество ресурсов для расширения облака при внезапной нарастающей вычислительной нагрузке. Таким образом теряются некоторые из ключевых преимуществ облачных систем.

При использовании стороннего частного облака, появляется большая гибкость в предоставлении дополнительных ресурсов в короткие сроки. Но данная инфраструктура будет частично зависеть от внешних сетей, что потребует усилий для обеспечения безопасности.

Для того чтобы задачи с требованиями реального времени могли выполнятся в Cloud системе, она должна удовлетворять следующим требованиям.

**Основные требования для облачных систем реального времени**

1. Высокоскоростные источники данных. Эти данные должны быть вытеснены в облако, а затем к пользователю. Опрос готовности данных требует слишком много времени и потребляет слишком много пропускной способности.[2]

2. Низкие задержки передачи данных. Данные должны передаваться быстро и легко с помощью системы в базу данных реального времени. Реляционные базы данных, обычно используемые для бизнес-систем, являются слишком медленными.

3. Несколько типов пользователей. Разные пользователи, такие как веб-браузеры, базы данных, электронные таблицы должны иметь доступ к одному источнику данных.[3]

4. Независимая система резервирования. Необходимо предоставить возможность обеспечить полное резервирование каналов передачи данных, которые будут задействованы в случае любого перерыва в обслуживании.

5. Локальная синхронизация. Система должна содержать полную копию данных с источника, и в реальном времени отправлять их пользователям по локальной сети. Если канал связи с облаком прерван, локальные клиенты и серверы не должны реагировать на сбой в работе сети. Вместо этого должны появиться отдельные области управления, которые смогут продолжить работу как "островки автоматизации", пока связь с облаком не будет восстановлена.[4]

**Основные нерешенные части общей проблемы.** Удовлетворение одновременно требований систем реального времени и Cloud системы сложная задача. Необходимо обеспечить заданное время отклика задачи и обеспечить гибкость выделения ресурсов в Cloud системе. Основными проблемами являются: выполнение планирования с учетом обеспечения заданного времени отклика, обеспечения требуемого уровня безопасности.

**Цель статьи.** Предложены улучшения существующего алгоритма для выполнения планирования в Cloud системе с учетом требований задач реального времени, а также предложена схема обеспечения безопасности как внутри Cloud системы так и при пересылки задач от клиента и при отправке результатов клиенту.

**Изложение основного материала статьи. Описание модели СРВ**

N

**Cloud система реального времени**

N

N – канальное соединение

N

**Группа клиентов**

**Уровень безопасности N**

**Группа клиентов**

**Уровень безопасности 1**

Входная очередь

Выходная очередь

Клиент

Клиент

SSA

Канал обслуживания

Планировщик

Канал обслуживания

\*\*\*

Клиент

Клиент

SSA

SSA

SSA

N

SSA

SSA

N

\*\*\*

Рис. 2 Структура разработанной модели Cloud системы реального времени

Клиенты системы разделяются на группы по уровню безопасности которую они требуют от системы и приоритетов. Для клиентов которые требуют уровень безопасности выше минимального, является необходимым иметь несколько каналов связи с Cloud системой, для возможности передачи частей задачи по разным каналам. Клиентам с более высоким уровнем приоритета гарантируется большая вероятность безотказной работы.

Для клиентов с уровнем безопасности выше минимального, задача разделяется по алгоритму Шамира на n частей и по разным каналам доставляется во входную очередь системы где и собирается из частей.

Если же пользователь требует только минимальный уровень безопасности, то задача доставляется без деления по одному каналу связи.

Во входной очереди накапливаются задачи на выполнение. Каждая задача имеет такие параметры: приоритет, уровень безопасности, требования к оборудованию (объем памяти, частота процессора), время выполнения на требуемом оборудовании, время за которое должен быть получен результат.

Через заданный в системе промежуток времени или после накопления определенного количества задач во входной очереди, производится планирование распределения задач по ресурсам.

Каждый ресурс системы имеет набор параметров: объем памяти, количество ядер и частоту процессора, уровень безопасности – определяется степенью защищенности машины.

После планирования задачи доставляются на каналы обслуживания, где происходит выполнение заданий.

После завершения обработки результаты задач попадают в выходную очередь.

Результаты задач с минимальным уровнем безопасности из выходной очереди доставляются клиентам, а все остальные разделяются на части по алгоритму Шамира и доставляются клиентам по нескольким каналам связи.

**Распределение задач по ресурсам в Cloud системе**

Для оптимальной загрузки ресурсов Cloud системы и для предоставления задачам требуемый уровень сервиса необходимо планировать распределения задач по ресурсам системы. Также необходимо учитывать требования реального времени. Рассмотрим существующие алгоритмы планирования.

**BackFill**

Алгоритм планирования BACKFILL разработан для максимально эффективного использования ресурсов и достижения высокой эффективности системы, предотвращения потенциально чрезмерных задержек, что появляются если начать работать и иметь большую потребность в ресурсах.

Этот алгоритм работает с большим количеством задач, потому ему необходимо большое количество рессусов. В то же время BACKFILL алгоритм может работать в параллельном режиме.

**Tivoli Workload**

Решение IBM Tivoli Workload Scheduler предназначено для автоматизации, отслеживания и управления потоком операций во всей инфраструктуре ИТ предприятия. Этот лучший на рынке инструмент автоматизации выполнения программ способен управлять сотнями тысяч рабочих нагрузок в день из единой точки управления. Приводя ИТ-инфраструктуру в соответствие с задачами компании, он помогает повысить производительность и снизить затраты.

Tivoli Workload Scheduler помогает создать среду автоматизации рабочих нагрузок предприятия, организуя работу с составными рабочими нагрузками в соответствии с бизнес-политиками.

**Алгоритм планирования в Cloud системе A\***

A\* - [алгоритм](http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC) поиска [по первому наилучшему совпадению](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B8%D1%81%D0%BA_%D0%BF%D0%BE_%D0%BF%D0%B5%D1%80%D0%B2%D0%BE%D0%BC%D1%83_%D0%BD%D0%B0%D0%B8%D0%BB%D1%83%D1%87%D1%88%D0%B5%D0%BC%D1%83_%D1%81%D0%BE%D0%B2%D0%BF%D0%B0%D0%B4%D0%B5%D0%BD%D0%B8%D1%8E) на [графе](http://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D1%84_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), который находит маршрут с наименьшей стоимостью от одной вершины (начальной) к другой (целевой, конечной).

Для тестирования модели Private Cloud системы используется этот алгоритм, поскольку он обеспечивает высокое качество планирования и позволяет гибко учитывать требования задач к реальному времени.

Порядок обхода вершин определяется [эвристической функцией](http://ru.wikipedia.org/wiki/%D0%AD%D0%B2%D1%80%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0) «расстояние + стоимость» (обычно обозначаемой как *f(x)*). Эта функция — сумма двух других: функций и стоимости достижения рассматриваемой вершины (*x*) изначальной (обычно обозначается как *g(x)* и может быть как эвристической, так и нет) и эвристической оценкой расстояния от рассматриваемой вершины к конечной (обозначается как *h(x)*).

Проиллюстрируем работу алгоритма A\* для задачи о назначениях. Учитывая набор из четырех задач {t0, t1, t2, t3,} и набор из трех процессоров {p0, p1, p2}, найдем результирующие поисковые деревья.

(a)

d1

d2

(b)

d4

d5

Рис. 3 (a) Граф задач, (b) Топология процессоров

Таблица 1

*Матрица стоимостей*

|  |  |  |  |
| --- | --- | --- | --- |
|  | P0 | P1 | P2 |
| T0 | c00 | c01 | c02 |
| T1 | c10 | c11 | c12 |
| T2 | c20 | c21 | c22 |
| T3 | c30 | c31 | c32 |

Узел в поисковом дереве включает в себя частичное распределение задач по процессорам, и значение f (стоимость частичного распределения). Постановка m задач на n процессоров отображается тройкой из m цифр, a0, a1, ..., аm - 1, где ai (0 ≤ i ≤ m - 1) - процессор (от 0 до n - 1) для которого алгоритм присвоил i-ю задачу, значение аi= x указывает, что i-я задача пока не назначена. Каждый уровень дерева соответствует задаче; таким образом, назначение этой задачи на процессор заменяет значение x в строке назначения некоторым номером процессора. Корневой узел включает в себя набор всех свободных задач xxxx. Далее мы рассматриваем стоимость размещения задачи t0 на p0 (0xxx), t0 на p1 (1xxx) и t0 на p2 (2xxx). Назначение t0 на p0 (0xxx) приводит к общей стоимости *f*(n) = *g*(n), в данном случае, равно c00, что является стоимостью выполнения t0 на p0. Аналогично рассчитываем затраты на назначение t0 на p1 (c01) и t0 на p2 (c02). Алгоритм добавляет эти три узла в список обработанных, а также выбирает узел с минимальной стоимостью для расширения.

Поиск продолжается до тех пор, пока процесс не выберет узел с полным назначением для расширения.

**Модифицированный алгоритм A\***

Модифицированный алгоритм A\*использует значительно меньше памяти, чем O \* и \* R и работает параллельно.

Параллельный алгоритм направлен на ускорение поиска с помощью параллельной обработки. Это делается путем деления дерево поиска среди процессорных элементов (ПЭ) как можно более равномерно и отбрасыванием несущественных узлов.

Первоначально, мы статически разделим дерево поиска в зависимости от количества ПЭ P в системе и максимального количества S наследников узла в дереве поиска. Существуют три способа начального разбиения:

* При P < S. Каждый ПЭ расширяется только начальным узлом, что порождает S новых узлы. Каждый ПЭ получает один узел, дополнительные узлы распределяются циклически (RR).

• P = S. Каждый ПЭ расширяется только начальным узлом, и каждый ПЭ получает один узел.

• P> S. Каждый ПЭ продолжает расширять узлы, начиная от начального узла (нулевое задание), пока порядковый номер узлов меньше P. Мы отсортируем список в порядке возрастания стоимости узлов. Первый узел в списке идет наПЭ1, второй узел к ПЭp, третий узел ПЭ2, четвертый узел ПЭp-1, и так далее. Дополнительные узлы распределяются циклически (RR). Хотя это распределение не гарантирует, что лучшая стоимость узла на начальных уровнях дерева приведет к лучшей стоимости узел в дальнейшем, алгоритм продолжает равномерно распределять хорошие узлы настолько равномерно, насколько возможны между всеми ПЭ.

Если поиск находит решение, алгоритм завершается.

После первоначального статического разделения, каждый ПЭ будет искать только в своем поддереве. Некоторые ПЭ могут работать схорошей части поискового пространства, в то время как другие могут расширять ненужные узлы. Чтобы избежать этого, ПЭ необходимо общаться друг с другом, поделить лучшую часть поискового пространства и избежать ненужной работы. Эта связь может быть глобальной ( ПЭ транслирует свои узлы на все другие элементы) или местной (ПЭ общается только со своими соседями).

При первоначальном разделении ,каждый ПЭ имеет один или несколько узлов в списке OPEN. ПЭ определяет своих соседей с помощью процессорной сетки и своих х и у координат, периодически выбирает соседа и посылает ему свой лучший узел. Помимо балансировки нагрузки, ПЭ также передает свое решение (когда он его находит) всем ПЭ. Это помогает избежать лишней работы для ПЭ, которые работают над плохой частью поискового пространства. После того, как ПЭ получает лучшее решение по сравнению со своим лучшим узлом, оно станавливает расширение ненужных узлов ПЭ, который находит первое решение транслирует свою стоимость на все другие элементы. После этого, ПЭ передает стоимость только в том случае, если она лучше полученных ранее.

**Модификация алгоритма для применения в Real Time системе**

Для работы в условиях реального времени алгоритм модифицирован. Каждый ресурс имеет коэффициент загрузки kload в диапазоне [0,1] – процент занятого процессорного времени. При загрузке задачи на ресурс, рассчитывается какой процент процессорного времени задача требуетk’load. Данный коэффициент вводится для того, чтобы избежать возможной перегрузки узла. Поскольку при перегрузке не гарантируется заданное время отклика системы.

Если kload+k’load>1, значит ресурс будет перегружен и не сможет соответствовать требованиям реального времени, потому загрузка этой задачи на этот ресурс невозможна. Значение функции стоимости для данного узла устанавливается в бесконечность.

Иначе коэффициент загрузки ресурса, после погружения задачи на этот ресурс, будет равен:

kload=kload+k’load

Также учитывается уровень безопасности задачи и ресурса. Если уровень безопасности ресурса выше или равен уровню безопасности задачи, значит выполнения задачи на этом ресурсе возможно, иначе ресурс для задачи не подходит и значение функции стоимости устанавливается в бесконечность. Это позволяет обеспечить требуемый уровень безопасности для задачи во время выполнения.

Таким образом модификация алгоритма планирования позволяет избежать перегрузки системы и обеспечивает требуемый уровень безопасности выполнения задач.

**Разделение данных для безопасной передачи по открытому каналу**

Для безопасной передачи данных по открытым каналам связи можно использовать разделение данных, для передачи частей по разным каналам. Для восстановления исходного сообщения, разделенного на n частей, необходимо собрать k частей. Таким образом безопасность передачи повышается.

**АлгоритмБлекли**

С помощью алгоритма Блекли можно создать (n,k)-алгоритм разделения секрета для любых n и k: для этого надо положить размерность пространства равную n, и каждому из n игроков дать одну гиперплоскость, проходящую через секретную точку. Тогда любые k из n гиперплоскостей будут однозначно пересекаться в секретной точке.

**Алгоритм Шамира**

Идея Алгоритм заключается в том, что двух точек достаточно для задания прямой, трех точек — для задания параболы, четырёх точек — для кубической параболы, и так далее. Чтобы задать многочлен степени *k* требуется *k+1* точек.

Для разделения данных таким образом, чтобы восстановление было возможно при наличии k частей, данные трансформируются в формулу многочлена степени. Восстановить этот многочлен можно по точкам. Количество же различных точек многочлена не ограничено.

Алгоритм Блекли менее эффективна, чем алгоритм Шамира: в алгоритме Шамира каждая доля такого же размера как и секрет, а в алгоритме Блекли каждая доля в k раз больше. Поэтому ми в нашей роботе используем алгоритм Шамира. Рассмотрим алгоритм Шамира детальней.

Выберем некоторое [простое число](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) p>M. Это число открыто сообщается всем участникам. Оно задаёт [конечное поле](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D0%B5%D1%87%D0%BD%D0%BE%D0%B5_%D0%BF%D0%BE%D0%BB%D0%B5) размера р. Над этим полем строится многочлен степени k-1 (то есть случайно выбираются все коэффициенты многочлена, кроме М):



В этом многочлене М — это разделяемый секрет, а остальные коэффициенты

 — некоторые случайные числа, которые уничтожаются после того, как процедура разделения секрета будет завершена.

Далее вычисляются координаты различных точек:



Номера секретов должны быть различны по модулю p.

После этого секреты вместе с их номером, числом и степенью многочлена передаются сторонам. Случайные коэффициенты удаляются. Теперь любые участники, зная координаты k различных точек многочлена, смогут восстановить многочлен и все его коэффициенты, включая последний из них — разделённый секрет.

Прямолинейное восстановление коэффициентов многочлена через решение системы уравнений заменяется на вычисление [интерполяционного многочлена Лагранжа](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%8F%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B9_%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE%D1%87%D0%BB%D0%B5%D0%BD_%D0%9B%D0%B0%D0%B3%D1%80%D0%B0%D0%BD%D0%B6%D0%B0). Формула многочлена будет выглядеть следующим образом:





Где xi, xj— координаты точек многочлена. Все операции выполняются также в конечном поле.

**Применение алгоритма Шамира в Cloud системах реального времени**

Для обеспечения безопасности доставки задач до cloud системы и доставки результатов клиенту целесообразно использовать алгоритм разделения секрета Шамира.

Для этого на клиенте устанавливаются программные средства для разделения задачи и задача отправляется по n каналам связи во входную очередь Cloud системы, где и собирается из частей.

**Моделирование системы**

Одной из важнейших характеристик моделирования, произвольной вычислительной системы, являются вычислительные ресурсы необходимые для его проведения. К наиболее существенным ресурсам следует отнести объем требуемой оперативной памяти ВС на которой производится моделирование и время, необходимое для его проведения. Если вышеназванные параметры, превышают возможности инструментальной вычислительной системы, то решение задачи моделирования невозможно, либо достигается оно за неприемлемое для пользователя время.

Основной целью проводимого вычислительного эксперимента, являются: исследование влияния многоканальности на работу Cloud. Ограниченный набор воздействий и исследуемых характеристик создает предпосылки для упрощения используемой модели, а тем самым и к уменьшению ресурсов необходимых для моделирования. При этом точность определяемых параметров ухудшается только незначительно.

Создание модели, учитывающей все свойства вычислительной системы возможно, однако ее решение требует чрезвычайно больших вычислительных ресурсов. Поэтому, с целью проведения процесса моделирования, следует применить упрощенную (приближенную) модель, сложность решения которой приемлема, а точность достаточно высока.

Для получения высокого качества моделирования, разработано программное обеспечение для моделирования в Cloud системе. Это позволяет гибко настраивать вычислительные мощности.

Для моделирования системы использовалось 100 потоков Эрланга, каждый из которых моделирует поведения пользователя. Согласно распределения потока Эрланга генерировалось поступление задач во входную очередь и параметры этих задач.

Модель Private Cloud системы состоит из 20 машин.

Снимались такие характеристики системы:

- Зависимость загрузки узла от количества задач во входной очереди;

- Зависимость времени ожидания задачи от количества задач во входной очереди

- Зависимость времени ожидания задачи от группы безопасности-приоритета пользователя;

- Зависимость длины входной очереди от времени.

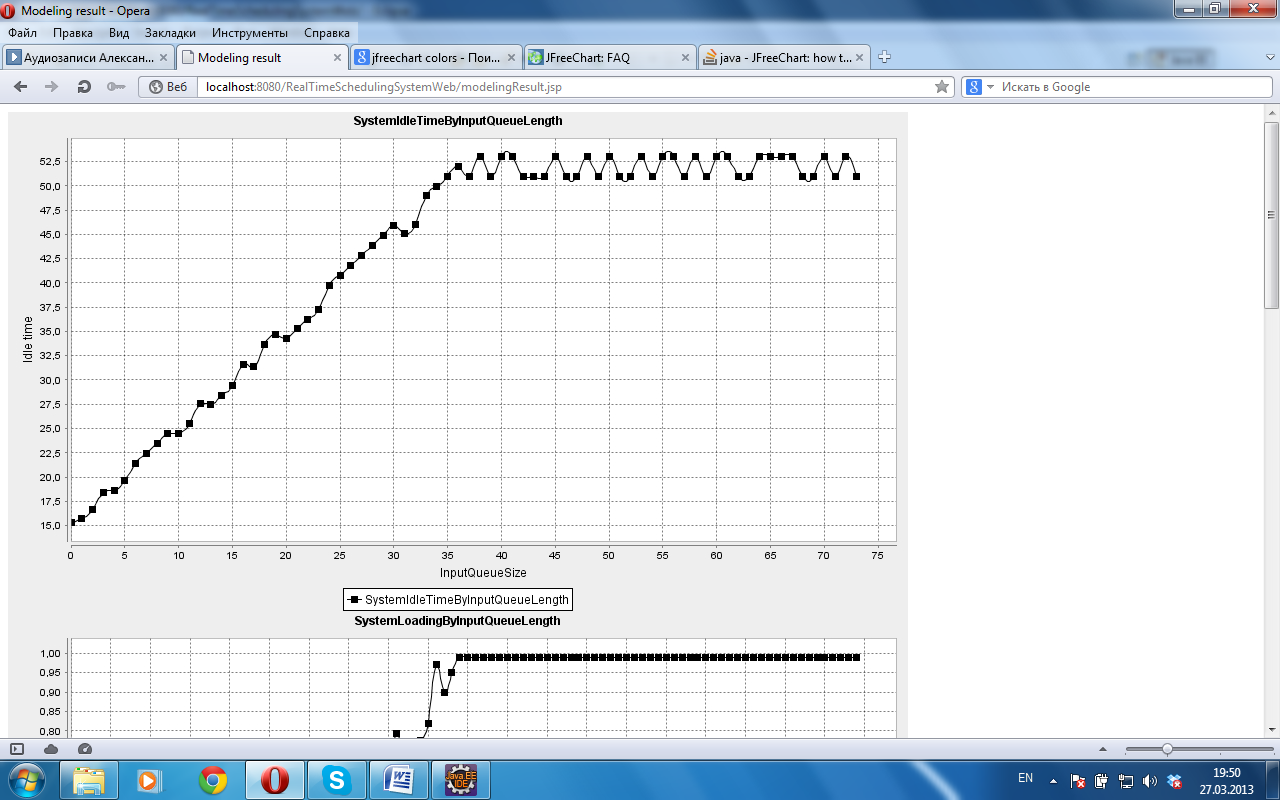
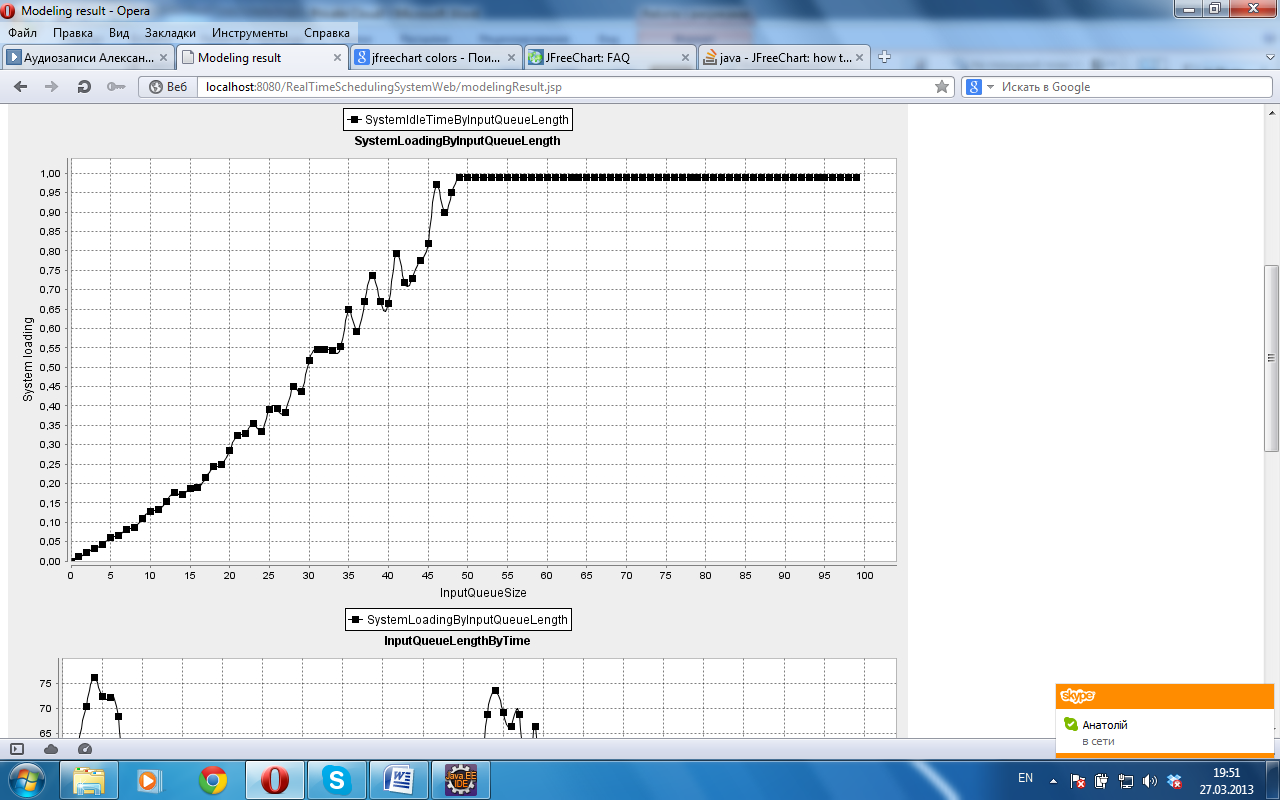


Рис. 4 График зависимости ожидания завершения выполнения задачи от длинны входной очереди

Как видно из рисунка 4, время ожидании задачи растет вместе с ростом длины входной очереди, это объясняется тем, что увеличивается время простоя в входной очереди и большей загрузкой узлов. При достижении полной загрузки, система отбрасывает новые входящие задачи, поскольку при приеме большего количества задач, система не сможет удовлетворять требованиям систем реального времени.

Минимальное время ожидания, равно времени выполнения задачи.

  
Рис. 5 График зависимости загрузки системы от длинны входной очереди

На рисунке 5 видно, что при увеличении количества задач во входной очереди, загрузка системы растет и когда наступает 100 процентная загрузка, задачи в систему не поступают. За счет отброса задач при достижении системы пиковой нагрузки, обеспечиваются требования реального времени.

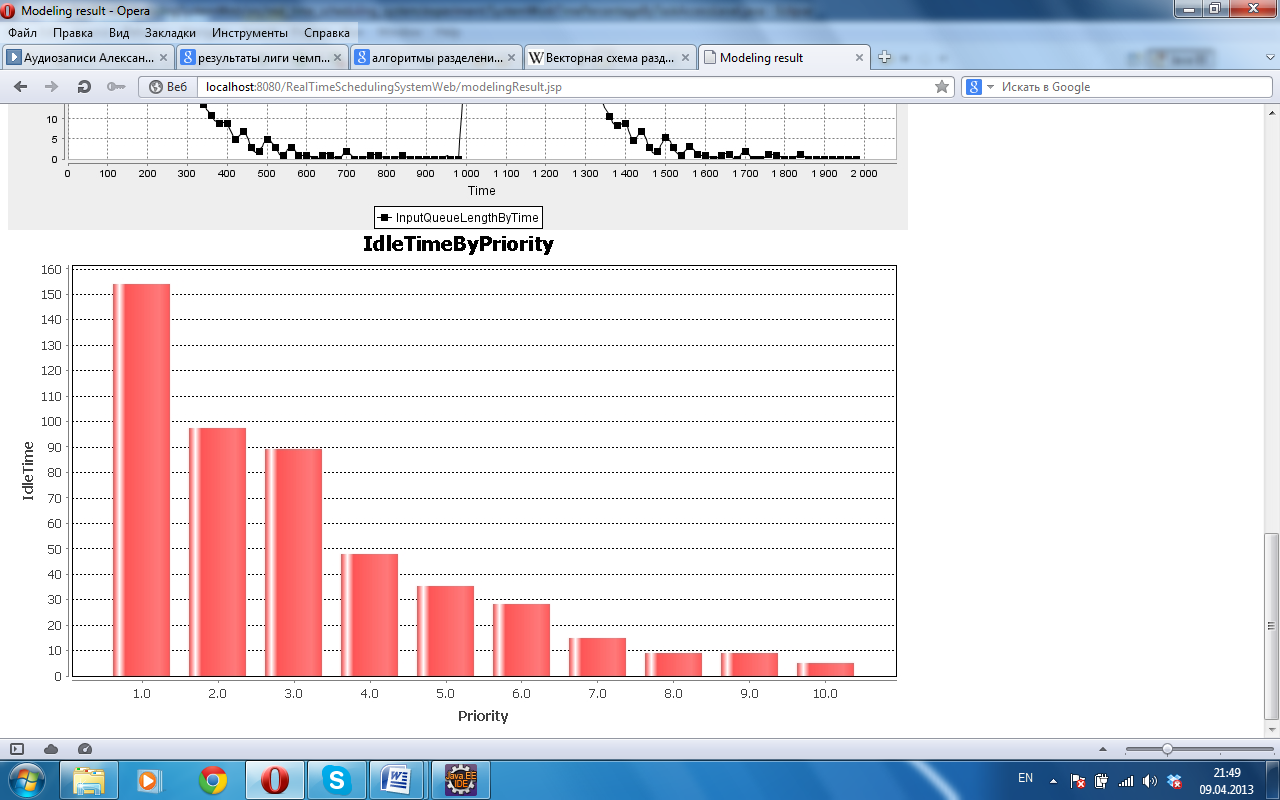
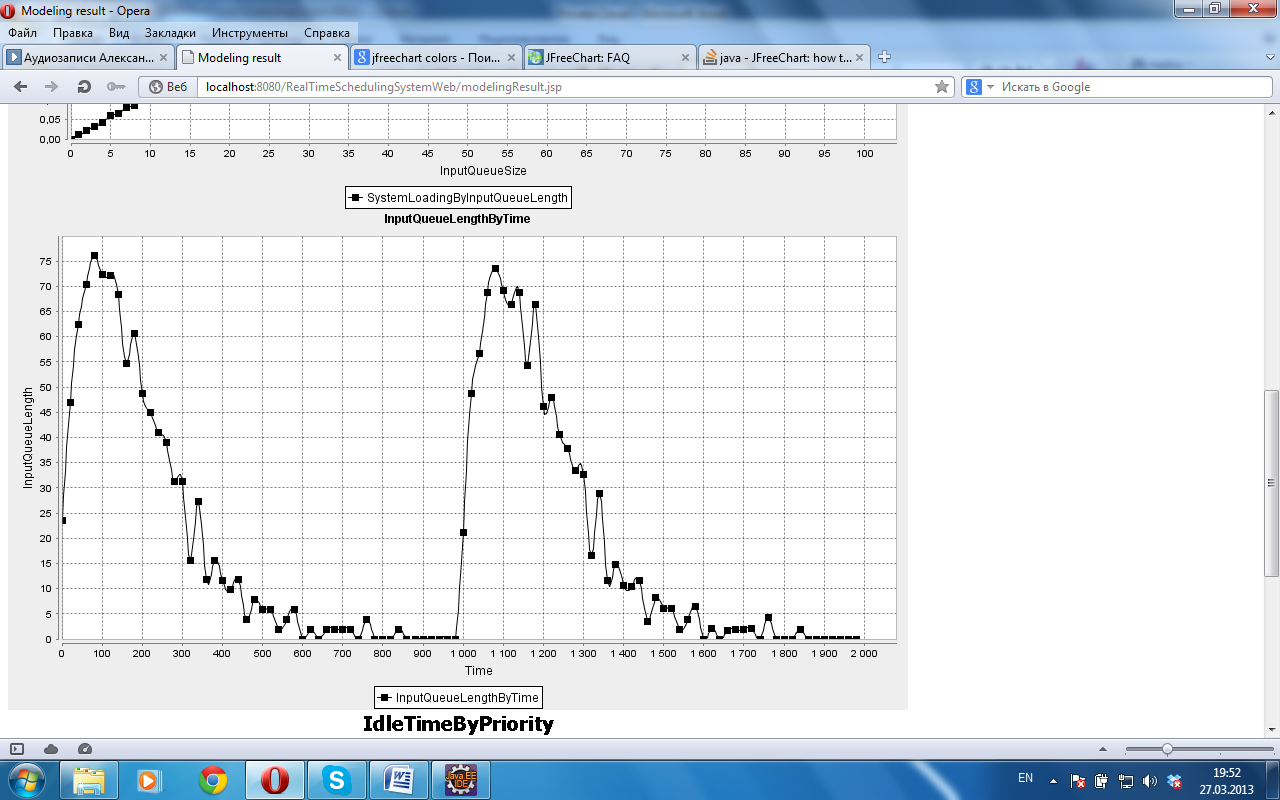


Рис. 6 График зависимости времени ожидания задачи от уровня приоритета задачи

Из графика 6 видно, что задачи с более высоким приоритетом проводят времени в ожидании меньше чем задачи с низким приоритетом. Чем выше загрузка системы, тем выше время ожидания для низкоприоритетных задач.



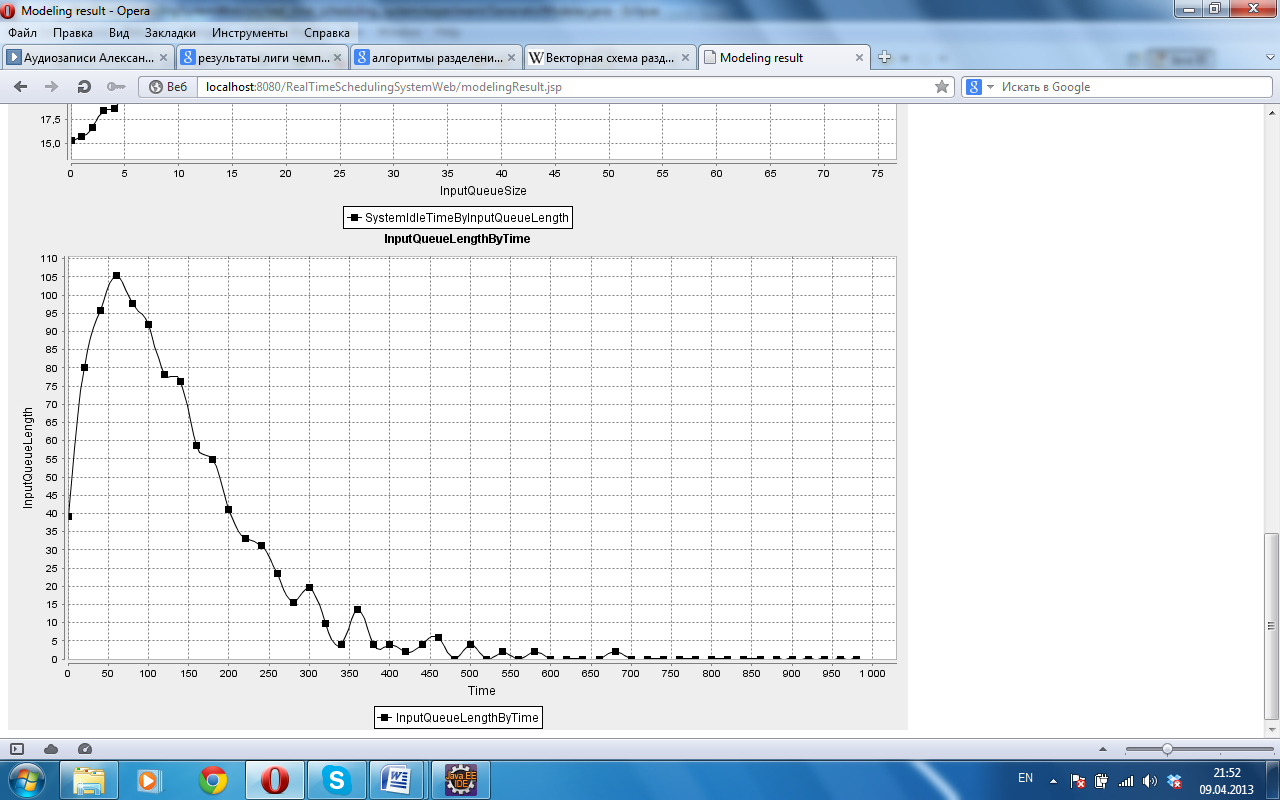


Рис. 7 График зависимости длины входной очереди от времени

Моделирование входного потока заявок проводилось сложением 100 потоков Эрланга, на выходе получается поток Эрланга, поскольку в обращении клиентов наблюдается периодичность, моделирование входной очереди также проводится с периодом.

Созданная модель Private Cloud системы реального времени доступна по адресу <http://rtss.elasticbeanstalk.com>. Выполнение моделирования в Cloud системе позволяет справляться с высокими требованиями к вычислительным ресурсам и динамической нагрузкой.

**Выводы.** Был рассмотрен алгоритм планирования выполнения задач в cloud системе A\*, адаптирован и модифицирован для работы в Cloud системе реального времени. Модуль, использующий этот алгоритм, выполняет функции распределения задач и балансировки нагрузки. Алгоритм позволяет задавать уровень безопасности и задача будет выполнятся только на машинах, которые имеют уровень безопасности не ниже указанного. Это позволяет обезопасить данные в момент выполнения задачи.

Для обеспечения необходимого уровня безопасности при передаче от клиента в систему и назад, использован алгоритм разделения секрета Shamir. Если пользователь требует уровень безопасности выше минимального, то задача и данные разделяются на части и передаются в Cloud систему по отдельным каналам, где собираются обратно. Это позволяет повысить уровень безопасности при передаче.

**Список литературы:**

1.National Institute of Standards and Technology<http://www.nist.gov/index.html>

2.[Smart Computing in Real Time](http://real-timecloud.com/2013/01/17/smart-computing-in-real-time/) <http://www.real-timecloud.com>

3.CloudComputingJournal <http://cloudcomputing.sys-con.com/>

4.Heinrich-Hertz-Institut <http://www.hhi.fraunhofer.de>

5.Optimal Task Assignment in Heterogeneous Distributed Computing Systems - Muhammad Kafil and Ishfaq Ahmad, The Hong Kong University of Science and Technology

6. Shamir, Adi (1979), "How to share a secret", Communications of the ACM