Краевая научно-практическая конференция
учебно-исследовательских работ учащихся 6-11 классов
«Прикладные и фундаментальные вопросы математики»

Математическое моделирование

# Математическая модель распространения сетевых червей

Ефимова Екатерина Ильинична,
11 кл., МБОУ «Лицей №1», г. Пермь,
Никитюк Александр Сергеевич,
учитель информатики.

Пермь. 2015.

# Оглавление

## Введение

Сетевые черви (другое название – компьютерные черви) – это программы, которые созданы с внутренним механизмом распространения по локальным и глобальным компьютерным сетям.

В нашем обществе почти у каждого человека есть свой компьютер, в котором может храниться важная информация. Атаки сетевых червей - это угроза сетевой безопасности. Данный вид программного обеспечения наносит сильный финансовый ущерб, а также является причиной других опасных угроз, среди которых несанкционированный доступ к данным, кража конфиденциальной и личной информации. Имеющиеся средства защиты не всегда своевременно справляются с эпидемиями сетевых червей, поэтому создания систем обнаружения и защиты нового поколения является актуальной задачей, способной предотвратить или сдержать эпидемию на ранних стадиях. Для достижения поставленной цели необходимо уметь моделировать эпидемии сетевых червей с целью детального исследования этого явления, анализа факторов, влияющих на распространение сетевых червей, и определения возможных механизмов обнаружения и противодействия.

Целью исследовательской работы является создание и исследование математической модели процесса распространения сетевых червей в компьютерных сетях.

Для достижения цели необходимо решить следующие задачи:
Ознакомиться с дополнительной информацией:
- что такое хост(узел);
- что такое вирусы, а именно сетевые черви;
- какие бывают виды вирусов;
- как они распространяются;
- как их активировать;
- познакомиться с методом Брутфорса.

Разработать математическую модель процесса распространения сетевых червей в компьютерных сетях.
Выбрать метод решения задачи.
Анализ и проверка корректности модели.
Проверить адекватность модели.
Исследовать динамику распространения сетевых червей в компьютерных сетях.

## Обзор литературы

Червь (сетевой червь) — тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.

Так же как для вирусов, жизненный цикл червей можно разделить на определенные стадии:

1.Проникновение в систему

2.Активация

3.Поиск "жертв"

4.Подготовка копий

5.Распространение копий

Стадии 1 и 5 симметричны и характеризуются в первую очередь используемыми протоколами и приложениями. Стадия 4 практически ничем не отличается от аналогичной стадии в процессе размножения вирусов. Сказанное о подготовке копий вирусов без изменений применимо и к червям. [5].

На этапе проникновения (распространение) в систему черви делятся преимущественно по типам используемых протоколов:

Сетевые черви — черви, использующие для распространения протоколы Интернет и локальных сетей. Обычно этот тип червей распространяется с использованием неправильной обработки некоторыми приложениями базовых пакетов стека протоколов tcp/ip. [2]. Данный вид компьютерных вредителей делится на следующие классы:

• Email-Worm — почтовые черви

Само название данного типа червей уже говорит о том, что эти вредители распространяются по средствам электронной почты. При этом червь отсылает либо свою копию, которую вкладывает в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе. В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором — при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков — активизируется код червя, и Ваш компьютер подвергается заражению.

Почтовые черви довольно «хитрые» создания и для того, что бы заразить как можно больше компьютеров применят следующие методы:

- ✓ рассылают себя по всем адресам, обнаруженным в адресной книге MS Outlook;
- ✓ считывает адреса из адресной базы WAB;
- ✓ сканируют «подходящие» файлы на диске и выделяет в них строки, являющиеся адресами электронной почты;
- ✓ отсылают себя по всем адресам, обнаруженным в письмах в почтовом ящике (при этом некоторые почтовые черви «отвечают» на обнаруженные в ящике письма).

• IM-Worm —черви, использующие для распространения системы мгновенного обмена сообщениями.

Известные компьютерные черви этого типа используют единственный способ распространения — рассылку на обнаруженные контакты сообщений, содержащих URL на файл, расположенный на каком-либо веб-сервере. Данный прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями.

• IRC-Worm — черви в IRC-каналах

У данного типа червей, как и у почтовых червей, существуют два способа распространения по IRC-каналам, повторяющие способы, описанные выше. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ — отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение). После чего и начинаются проблемы с компьютером

• Net-Worm — прочие сетевые черви.

- ✓ существуют прочие способы заражения удаленных компьютеров, например:
- ✓ копирование червя на сетевые ресурсы;
- ✓ проникновение червя на компьютер через уязвимости в операционных системах и приложениях;
- ✓ проникновение в сетевые ресурсы публичного использования;
- ✓ паразитирование на других вредоносных программах.

• P2P-Worm — черви для файлообменных сетей.

Механизм работы большинства подобных червей достаточно прост — для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-сеть берет на себя — при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера.

Еще один вид ПО – это троянские программы.

Первоначальное распространение «троянец» получил благодаря обыкновенной спам-рассылке, которая в последнее время все чаще используется вирусописателями для запуска во всемирную сеть своих вредоносных творений.

Опасность для пользователей представляют «троянцы», устанавливающие на зараженном компьютере прокси-серверы – специальные программы, при помощи которых злоумышленники могут рассылать спам и любые другие данные. Эти «троянцы» и сами распространяются по Интернет благодаря массовой почтовой рассылке. Если пользователь запускает зараженный файл, «троянец» незаметно загружает с удаленного Web-сервера дополнительные компоненты и устанавливает их на компьютере, чтобы потом использовать для ретрансляции спама. В качестве побочных действий он также пересылает своему «хозяину» список обнаруженных в кэш-памяти паролей.

На этапе активации черви делятся на две большие группы, отличающиеся как по технологиям, так и по срокам жизни:

1. Для активации необходимо активное участие пользователя
2. Для активации участие пользователя не требуется вовсе либо достаточно лишь пассивного участия. (Под пассивным участием - просмотр писем в почтовом клиенте, при котором пользователь не открывает вложенные файлы, но его компьютер, тем не менее, оказывается зараженным.)

Отличие в этих подходах глубже, чем может показаться на первый взгляд. Активация сетевого червя без участия пользователя всегда означает, что червь использует бреши в безопасности программного обеспечении компьютера. Это приводит к очень быстрому распространению червя внутри корпоративной сети с большим числом станций, существенно увеличивает загрузку каналов связи и может полностью парализовать сеть. Именно этот метод активации использовали черви Lovesan и Sasser. В результате вызванной таким сетевым червем эпидемии, используемая брешь закрывается администраторами либо пользователями, и по мере уменьшения компьютеров с открытой брешью эпидемия завершается. Для повторения эпидемии разработчикам вирусов приходится эксплуатировать другую брешь. В итоге, эпидемии, вызванные активными червями, существеннее влияют на работу сети в целом, однако случаются значительно реже, чем эпидемии пассивных сетевых червей. Обязательной мерой защиты от таких эпидемий является своевременная установка заплат безопасности. Отметим также, что особенно уязвимыми для этого типа червей являются операционные системы с заложенными возможностями удаленного управления или запуска программ - это семейство Microsoft Windows NT/2000/XP/2003.

Поиск "жертв" Способ поиска компьютера-жертвы полностью базируется на используемых протоколах и приложениях.

Подготовка копий для распространения. Наиболее часто среди червей встречаются упрощенные реализации метаморфизма. Некоторые черви способны рассылать свои копии в письмах, как с внедрением скрипта приводящего к автоматической активации червя, так и без внедрения. Такое поведение червя обусловлено двумя факторами: скрипт автоматической активации повышает вероятность запуска червя на компьютере пользователя, но при этом уменьшает вероятность проскочить антивирусные фильтры на почтовых серверах. Аналогично, черви могут менять тему и текст инфицированного сообщения, имя, расширение и даже формат вложенного файла - исполняемый модуль может быть приложен как есть или в заархивированном виде. Все это нельзя считать мета- или полиморфизмом, но определенной долей изменчивости черви, безусловно, обладают. [5].

Брутфорс (brute force) - полный перебор (или метод «грубой силы» от англ. brute force) -метод поиска и взлома пароля путем перебора всех теоретически возможных вариантов. Позволяет перебрать все возможные пароли, составленные из определенного набора символов.

Также к этому типу взлома относится атака по словарю. В этом случае перебор происходит по набору хорошо известных распространенных паролей.

Большинство встречающихся в литературе моделей распространения червей представляют собой, так называемые *детерминированные модели эпидемий.*

Они пригодны для моделирования эпидемии в той фазе, когда число инфицированных хостов достигло больших значений.

В работе будет рассматриваться несколько различных моделей, описывающих динамику распространения сетевых червей:

- SIS-модель (простая эпидемическая модель, или “Susceptible–Infected–Susceptible model”);
- SIR-модель (“Susceptible–Infected–Removed model”);
- SEIR-модель (“Susceptible–Exposed–Infected–Removed model”);
- SAIR-модель (“Susceptible–Antidotal–Infected–Removed model”);
- PSIDR-модель (“Progressive Susceptible–Infected–Detected–Removed model”).

## Математическая модель распространения сетевых червей

### Содержательная постановка

Для того, чтобы достигнуть поставленную цель необходимо разработать математическую модель рассматриваемого в работе процесса. На первом этапе разработки математической модели необходимо выполнить содержательную постановку задачи. На основе проведенного обзора литературы постановка выглядит следующим образом.

*Модель должна позволять:*

- описывать динамику доли инфицированных узлов сети.

*Исходные данные модели:*

- количество узлов компьютерной сети;
- размер адресного пространства сети;
- начальная зараженность сети;
- средняя скорость сканирования червем сети.

### Концептуальная постановка

Определить закон изменения количества инфицированных узлов сети I, если известны скорость сканирования червем сети $\beta$ и начальное количество неинфицированных хостов S.

Объектом исследования является компьютерная сеть. Предметная область - информатика.

Хост - основной узловой компьютер или любое устройство, подключенное к сети и использующее протоколы TCP/IP. Другими словами, хост - это информационный узел сети, который не передаёт информацию из одной сети в другую. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый к локальной или глобальной сети. [1].

Любой узел может находиться в двух состояниях: инфицированный и неинфицированный.

На одном зараженном хосте может существовать только одна копия.

Копия выбирает в доступном адресном пространстве потенциальную жертву со средней скоростью - $\beta$ (хостов в секунду);

## Математическая постановка

β - хосты в секунду;

t - время (в секундах);

I - количество инфицированных;

S - количество неинфицированных;

N – количество хостов в сети;

Vs - скорость сканирования червями сети;

Nip – размер адресного пространства;

i – вводятся для описания динамики доли инфицированных хостов в конкретный период времени;

s – вводятся для описания динамики доли неинфицированных хостов в конкретный период времени;

Vi – скорость изменения доли инфицированных хостов во времени.

$$t = \frac{1}{\beta} \tag{1}$$

Расчета времени распространения сетевого червя.

$$\beta = Vs * \frac{N}{Nip} \tag{2}$$

β - средняя постоянная скорость.

Что бы узнать количество хостов в сети, где I - количество инфицированных; S-количество неинфицированных.

$$I + S = N \tag{3}$$

Для описания динамики доли инфицированных и неинфицированных хостов в конкретный период времени:

$$i = \frac{I}{N} \tag{4}$$

$$s = \frac{S}{N} \tag{5}$$

Динамика распространения рассчитывается

$$\frac{di}{dt} = \beta * (1 - i) * i \tag{6}$$

Формула задающая начальное условие:

$$i(t_0) = i_0 \tag{7}$$

## Метод решения

Для решения дифференциального уравнения (6) с начальными условиями (7) использовался метод Эйлера. Данный метод — простейший численный метод решения систем обыкновенных дифференциальных уравнений. Впервые описан в 1768 году Леонардом Эйлером в работе «Интегральное исчисление». Метод Эйлера является явным, одношаговым методом первого порядка точности, основанном на аппроксимации интегральной кривой кусочно-линейной функцией, так называемой ломаной Эйлера.

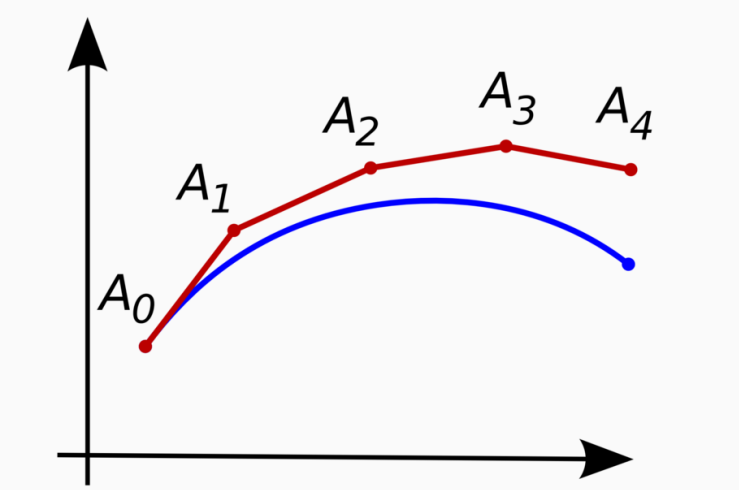



Рис. 1. Ломаная Эйлера (красная линия) — приближённое решение в пяти узлах задачи Коши и точное решение этой задачи (выделено синим цветом).

Решение сводится к интегрированию обыкновенного дифференциального уравнения первого порядка:

$$\frac{dy}{dx} = f(x,y), \text{ или } y' = f(x,y)$$

Функция y=y(x), удовлетворяющая этому уравнению, то есть такая, что $y'(x) \equiv f(x,y(x))$ на некотором участке изменения аргумента x называется дифференцируемая.

Рассмотрим задачу Коши, когда для искомой функции задается условие для одного из значений аргумента, принимаемого за начальное, $y(x_0) = y_0$ ;

Пусть для отрезка [a, b], на котором ищется решение дифференциального уравнения (2.1), построена сеточная область $\Omega_n = \{a = x_0 < x_1 < K < x_n = b\}$ с постоянным шагом h. Для построения решения уравнения (2.1) воспользуемся разложением искомой функции y(x) в ряд Тэйлора вблизи произвольной точки $x_k \in \Omega_n$ :

$$y(x_{k+1}) = y(x_k) + y'(x_k) \cdot h + K$$

Учитывая, что согласно уравнению (2.1) $y'(x_k) = f(x_k, y(x_k))$, это разложение решения можно записать в виде

$$y(x_{k+1}) = y(x_k) + f(x_k, y(x_k)) \cdot h + K$$

С помощью полученного выражения построим вычислительный процесс

$$y_{k+1} = y_k + f(x_k, y_k) \cdot h, \quad k = 1,2,K, \quad y_0 = y(0).$$

Здесь и далее будем обозначать символами $y_k$ результат численного решения уравнения (2.1), а выражение $y(x_k)$ будем использовать для обозначения точного решения исходной задачи.

## Результаты

Решение дифференциального уравнения (6) с начальными условиями (7) использовался метод Эйлера. Исходные данные: n=100, a=0, b=1 (n-количество отрезков разбитых на промежутке от a до b), t0=0, i0=0.5, Vs=1, N= 2^10, Nip=2^23. Графики построены i(t).

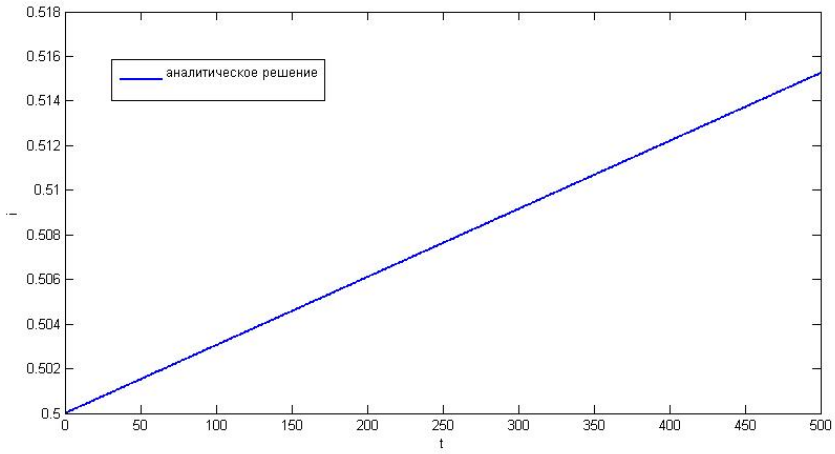



Рис. 2. График 1 описывающий эволюцию доли инфецированных хостов в зависимости от времени. Изображена линейная функция, полученная в результате аналитического решения уравнения

$$i(t) = \frac{1}{1 + \left(\frac{1}{i_0} - 1\right) * \exp(-\beta * t)}$$

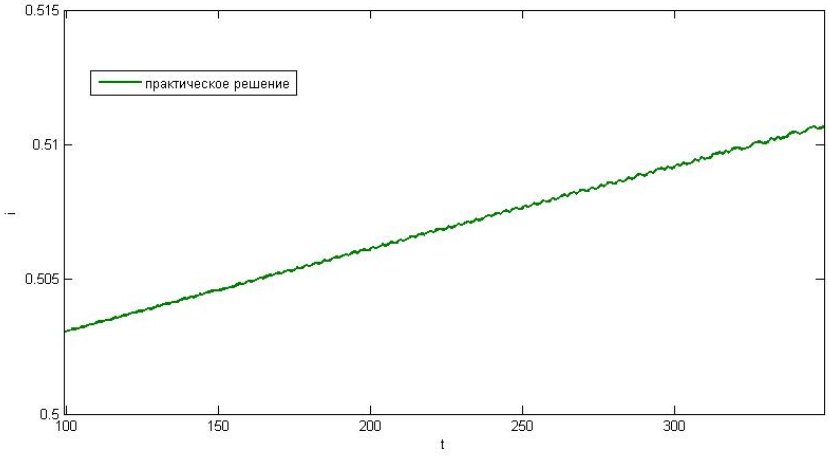
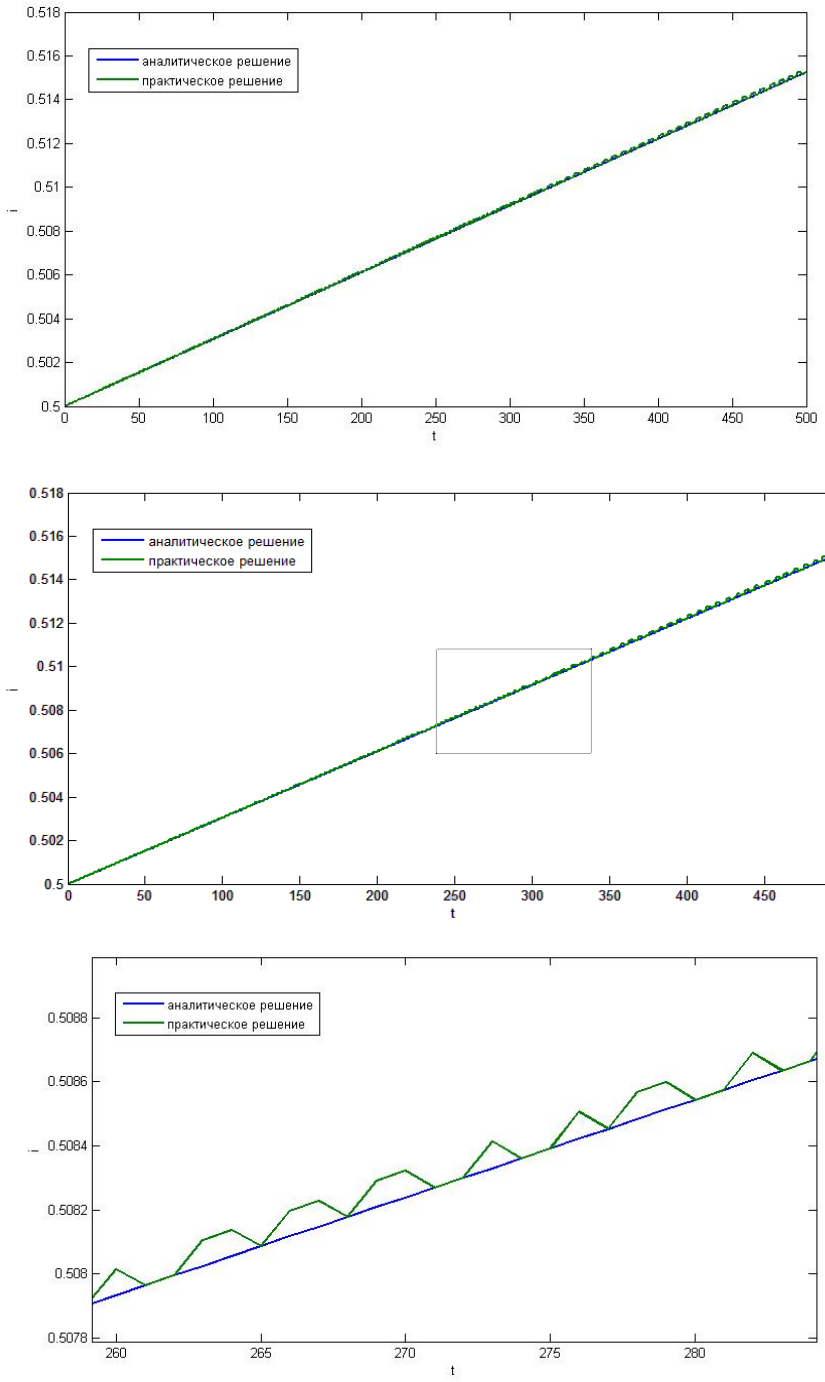



Рис. 3.

Рис. 3. График 2 описывающий эволюцию доли инфецированных хостов в зависимости от времени. Изображена линейная функция, полученная в результате численного решения уравнения методом Эйлера**.**

$$\frac{di}{dt} = \beta * (1 - i) * i$$

Наложим график 1 на график 2.



Проанализируем два графика при его увиличение, можно сказать что аналитическая формула дает более точный результат, нежели практическое решиение дифференциального уравнения при заначениях t от 1 до 500.

## Заключение.

В данной работе рассмотрена задача о распространение сетевых червей. Разработана математическая модель процесса распространения сетевых червей в компьютерных сетях. Уравнения решены методом Эйлера. Математическая модель проверена на корректность. Проведен анализ результатов, вследствие которого установлено, что аналитическая формула дает более точные результаты, нежели практическое решение.

## Список литературы


1. [Электронный ресурс]. – URL : http://www.arisfera.ru/glossary/web/Hosts.html (дата обращения: 29.05.2015г.).
2. [Электронный ресурс]. – URL : http://thelocalhost.ru/setevye-chervi/ (дата обращения: 29.05.2015г.).
3. Официальный сайт Википедия — свободная энциклопедия [Электронный ресурс]. – URL : https://ru.wikipedia.org/wiki/Сетевой_червь (дата обращения: 3.06.2015г.).
4. Владимир Дронов PHP 5/6, MySQL 5/6 и Dreamweaver CS4 Разработка интерактивных Web-сайтов (дата обращения: 7.06.2015г.).
5. Официальный сайт Северный филиал МГУТУ (ранее СФ РГУИТП) [Электронный ресурс]. – URL : http://www.in-nov.ru/node/895 (дата обращения: 3.09.2015г.).
6. Официальный сайт Википедия — свободная энциклопедия [Электронный ресурс]. – URL : https://ru.wikipedia.org/wiki/Метод_Эйлера (дата обращения: 11.09.2015г.).
7. В.Г.Потемкин "Справочник по MATLAB" . Графические команды и функции [Электронный ресурс]. – URL : http://matlab.exponenta.ru/ml/book2/chapter10/contens.php (дата обращения: 8.10.2015г.).
8. Котенко И. В., Воронцов В. В. "Аналитические модели распространения сетевых червей" Санкт Петербург институт информатики и автоматизации РАН. Наука, 2007.
9. [Электронный ресурс]. – URL : http://pw-nakama.clan.su/forum/17-136-1 (дата обращения: 15.06.2015г.).