УДК 004.10:519.872

# НАХОЖДЕНИЕ ОЖИДАЕМЫХ ДОХОДОВ СИСТЕМ В G-СЕТИ С КОНТРОЛЬНОЙ И КАРАНТИННОЙ ОЧЕРЕДЯМИ И ПЕРЕМЕЩЕНИЯМИ ОТРИЦАТЕЛЬНЫХ ЗАЯВОК МЕЖДУ СИСТЕМАМИ СЕТИ

***канд. физ.-мат. наук Д. Я. КОПАТЬ***
***(Гродненский государственный университет им. Янки Купалы, Беларусь)***

***Аннотация.*** *Объектом исследования в данной статье является компьютерная сеть (КС) с установленным антивирусным программным обеспечением (ПО) в каждом компьютере сети. Данная КС исследуется с помощью её математической модели – G-сети с системами с контрольными и карантинными очередями и перемещением отрицательных заявок между системами сети. Целью исследования является нахождение зависящих от времени ожидаемых доходов систем сети.*

***Ключевые слова:*** *ожидаемые доходы; антивирусное программное обеспечение; компьютерная сеть; G-сеть; среднее число заявок в системах сети.*

**Введение.** До сих пор разрабатывались математические модели компьютерных систем, которые учитывали попадание в них компьютерных вирусов. Первая из моделей поведения информационных систем и сетей (ИСС) с учетом попадания в них компьютерных вирусов в стационарном режиме была исследована в статье [1]. Моделирование текущего поведения G-сетей с течением времени исследовалось в статье [2] в том числе и ожидаемых доходов [3]. Однако в современных ИСС установлено антивирусное ПО, которое позволяет уменьшить величину убытка от действия компьютерных вирусов. Как известно авторам статьи, несмотря на то, что первые антивирусные программы на территории бывшего СССР появились в конце 80-х годов XX [4], однако математические модели компьютерных антивирусов без учета поведения вирусов с помощью сетей массового обслуживания (СеМО) были исследованы только в статье [5] в 2017 году. В статье [6] была предложена данная модель в сохранении преемственности в поведении отрицательной заявки с работами Gelenbe: после уничтожения одной положительной заявки отрицательная заявка покидала сеть, а в работе [7]. Данная статья предлагает модель, отличающаяся от статьи [6] тем, что мы предлагаем новое поведение отрицательных заявок: после уничтожения положительной заявки она может перемещаться по системам сети до обнаружения антивирусным ПО.

**1. Описание стохастической модели КС с антивирусным ПО.** Рассмотрим стохастическую модель КС с антивирусным ПО. Она представляет собой G-сеть, состоящую из $n$ систем массового обслуживания (СМО) $S_i, i=\overline{1,n}$, в каждую из которых поступают простейшие потоки положительных заявок и отрицательных заявок с интенсивностями $\lambda_{0i}^{+}, \lambda_{0i}^{-}, i=\overline{1,n}$, соответственно. Для компьютерной сети $\lambda_{0i}^{+}, \lambda_{0i}^{-}$ понимаются соответственно как количество неопасных для ПК и представляющих для него угрозу файлов, пришедших в RAM компьютера из его жесткого диска или из-за пределов КС в единицу времени.

Перед поступлением на обслуживание заявка, поступившая в $i$-ю СМО, становится в контрольную очередь для проверки на стандартность, что соответствует проверке файла на наличие вируса. После завершения ожидания заявки в очереди, заявка проверяется на стандартность в течении времени, имеющего экспоненциальное распределение (ф.р.) с параметром $\mu_i^{(v)}, i=\overline{1,n}$. Под контрольной очередью будем понимать место RAM, отведенное для антивирусного ПО. По результатам проверки на стандартность в контрольной очереди i-й СМО положительная заявка признается таковой с вероятностью $p_i^{+}$ и переходит в очередь этой системы для обработки, а с вероятностью $1-p_i^{+}$ будет признана отрицательной и отправится в карантин на лечение. С вероятностью $p_i^{-}$ отрицательная заявка после проверки на стандартность в контрольной очереди i-й СМО признается таковой и переходит в карантинную очередь на лечение; с вероятностью $1-p_i^{-}$ отрицательная заявка может ошибочно быть признана положительной, например, из-за не обновления антивирусных БД, и поступит в очередь $i$-й СМО на обработку, где она немедленно уничтожает положительную заявку, при их наличии, а затем с вероятностью $n_{ij}$ переходит в контрольную очередь $j$-й СМО или с вероятностью $n_{i0}$ уходит из сети.

Успешно прошедшая проверку на стандартность в $i$-й СМО положительная заявка, после завершения ожидания в очереди на обслуживание, обрабатывается линией обслуживания в течении времени имеющего экспоненциальную ф.р. с параметром $\mu_i$, $i=\overline{1, n}$, после чего с вероятностью $p_{ij}^{+}$ переходит в контрольную очередь системы в $j$-й СМО как положительная заявка, с вероятностью $p_{ij}^{-}$ – как отрицательная заявка и с вероятностью $p_{i0}=1-\sum_{j=1}^{n}\left(p_{ij}^{+}+p_{ij}^{-}\right)$ покидает сеть, $i, j=\overline{1, n}$.

Заявки, признанные отрицательными, становятся в очередь на лечение в карантине, которая физически представляет собой папку файлов, помещенных в карантин. Предположим, что длительность лечения заявки в карантине $i$-й СМО – это СВ с экспоненциальной ф.р. с параметром $\mu_i^{(c)}, i=\overline{1,n}$. При лечении файл достаётся из папки по дисциплине FIFO. Определим вероятность $p_i^{(s)}, i=\overline{1,n}$, что заявка в карантине будет вылечена, после чего она направляется на обслуживание в очередь $i$-й СМО. Тогда с вероятностью $1-p_i^{(s)}$ заявка из карантина удаляется из сети.

Состояние описанной сети определяется вектором

$$\left(\vec{k},\vec{l},t\right)=\left(\vec{k}_1,\vec{k}_2,...,\vec{k}_n,\vec{l}_1,\vec{l}_2,...,\vec{l}_n;t\right), \tag{1}$$

где $\vec{k}_i=\left(k_i^{(p)},k_i^{(s)}\right)$, $\vec{l}_i=\left(l_i^{(n)},l_i^{(c)}\right)$, $k_i^{(p)},k_i^{(s)}$ – это число положительных заявок в контрольной очереди и на обслуживании $i$-й СМО соответственно;

$l_i^{(n)},l_i^{(c)}$ – число отрицательных заявок в контрольной очереди $i$-й СМО и карантине $i$-й СМО соответственно, т. е. вектор состояния сети имеет размерность $2n$.

Пусть заявки выбираются на проверку на стандартность из очереди случайным образом, т. е. вероятность проверки на стандартность положительной заявки аппроксимируется выражением

$$q_i^+=\left(\lambda_{0i}^+ +\sum_{j=1}^{n}\mu_j p_{ji}^+\right)\left(\lambda_{0i}^+ +\lambda_{0i}^- +\sum_{j=1}^{n}\mu_j\left(p_{ji}^+ +p_{ji}^-\right)\right)^{-1},\ i=\overline{1,n}.$$

**2. Нахождение ожидаемых доходов систем сети.** Описанная в пункте 1 СеМО может служить моделью работы антивирусного ПО, которое позволяет снизить риски, связанные с вредоносными файлами. Достоинства и недостатки данной ПО, описано в статье [4]. Рассмотрим динамику изменения доходов некоторой СМО $S_i$ сети. Воспользуемся методикой, описанной в [3]. Обозначим через $V_i(t)$ ее доход в момент времени $t$, если $V_i(0)=v_{i0}$. Доход этой СМО в момент времени $t+\Delta t$ имеет вид

$$V_i\ (t+\Delta t)=V_i(t)+\Delta V_i(t,\Delta t), \tag{2}$$

где $\Delta V_i(t,\Delta t)$ – изменение дохода системы $S_i$ на интервале времени $[t,t+\Delta t)$.

Можно показать, что $\Delta V_i\left(t,\Delta t\right)$ имеет вид

$$\Delta V_i\ (t,\Delta t)=\begin{cases}
R_{0i}^{+}-r_i\ \Delta t & \text{с вер-ю}\quad \lambda_{0i}^{+}\Delta t+o(\Delta t),\\
-R_{0i}^{-}-r_i\ \Delta t & \text{с вер-ю}\quad \left(\lambda_{0i}^{-}+\sum_{j=1}^{n}\mu_j^{(v)}(1-q_j^{+})(1-p_j^{-})n_{ji}u\left(l_j^{(n)}\right)\right)\times\\
 & \times\Delta t+o(\Delta t),\\
-r_i^{+}-r_i\ \Delta t & \text{с вер-ю}\quad \mu_i^{(v)}q_i^{+}p_i^{+}u\left(k_i^{(p)}\right)\Delta t+o(\Delta t),\\
-R_i^{+}-r_i\ \Delta t & \text{с вер-ю}\quad \mu_i^{(c)}(1-p_i^{(s)})u\left(l_i^{(c)}\right)\Delta t+o(\Delta t),\\
-L_{i0}^{+}-r_i\ \Delta t & \text{с вер-ю}\quad \mu_i^{(v)}(1-q_i^{+})(1-p_i^{-})n_{i0}u\left(l_i^{(n)}\right)\Delta t+o(\Delta t),\\
-L_{ij}^{+}-r_i\ \Delta & \text{с вер-ю}\quad \mu_i^{(v)}(1-q_i^{+})(1-p_i^{-})n_{ij}u\left(l_i^{(n)}\right)\Delta t+o(\Delta t),\\
-R_i^{c}-r_i\ \Delta t & \text{с вер-ю}\quad \mu_i^{(v)}q_i^{+}(1-p_i^{+})u\left(k_i^{(p)}\right)\Delta t+o(\Delta t),\\
r_i^{-}-r_i\ \Delta t & \text{с вер-ю}\quad \mu_i^{(v)}(1-q_i^{+})\left(p_i^{-}+(1-p_i^{-})\left(1-u\left(k_i^{(s)}\right)\right)\right)\times\\
 & \times u\left(l_i^{(n)}\right)\Delta t+o(\Delta t),\\
R_i^{+}-r_i\ \Delta t & \text{с вер-ю}\quad \mu_i^{(c)}p_i^{(s)}u\left(l_i^{(c)}\right)\Delta t+o(\Delta t),\\
R_{ji}^{+}-r_i\ \Delta t & \text{с вер-ю}\quad \sum_{j=1}^{n}\mu_j p_{ji}^{+}u\left(k_j^{(s)}\right)\Delta t+o(\Delta t),\\
-R_{ji}^{-}-r_i\ \Delta t & \text{с вер-ю}\quad \sum_{j=1}^{n}\mu_j p_{ji}^{-}u\left(k_j^{(s)}\right)\Delta t+o(\Delta t),\\
 & 1-\Big[\mu_i^{(v)}\left((1-q_i^{+})u\left(l_i^{(n)}\right)\times\right.\\
 & \times\left(\left(1+(1-p_i^{-})\left(1-u\left(k_i^{(s)}\right)\right)\right)+\mu_i^{(v)}q_i^{+}u\left(k_i^{(p)}\right)+\right.\\
-r_i\ \Delta t & \text{с вер-ю}\quad \lambda_{0i}^{+}+\lambda_{0i}^{-}+\mu_i^{(c)}u\left(l_i^{(c)}\right)+\mu_i+\\
 & +\sum_{j=1}^{n}\mu_j\left(p_{ji}^{+}+p_{ji}^{-}\right)u\left(k_j^{(s)}\right)\Big]\Delta t+o(\Delta t).
\end{cases}\qquad(3)$$

$R_{ij}^{+}, R_{ij}^{-}, R_{0i}^{+}, R_{0i}^{-},\ r_i^{+}, r_i^{+}, R_i^{c}$ – независимые СВ по отношению к $r_i$ , $i,j=\overline{1,n}$, обозначающие доход от различных переходов между состояниями сети.

При фиксированной реализации процесса $(\vec{k},\vec{l},t)$ и усреднив его с учетом условия нормировки $\sum_{k,l}P(k,l,t)=\left(k^{(p)},k^{(s)},l^{(n)},l^{(c)}\right)=1$, для изменения ожидаемого дохода СМО $S_i$ получаем, что математическое ожидание изменения дохода $i$-й СМО будет равно:

$$\mathbf{E}\left[\Delta V_i\ (t,\Delta t)\right]=\left[a_{0i}^{+}\lambda_{0i}^{+}+a_i^{+}\mu_i^{(c)}u\left(l_i^{(c)}\right)+\mu_i^{(v)}q_i^{+}\left((a_i^{c}-b_i^{+})p_i^{+}-a_i^{c}\right)u\left(k_i^{(p)}\right)-\right.$$

$$-a_{0i}^{-}\left(\lambda_{0i}^{-}+\sum_{j=1}^{n}\mu_j^{(v)}(1-q_j^{+})(1-p_j^{-})n_{ji}u\left(l_j^{(n)}\right)\right)+\mu_i^{(v)}(1-q_i^{+})u\left(l_i^{(n)}\right)\left(p_i^{-}b_i^{-}-\right.$$

$$\left.\left.-(1-p_i^{-})\left(a_{i0}^{(n)}n_{i0}+\sum_{j=1}^{n}n_{ij}a_{ij}^{(n)}\right)u\left(k_i^{(s)}\right)\right)+\sum_{j=1}^{n}\mu_j\left(a_{ji}^{+}p_{ji}^{+}-a_{ji}^{-}p_{ji}^{-}\right)u\left(k_j^{(s)}\right)-b_i\right]\Delta t+o(\Delta t).$$

Последнее выражение можно разбить на 2 частных случая: 1) когда сеть функционируем в режиме насыщения, т. е. $k_i^{(p)}(t)$, $k_i^{(s)}(t)$, $l_i^{(n)}(t)$, $l_i^{(c)}(t)$ всегда больше нуля; 2) все системы сети функционируют в режиме низкой нагрузки. Введем обозначение $v_i(t)=\mathbf{E}[V_i(t)]$, $i=\overline{1,n}$. Подставляя в (2) выражение (4) и переходя к пределу при $\Delta t\to 0$ в случае 1), получим неоднородные линейные ОДУ

$$\frac{dv_i(t)}{dt}=a_{0i}^{+}\lambda_{0i}^{+}-a_{0i}^{-}\left(\lambda_{0i}^{-}+\sum_{j=1}^{n}\mu_j^{(v)}\left(1-q_j^{+}\right)(1-p_j^{-})n_{ji}\right)+\mu_i^{(v)}q_i^{+}\left((a_i^{c}-b_i^{+})p_i^{+}-a_i^{c}\right)+a_i^{+}\mu_i^{(c)}+$$

$$+\mu_i^{(v)}\left(1-q_i^{+}\right)\left(p_i^{-}b_i^{-}-(1-p_i^{-})\left(a_{i0}^{(n)}n_{i0}+\sum_{j=1}^{n}n_{ij}a_{ij}^{(n)}\right)\right)+\sum_{j=1}^{n}\mu_j\left(a_{ji}^{+}p_{ji}^{+}-a_{ji}^{-}p_{ji}^{-}\right)-b_i,i=\overline{1,n}.$$

**Заключение.** В статье впервые представлена модель КС с антивирусным ПО. Найдены ожидаемые доходы систем КС с антивирусным ПО в виде линейной функции от времени. В случае, когда СМО сети функционируют в режиме насыщения. Дальнейшие исследования в этом направлении будут связаны с механизмами управления нагрузкой в сетях с антивирусным ПО.

## ЛИТЕРАТУРА


1. Gelenbe, E. Product form queueing networks with negative and positive customers / E. Gelenbe // Journal of Applied Probability. – 1991. – Vol. 28, No3. – P. 656–663.
2. Matalytski, M. Non-stationary analysis of queueing network with positive and negative messages / M. Matalytski, V. Naumenko // Journal of Applied Mathematics and Computational Mechanics. – 2013. – Vol. 12, № 2. – P. 61–71.
3. Науменко, В. В. Анализ сетей с положительными и отрицательными заявками в переходном режиме / В. В. Науменко, М. А. Маталыцкий // Вестник ТГУ. Серия УВТИ. – 2013. – № 4 (25). – С. 61–70.

4. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста: монография / К.Е. Климентьев. – Москва, ДМК Пресс, 2013. – 656 с.
5. Летунович, Ю.Е. Открытые марковские сети массового обслуживания с контрольными очередями и карантинным узлом /Ю.Е. Летунович, О.В. Якубович //Вестник ТГУ. Серия УВТИ. – 2017. – №. 41. – С. 32–38.
6. Kopats, D. Analysis of the Probabilistic and Cost Characteristics of the Queueing Network with
7. a Control Queue and Quarantine in Systems and Negative Requests by Means of Successive Approximation /D. Kopats, K. Kosareva // Communicaton in Computer and Information Science. Proc. 24th Intern. Conf., M., Russia, September 20-24, 2021, – P. 259–271.
8. Косарева, Е. В. Нахождение ожидаемых доходов систем в G-сети с контрольной и карантинной очередями/ Е. В. Косарева, Д. Я. Копать // Веснiк ГрДУ. Сер. 2. – 2021. – Т. 11. – № 3. – С. 115–123.