

Исследование SIR-модели динамики распространения вредоносных программ в системе AnyLogic



**Обухова Ю.М. – студентка гр. КЗИ-106
Руководитель Л.М. Груздева – ст. преподаватель
кафедры «Информатика и защита информации»
Владимирского государственного университета**

Содержание

SIR-модель

3

Постановка задачи

4

Система имитационного моделирования AnyLogic™

5

Структура имитационной модели распространения ВП

7

Эксперимент

9

Выводы

11

SIR-модель

- ❖ В исследовании динамики распространения вредоносных программ нашли широкое применение претерпевшие различные модификации эпидемиологические математические модели, представляющие собой дифференциальные уравнения и системы.
- ❖ SIR-модель учитывает процесс вывода заражённых субъектов из компьютерной системы. Она базируется на предположении, что во время эпидемии некоторое количество заражённых субъектов либо избавляется от вредоносной программы, либо перестаёт функционировать. Как только субъект избавляется от ВП, он приобретает к ней иммунитет.

Постановка задачи

Пусть каждый зараженный субъект в единицу времени заражает в среднем один из u восприимчивых субъектов. Через v единиц времени зараженный узел восстанавливается, приобретая защиту. Через t единиц времени в сети появляется новая модификация вредоносной программы и восстановленные субъекты переходят в восприимчивое состояние.

$$\begin{cases} \frac{dS(t)}{dt} = \mu R(t) - \beta S(t)J(t) \\ \frac{dJ(t)}{dt} = \beta S(t)J(t) - \gamma J(t) \\ \frac{dR(t)}{dt} = \gamma J(t) - \mu R(t) \end{cases}$$

$S(t)$ – число субъектов подверженных заражению;

$J(t)$ – число разносчиков ВП;

$R(t)$ – число восстановленных и имеющих защиту;

K – общее количество субъектов

$$\mu = \frac{1}{\tau} \quad \gamma = \frac{1}{v} \quad \beta = \frac{1}{u} \quad (K = S(t) + J(t) + R(t)).$$

Система имитационного моделирования AnyLogic™

- ❖ AnyLogic – относительно новая разработка в области имитационного моделирования.
- ❖ Уникальность AnyLogic™ состоит в его способности эффективно решать задачи моделирования любого масштаба и уровня абстракции.
- ❖ Используя различные подходы к решению поставленных задач, сочетая их со средствами анимации, оптимизируя с помощью неоднократного использования объектов, система позволяет строить гибкие, наглядно представленные модели, используя наименьшее количество ресурсов.

Возможности AnyLogic



Структура имитационной модели распространения ВП

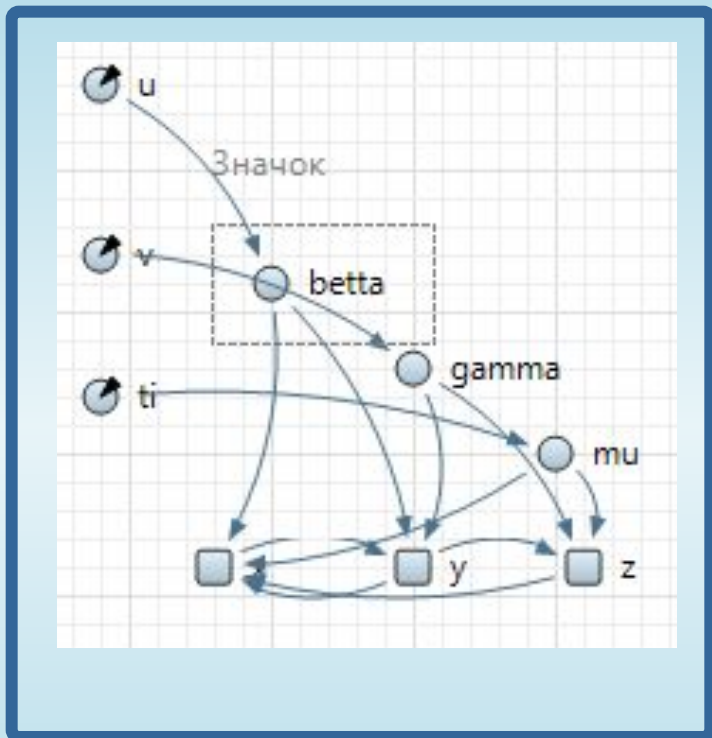


Рис. 1 – Структура SIR-модели в среде AnyLogic

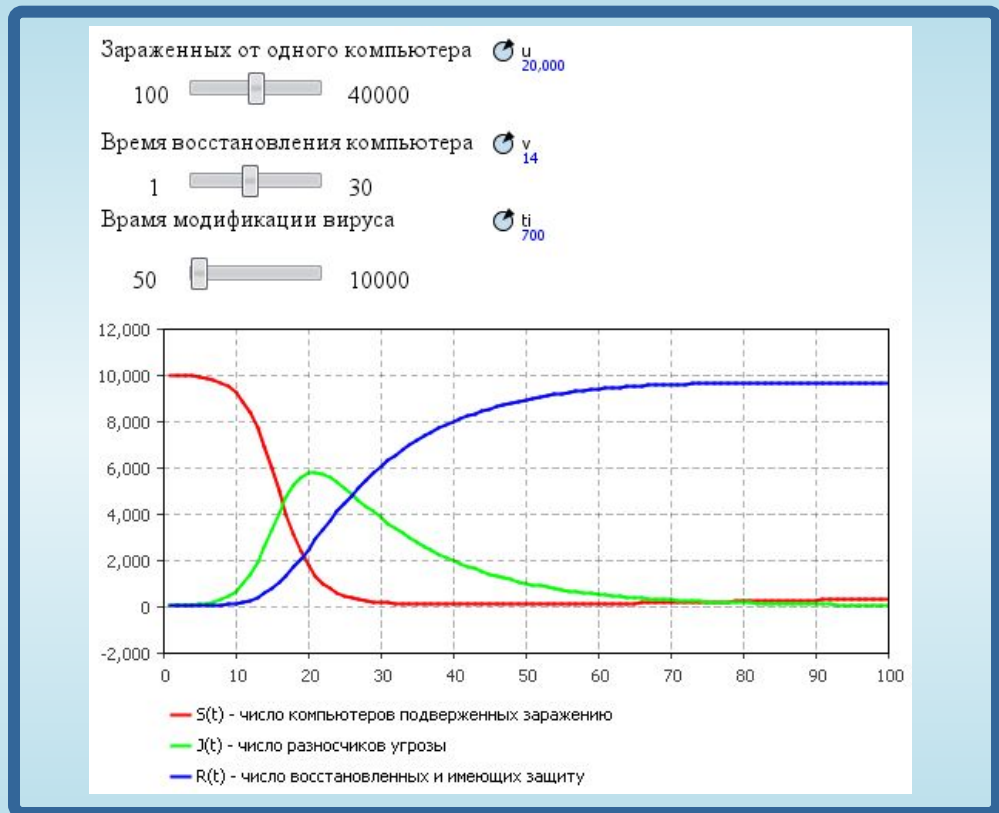


Рис. 2 – Анимация модели с начальными значениями параметров

Изменение параметров модели

Разработанная модель в среде AnyLogic предназначена для исследования характеристик эпидемии в КС и процесса восстановления системы. Среда позволяет изменять значения параметров модели непосредственно во время ее работы, что в жизни аналогично вмешательству человека в различные процессы КС.

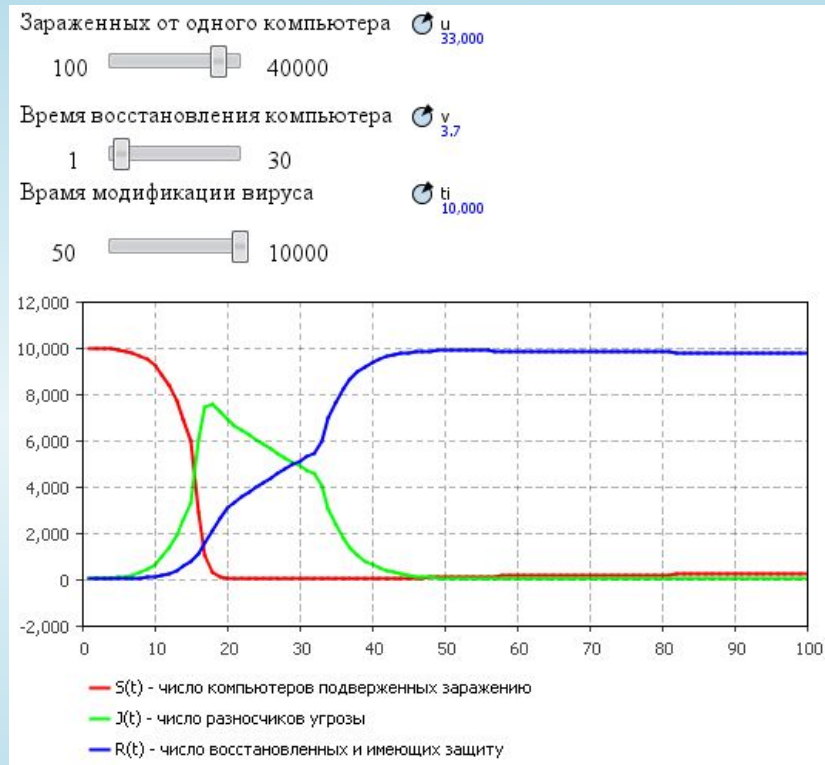


Рис. 3 – Анимация модели при изменении значений параметров

Эксперимент

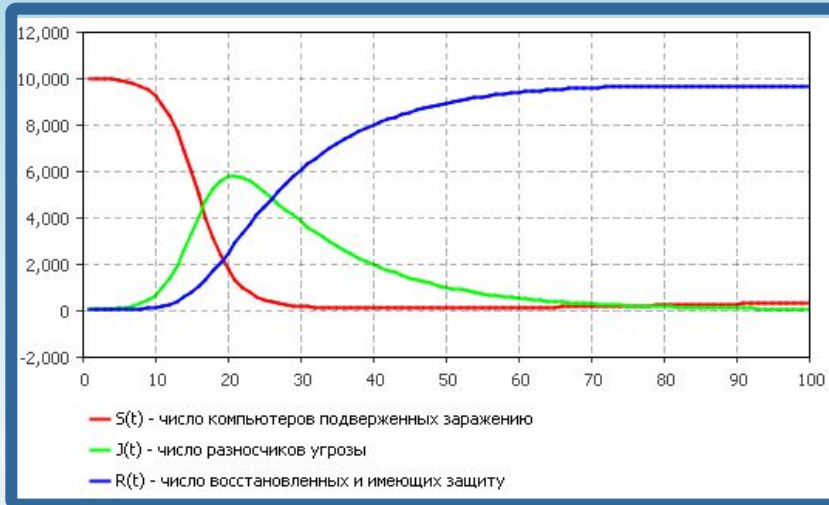


Рис. 4.
Результаты тестирования
SIR-модели при $K=10000$;
 $S(0)=9988$; $J(0)=10$;
 $R(0)=K - S(0) - J(0)$;
 $\beta = 5 \cdot 10^{-5}$ $\gamma = 0,071$

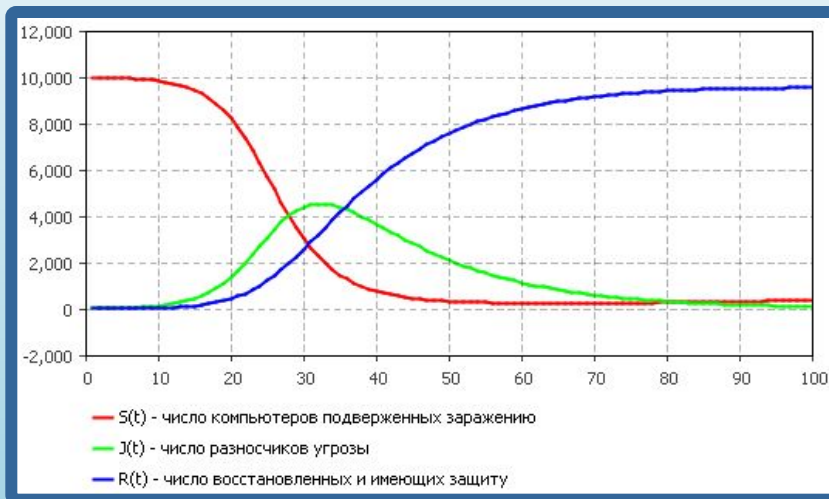


Рис. 5.
Результаты тестирования
SIR-модели при $K=10000$;
 $S(0)=9988$; $J(0)=10$;
 $R(0)=K - S(0) - J(0)$;
 $\beta = 3,3 \cdot 10^{-5}$ $\gamma = 0,071$

Эксперимент

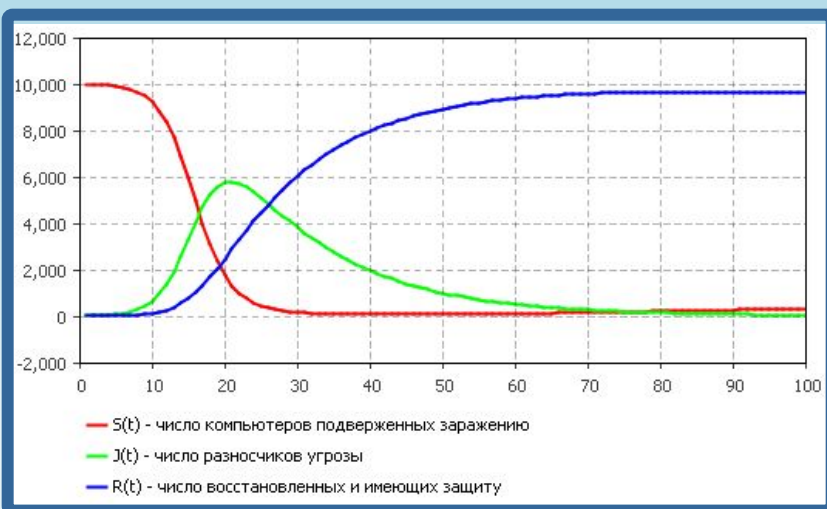


Рис. 6.
Результаты тестирования
SIR-модели при $K=10000$;
 $S(0)=9988$; $J(0)=10$;
 $R(0)=K - S(0) - J(0)$;
 $\beta = 5 \cdot 10^{-5}$ $\gamma = 0,071$

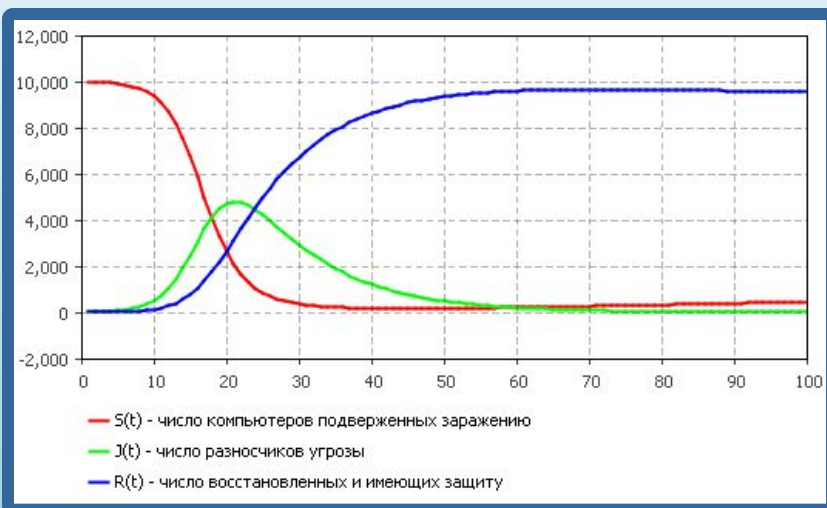


Рис. 7.
Результаты тестирования
SIR-модели при $K=10000$;
 $S(0)=9988$; $J(0)=10$;
 $R(0)=K - S(0) - J(0)$;
 $\beta = 5 \cdot 10^{-5}$ $\gamma = 0,1$

Выводы

С помощью изоляции зараженных субъектов (исключение восприимчивых узлов из сети на время распространения вредоносной программы) и применения более эффективных средств восстановления зараженных субъектов можно сгладить кривую зараженных (получить меньший пик числа зараженных), с помощью последнего метода также можно сократить время эпидемии.



Спасибо за внимание