ПРИМЕНЕНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ ИССЛЕДОВАНИЯ ХАРАКТЕРИСТИК ЭПИДЕМИИ В РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ И ПРОЦЕССА ВОССТАНОВЛЕНИЯ СИСТЕМЫ

Л. М. Груздева (г. Владимир)

Современная наука определяет распределенную информационно-вычислительную систему (РИВС) в качестве технологической основы АСУП, часто делая данные понятия синонимами. Распределенная обработка данных, используя разделение функций АСУП, обладает несомненными достоинствами, такими как открытость, малое время отклика, высокая доступность, возможность совместного использования ресурсов, инкрементального наращивания мощности как системы в целом, так и ее компонентов.

Тем не менее эти качества порождают и уязвимости, среди которых одна из важнейших – слабая защита от вредоносных программ (ВП, вирусов). Конечно, выстраиваются различные системы защиты, включающие аппаратные и программные средства, однако всегда существует вероятность поражения РИВС, даже если косвенные признаки угрозы в каких-то из узлов определены. Поражение ресурсов РИВС влечет за собой как минимум снижение качества функционирования всей АСУП.

Модель распространения вредоносных программ будет способствовать лучшему пониманию процессов тотального поражения РИВС, позволит предсказать зарождение катастрофической ситуации (эпидемии), а значит, выработать необходимое противодействие, в случае же невозможности защиты – заранее инициировать процессы эвакуации охраняемых информационных ресурсов.

В исследовании динамики распространения ВП нашли широкое применение претерпевшие различные модификации эпидемиологические математические модели, в том числе SI-модели и SIS-модели [1–3]. Но данные модели не учитывает наличия некоторого блокирующего фактора, скажем, антивирусного программного обеспечения.

Рассмотрим Progressive SIDR (PSIDR) модель, состоящую из двух фаз (рис. 1): *начальное заражение* – ВП заражает один узел РИВС и затем в течение некоторого времени распространяется свободно, т.е. согласно SI-модели; *фаза реакции* – по прошествии некоторого времени ВП обнаруживается и со стороны субъектов производятся немедленные действия. Все принципалы, оставшиеся незаражёнными, автоматически вакцинируются, а инфицированные – обнаруживаются с определённой скоростью, избавляются от инфекции и приобретают иммунитет. В этой фазе скорость распространения остаётся прежней, однако восприимчивые принципалы вакцинируются со скоростью μ, а инфицированные субъекты обнаруживаются со скоростью μ и «лечатся» со скоростью δ (μ представляет собой не что иное, как скорость обновления антивируса).

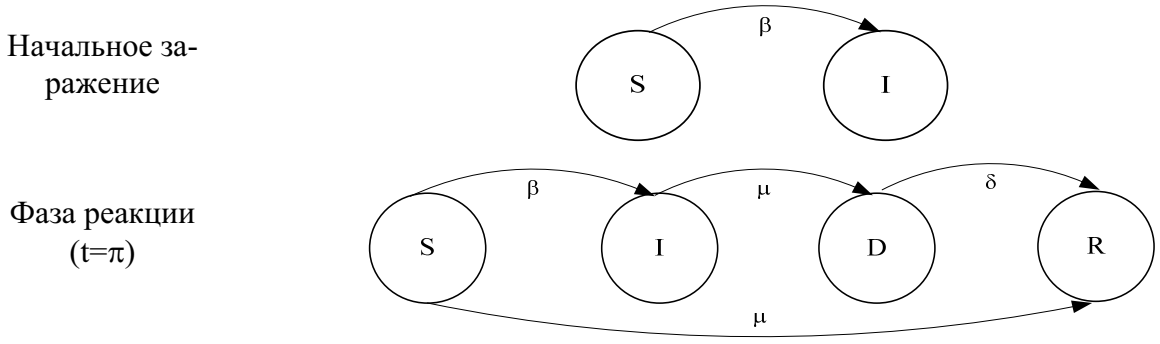

Рис. 1. Графы состояния субъекта в модели PSIDR

В первой фазе система ведёт себя согласно законам: $\begin{cases} \frac{dS(t)}{dt} = -\beta S(t)I(t) \\ \frac{dI(t)}{dt} = \beta S(t)I(t) \end{cases}$,

а во второй – $\begin{cases} \frac{dS(t)}{dt} = -\beta S(t)I(t) - \mu S(t) \\ \frac{dI(t)}{dt} = \beta S(t)I(t) - \mu I(t) \\ \frac{dD(t)}{dt} = \mu I(t) - \delta D(t) \\ \frac{dR(t)}{dt} = \delta D(t) + \mu S(t), \end{cases}$

где $S(t)$ – число субъектов подверженных заражению, $I(t)$ – число разносчиков ВП, $R(t)$ – число восстановленных и имеющих защиту, $D(t)$ – количество обнаруженных инфицированных субъектов. При этом начальные условия для системы таковы: $S > 0$, $I > 0$, $D=0$, $R=0$.

Зависимость продолжительности эпидемии от времени беспрепятственного распространения ВП исследовалась с помощью системы AnyLogic. Структура и анимация имитационной модели распространения ВП представлена на рис. 2 (взаимодействия между переменными показаны стрелками).

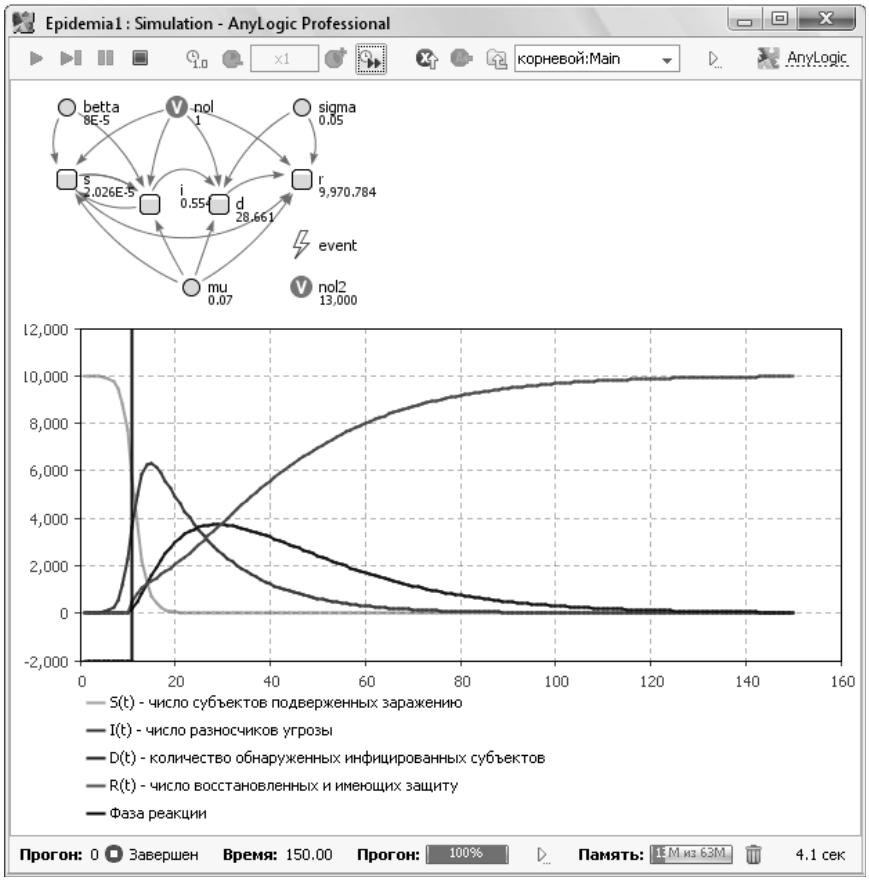

Рис. 2. Структура и анимация PSIDR-модели

Разработанная модель в среде AnyLogic предназначена для исследования характеристик эпидемии в РИВС и процесса восстановления системы. Среда позволяет изменять значения параметров модели непосредственно во время ее работы, что в жизни аналогично вмешательству человека в различные процессы РИВС. За счет этого можно оценить влияние каждого из параметров или сочетания параметров в период протекания эпидемии, точно и всесторонне исследовать процесс распространения ВП в РИВС.

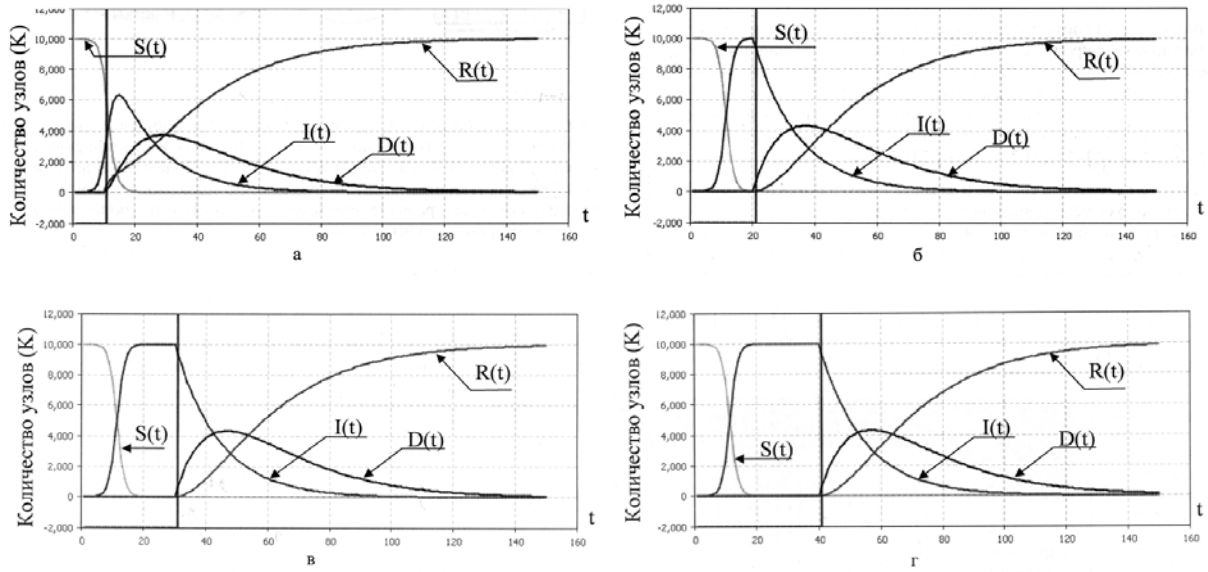

Рис. 3. Результаты тестирования PSIDR-модели (*K=10000; S(0)=9999; I(0)=1; R(0)=D(0)=0;* $\beta = 8 \cdot 10^{-5}$ $\delta = 0{,}05$; $\mu = 0{,}07$):
а **–** $\pi = 10$; ***б*** **–** $\pi = 20$; ***в*** **–** $\pi = 30$; ***г*** **–** $\pi = 40$

Анализ модели выявляет тот факт, что обновление антивируса должно происходить как можно раньше (рис. 3), потому что любая задержка обновления приводит ко всё большим и большим периодам «взрыва» эпидемии. Тем не менее, даже если вакцина будет доступна немедленно, эпидемия будет распространяться довольно быстро, так как начнётся «борьба» за субъекты между ВП и системой защиты. Этот феномен предполагает, что общая безопасность РИВС может быть значительно увеличена за счёт скорости доставки обновлений (например, это можно реализовать, регулируя частоту запроса клиентами «заплаток» с центральных серверов).

Для проверки адекватности представленной модели был поставлен ряд экспериментов в экспериментальной сети (ее схема представлена в [4]). Экспериментальные данные в целом подтвердили адекватность моделей. Наибольшие расхождения (максимальная относительная погрешность 7,33%) наблюдаются при высокой интенсивности ВП, что можно объяснить тем, что в моделях практически невозможно учесть ограничения, обусловленные задержками сканирующих подключений в ОС, ограничения на количество полуоткрытых исходящих соединений, интервал времени, в течение которого подключение находится в режиме ожидания, ограничение на общее число одновременно открытых подключений.

Литература

1. Leveille J. Epidemic Spreading in Technological Networks http://www.hpl.hp.com/techreports/2002/HPL-2002-287.pdf.
2. **Груздева Л. М., Монахов Ю. М.** Об одной математической модели динамики распространения вредоносных программ. // Математические методы в технике и технологиях – ММТТ-20. Сб. трудов XX междунар. науч. конф. В 10 т. Т. 6. Секция 12 / Под общ. ред. В.С. Балакирева. Ярославль: Изд-во Ярос. гос. техн. ун-та, 2007. С. 65–66.
3. **Куличкова О. Э., Обухова Ю. М., Груздева Л. М.** Исследование SIR-модели динамики распространения вредоносных программ в системе AnyLogic // Управление качеством машиностроения технологических процессов формообразования: труды международной студенческой конференции. М.: ГОУ ВПО МГТУ «Станкин», 2010. С. 123–127.
4. **Груздева Л. М., Монахов Ю. М., Монахов М. Ю.** Экспериментальное исследование производительности корпоративной телекоммуникационной сети // Проектирование и технология электронных средств. 2009. № 4. С. 21–24.