– определяется количество мер возможности противодействия каждого средств защиты каждой угрозы.

Очевидно, если множество {M} такое, что устраняются все ребра графа, то такая система является системой с полным перекрытием (рис.3).

Данная модель позволяет оценить защищенность информационной системы, рассчитать затраты на построение системы защиты, а также выбрать оптимальный вариант на построение системы сетевой защиты.

Список литературы

1. Математическое моделирование процесса выбора средств защиты персональных данных / В. И. Аверченков и др. // Вестник БГТУ. 2013. № 3. С. 95–99.

2. Волклов О. А. Разработка и анализ моделей политики безопасности компьютерной сети // Известия высших учебных заведений. Поволжский регион. 2011. № 2 (18). С. 38–45.

3. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М., 1996. 192 с.

4. Шаньгин В. Ф. Защита информации в компьютерных системи сетях // ДМК прес. 2012. 592 с.

УДК 004.94

В. А. Минаев, М. П. Сычёв,
Е. В. Вайц, Ю. В. Грачёва
(Московский государственный технический университет
имени Н. Э. Баумана)

МОДЕЛИРОВАНИЕ ВИРУСНЫХ ЭПИДЕМИЙ В КОМПЬЮТЕРНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ ПРИНЦИПОВ СИСТЕМНОЙ ДИНАМИКИ

Вирусная атака – действие, целью которого является захват контроля (повышение прав) над удаленной/локальной вычислительной системой, либо ее дестабилизация, либо отказ в обслуживании. В результате успешной вирусной атаки в компьютерную сеть могут внедряться вредоносные программы, самостоятельно распространяющиеся через локальные и глобальные компьютерные сети. Исследование динамики распространения таких вредоносных программ по сети является актуальной задачей и на текущий момент накоплен определенный опыт в данном направлении [1–4]. Развитием данных работ является применение методов имитационного моделирования, позволяющих исследо-

вать взаимное влияние различных параметров моделей распространения компьютерных вирусов, решать задачи оптимизации и управления [5].

В качестве метода имитационного моделирования для исследования эпидемий в компьютерных сетях выбран метод системной динамики, впервые предложенный и обоснованный Дж. Форрестером в 1950 годах и позволяющий учитывать большое количество причинно-следственных связей между объектами. Основными элементами системно-динамических моделей являются уровни, отражающие различного рода накопления, происходящие в модели, и темпы, определяющие динамику модели [6].

Рассмотрим в статье базовую системно-динамическую SIR-модель (susceptible – infected – removedmodel) динамики распространения компьютерных вирусов по сети, основывающуюся на модели биологических процессов эпидемий [1], [7–9].

В SIR-модели хосты сети существуют в трех состояниях: уязвимом (*S*), зараженном (*I*) и «вылеченном» (*R*) (рис. 1).

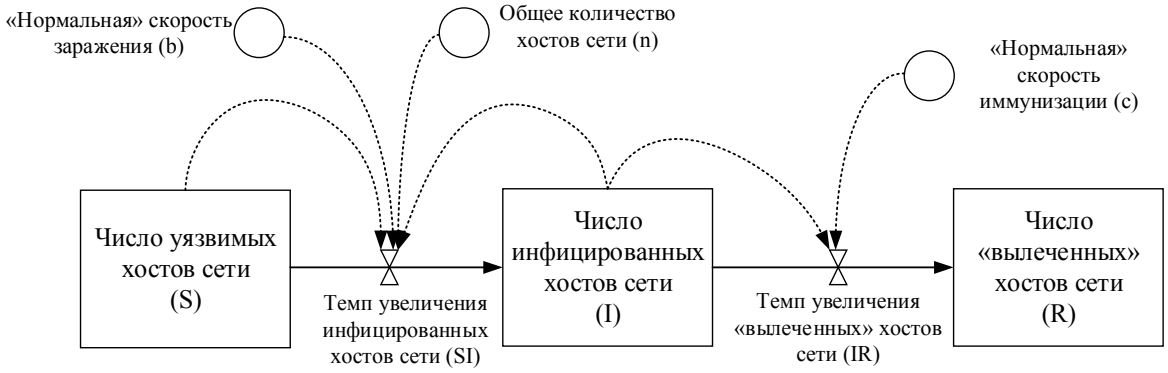

Рис. 1. Системно-динамическая модель распространения компьютерных вирусов по сети на основе SIR-модели

Приведем расшифровку условных обозначений, используемых в модели (таблица 1).

Таблица 1

Условные обозначения, используемые в модели

№ п/п	Условное обозначение элемента	Название элемента (единицы измерения)
1	S	Число уязвимых хостов сети (шт.)
2	I	Число инфицированных хостов сети (шт.)
3	R	Число «вылеченных» хостов сети (шт.)
4	n	Общее количество хостов в сети (шт.)
5	SI	Темп увеличения инфицированных хостов сети (шт./час)
6	IR	Темп увеличения «вылеченных» хостов сети (шт./час)
7	b	«Нормальная» скорость заражения (часть/час)
	c	«Нормальная» скорость иммунизации (часть/час)

Понятие «нормальной» скорости введено Дж. Форрестером [6], представляя отношение числа зараженных или «вылеченных» хостов в час к общему количеству уязвимых хостов.

Системно-динамическая модель описывается следующей системой равнений:

$$\begin{cases} \frac{dS}{dt} = -SI(\mathrm{t}) \\ \frac{dI}{dt} = SI(\mathrm{t}) - IR(\mathrm{t}) \\ \frac{dR}{dt} = IR(\mathrm{t}) \\ SI(\mathrm{t}) = \frac{b \cdot I(\mathrm{t}) \cdot S(\mathrm{t})}{n} \\ IR(\mathrm{t}) = c \cdot I(\mathrm{t}) \end{cases} \quad (1)$$

Модель распространения компьютерных вирусов в сети на основе SIR-модели реализована в программе Anylogic, ее общий вид приведен на рисунке 2.

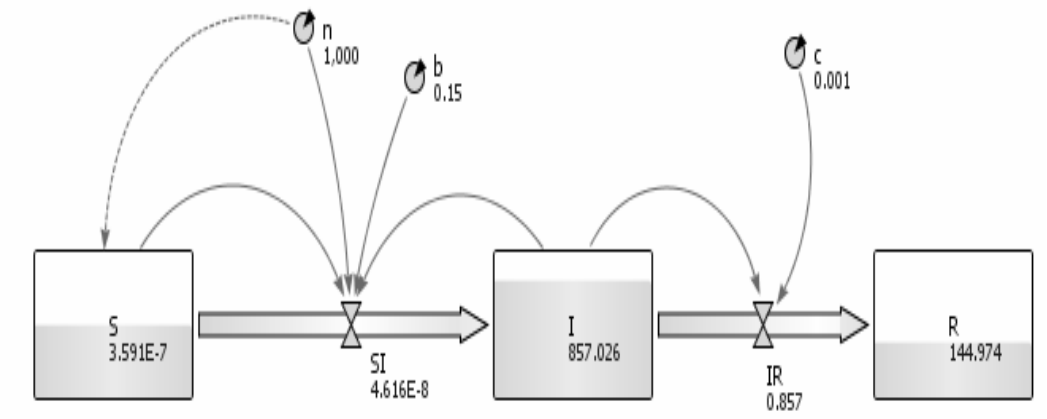

Рис. 2. Общий вид модели распространения компьютерных вирусов в сети

Проведены два имитационных эксперимента, в которых исследуется динамика количества уязвимых, инфицированных и «вылеченных» хостов сети в зависимости от «нормальной» скорости иммунизации.

Задачей экспериментов является выявление степени влияния различных значений параметра *c* («нормальная» скорость иммунизации) на динамику множеств: *S* (уязвимые хосты сети), *I* (инфицированные хосты сети), *R* («вылеченные» хосты сети). В таблице 2 приведены значения параметров модели и обозначения её выходных данных в результате экспериментов.

Таблица 2

Значения параметров модели и обозначения ее выходных данных

№ эксперимента	Значение параметра			Значение отклика		
	b	c	n	S	I	R
1	0,15	0,001	1000	$S_1(t)$	$I_1(t)$	$R_1(t)$
2	0,15	0,02	1000	$S_2(t)$	$I_2(t)$	$R_2(t)$

Начальные значения других параметров модели определены следующим образом: $\{S(0) = n; I(0) = 2; R(0) = 0\}$.

Временные графики, отражающие результаты первого эксперимента (рис. 3а), показывают, что в данном случае эпидемию распространения компьютерного вируса не удалось остановить за приемлемый период времени. Временные графики, отражающие результаты второго эксперимента (рис. 3б), при котором «нормальная» скорость иммунизации была увеличена в 20 раз, показывают, что эпидемию распространения компьютерного вируса удалось остановить за конкретный приемлемый период времени.

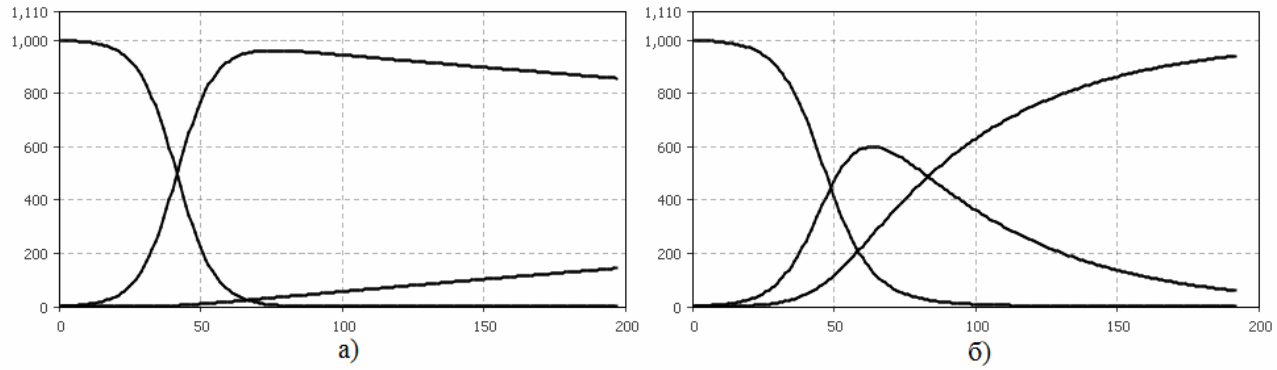

Рис. 3. Динамика уязвимых, инфицированных и «вылеченных» хостов при первом (а) и втором (б) эксперименте

Выводы по результатам экспериментов: проведенные эксперименты продемонстрировали два возможных варианта развития эпидемии компьютерного вируса при разных значениях «нормальной» скорости иммунизации.

Выводы

1. Задача исследования и прогнозирования динамики распространения компьютерных вирусов по сети является актуальной, как для организаций – владельцев компьютерных сетей, так и для организаций, разрабатывающих антивирусное программное обеспечение. Разработанный на сегодняшний день математический аппарат позволяет продвинуться в построении имитационных моделей, отражающих динамику эпидемий компьютерных вирусов в сетях и позволяющих выявлять их наиболее критичные параметры и степень воздействия на эпидемии.

2. В качестве методологической основы исследования распространения компьютерных вирусов выбран метод системно-динамического моделирования, широко применяемый на сегодняшний день для решения различных практических задач по прогнозированию, управлению и оптимизации деятельности по борьбе с компьютерными вирусами.

3. Предложенная системно-динамическая модель распространения компьютерных вирусов реализована в перспективной программной среде Anylogic, что позволяет проводить с данной моделью самые раз-

личные теоретически и практически важные имитационные эксперименты

4. Дальнейшим развитием работы является построение комплекса модифицированных системно-динамических моделей распространения компьютерных вирусов по сети и процессов обеспечения её информационной безопасности и проведение дополнительной серии имитационных экспериментов с различными комбинациями факторов, определяющих вирусных эпидемий.

Список литературы

1. Котенко И. В., Воронцов В. В. Аналитические модели распространения сетевых червей : тр. СПИИРАН. СПб., 2007. С. 208–224.

2. Захарченко А. Черводинамика: причины и следствия // Защита информации. Конфидент. 2004. № 2. С. 50–55.

3. Семыкина Н. А., Шавыкина И. В. Математическая модель защиты компьютерной сети от вирусов // Программные продукты и системы / Software&Systems. 2016. Т. 29. № 4. С. 125–128.

4. Семенов С. Г., Давыдов В. В. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом. Сер. Информатика и моделирование. Харьков, 2012. № 38. С. 163–171.

5. Аверенков В. И., Федоров В. П., Хейфец М. Л. Основы математического моделирования технических систем. М., 2011. 271 с.

6. Форрестер Д. Основы кибернетики предприятия (индустриальная динамика). М., 1971. 340 с.

7. Эпидемиологические детерминанты неравномерного территориального распространения брюшного тифа / Ю. П. Солодовников [и др.] // Журн. микробиол., эпидемиол. и иммуноб. 1995. № 6. С. 31–33.

8. Моделирование динамики заболеваемости сифилисом с учетом влияния на параметры деятельности системы здравоохранения / О. Т. Тесалова [и др.]. 1983. № 2. С. 39–44.

9. Kephart J. O., White S. R. Directed graphepidemiological models of computer viruses // Proceeding sof the 1991 IEEE computer society symposium on research in Security and privacy. Oakland, California. 1991, pp. 343–359.

10. Минаев В. А., Вайц Е. В., Грачева Ю. В. Динамическая модель обеспечения информационной безопасности организационных систем, подверженных риску : материалы Междунар. науч.-техн. конф. «Системы безопасности» (г. Москва, 24 нояб. 2016 г.). М., 2016. С. 24–27.